OIPC File No: F15-63155

Inquiry under Part 5 of the Freedom of Information and Protection of Privacy Act ("FOIPPA") between:

An Applicant

and

the Vancouver Police Department ("VPD")

and

BC Association of Chiefs of Police (intervenor) and BC Association of Municipal Chiefs of Police (intervenor) and BC Civil Liberties Association (intervenor) and BC Freedom of Information and Privacy Association (intervenor) and Open Media (intervenor) and Canada Research Chair of Ethics, Law and Technology, University of Ottawa (intervenor)

Reference Material for the Submissions of the British Columbia Civil Liberties Association and Canada Research Chair of Ethics, Law and Technology, University of Ottawa

---

Micheal Vonn and Michael Elliot
British Columbia Civil Liberties Association
900 Helmcken St., 2nd Floor
Vancouver BC V6Z 1B3
Tel: 604.630.9753
Email: micheal@bccla.org

Ian Kerr
Canada Research Chair of Ethics, Law & Technology
University of Ottawa
57 Louis pasteur St.,
P.O. Box 450, Stn. A
Ottawa ON K1N 6N5
Tel: 613.562.5800 ext 3281
Email: iankerr@uottawa.ca

I N D E X

SURVEILLANCE, THEN AND NOW: Securing Privacy in Public Spaces

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

June 2013

Acknowledgements

I would like to express my deepest appreciation to Stephen McCammon for all his hard work and dedication! His invaluable contributions were vital in giving this paper life.

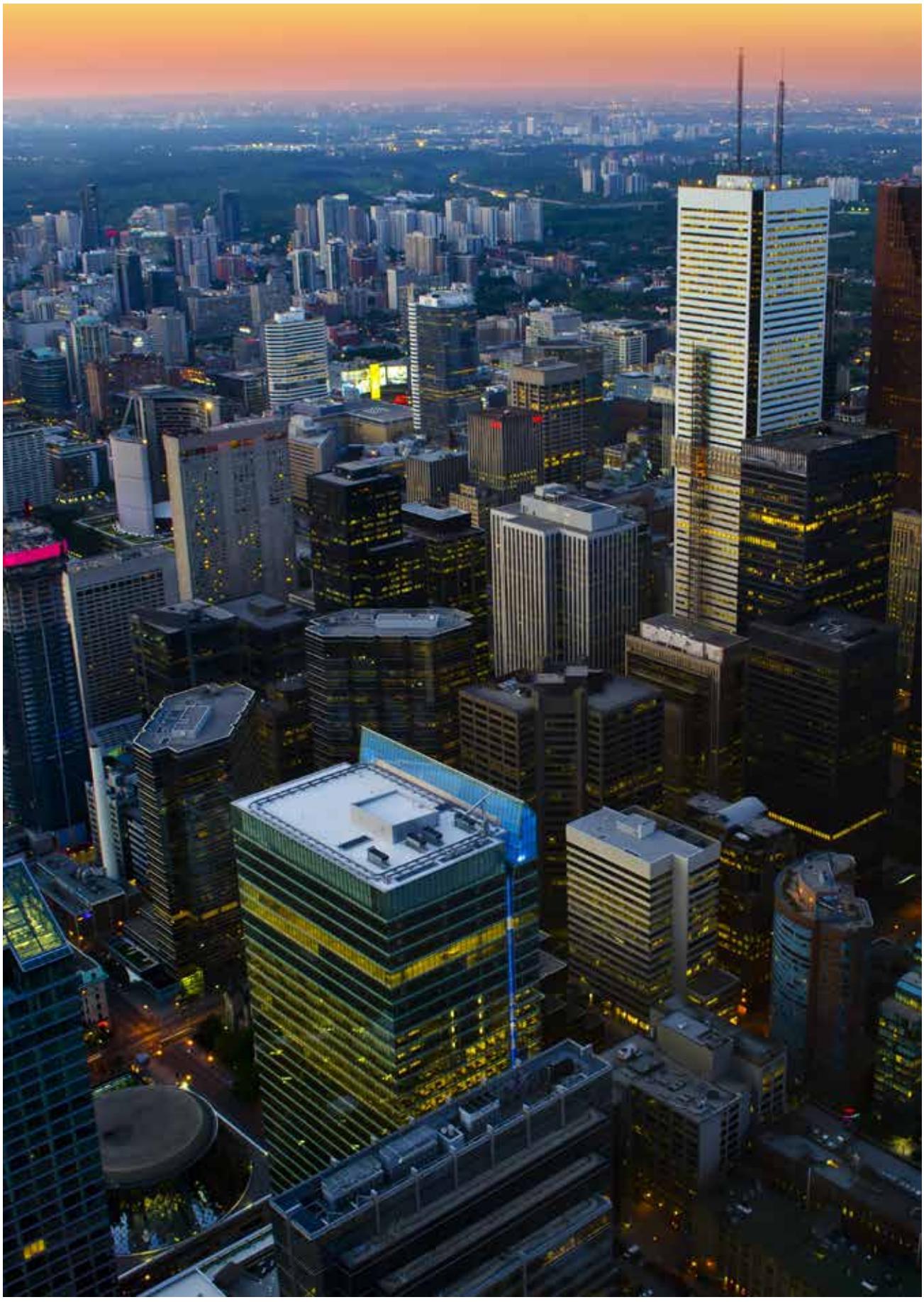
I would also like to recognize Hannah Draper for her tireless efforts and Jenny Ryu for her support in preparing this paper.

Information and Privacy Commissioner, Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Table of Contents



Executive Summary

Surveillance is growing, as are the technologies that extend its reach. But surveillance that facilitates the sustained monitoring of people engaged in everyday activities in public is, in Justice Gérard La Forest's unforgettable words, "an unthinkable prospect in a free and open society such as ours."[1]

Unthinkable as it may be, the prospect of close and continuous surveillance is no longer simply the stuff of science fiction. Governments now have access to precise and affordable technologies capable of facilitating broad programs of indiscriminate monitoring. The unfettered use of these technologies raises the spectre of a true surveillance state. To freedom-loving people, that is an unacceptable prospect.

The purpose of this paper is to assist law enforcement, lawmakers, and the broader public in understanding and protecting our fundamental right to privacy with respect to surveillance by the state of our activities in public spaces through the use of ever-growing new technologies.

Of course, our expectation of privacy in public spaces is lower than in private places. However, it is not entirely eliminated. Let us remember that the right to privacy protects people, not places. In addition, as governments consider the implications of recent terrorism-related developments in Canada and the United States, we must consider that new technologies may be able to provide increased efficiencies for law enforcement and their performance of vital public safety functions.

How can free and democratic societies ensure that the public receives the benefits associated with these new technologies, while continuing to provide strong privacy protections? To secure our right to privacy in public, in an era of explosive new technologies, requires a proactive approach that emphasizes the right to informational privacy owed to all citizens. The true value of privacy must be recognized, and ideally enhanced, not diminished, in any effort to modernize law enforcement powers.

A proactive *Privacy by Design* approach is central to designing and implementing the regulatory framework needed to properly supervise state surveillance. It is our experience that, where the use of a particular surveillance technology is justified, proportionate, and effective at delivering public safety, a proactive *positive-sum* approach is available that will ensure that privacy, accountability, and transparency are embedded into the legal and technical design specifications of any proposed surveillance system.

In an effort to encourage a proactive approach to the use and supervision of the next generation of surveillance technologies, this paper examines the following:

- The vital importance of privacy to freedom and liberty (Part I);
- How we came to secure privacy in government's information-handling practices, as well as in our private communications and activities (Part II); and
- A range of the current challenges to securing privacy in the online and digital world (Part III).

What emerges from this study is a set of 10 principles that we apply to law enforcement's use of four emerging surveillance technologies: video surveillance cameras and closed circuit television (CCTV), automatic licence plate recognition systems, geolocational tracking, and drone-based surveillance (Part IV).

One of the crucial principles is that the police power to deploy any form of intrusive surveillance technology must be supervised under a system of prior judicial authorization. The importance of this point cannot be overemphasized. Unfettered law enforcement access to surveillance technologies that are capable of facilitating indiscriminate monitoring threatens our right to a reasonable expectation of privacy, particularly where that monitoring may be continuous and persistent.

At the same time, not all surveillance programs are equally intrusive. For example, it is possible that surveillance may be effective without being persistent or penetrating. Nonetheless, with respect to the deployment of *any* surveillance technology, what will be required is the right mix of legal, administrative and technical controls to *ensure* that their use is appropriate and accountable.

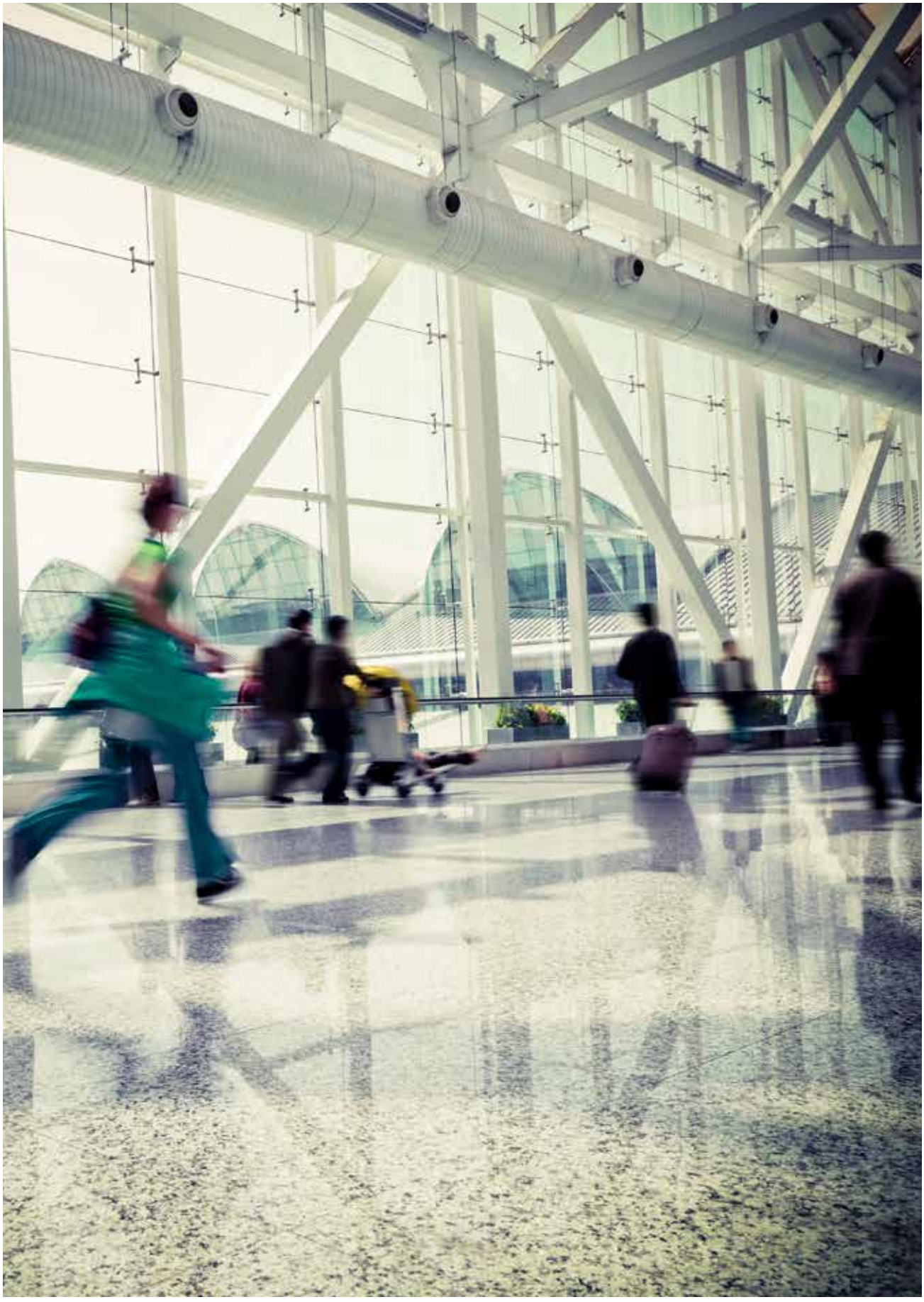
This paper sets out what we believe to be the controls necessary to ensure the appropriate and accountable use of CCTV video surveillance cameras, automatic licence plate recognition systems, geolocational tracking, and drone-based surveillance. Those controls include open, accountable and proportionate information-handling practices that are subject to independent scrutiny, including through notification and reporting requirements.

Whatever the future holds, we know that, in addition to privacy and freedom, people will require safety and security. We believe that now, and for the foreseeable future, it is essential that we strive to have both, in tandem. Freedom must be preserved from both terrorism and tyranny. While eternal vigilance will be required to secure our fundamental rights, including our right to privacy, we remain confident that we can have both public safety and personal privacy in public spaces. There is neither reason, nor need, to settle for anything less.

In summary, our approach to the proper supervision of law enforcement's use of new and emerging surveillance technologies is based upon the following key principles:

Privacy Principles in Public Spaces

1. *Data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate social objectives, and subjected to controls over its retention, subsequent use, and disclosure.*
2. *The state should be open and accountable for its information-handling practices.*
3. *Compliance with privacy rules and restrictions should be subject to independent scrutiny.*
4. *The authority to employ intrusive surveillance powers should generally be restricted to limited classes of individuals such as police officers.*
5. *The police power to deploy any form of intrusive surveillance must be supervised under a system of prior judicial authorization.*
6. *Even where genuine emergencies make it impracticable for the police to obtain judicial authorization before they employ surveillance measures, the state must remain transparent and accountable for its use of intrusive powers through subsequent, timely, and independent scrutiny of their use.*
7. *A positive-sum approach to designing a regulatory framework governing state surveillance can avoid false dichotomies and unnecessary trade-offs, demonstrating that it is indeed possible to have both public safety and personal privacy. We can and must have both effective law enforcement and rigorous privacy protections.*
8. *Close attention must be paid to the privacy impact of new technologies, business practices, and police tactics if we are to continue to ensure strong, principle-based privacy protections.*
9. *Surveillance practices that intrude upon privacy by leveraging new technological platforms or transmission processes must be scrutinized to ensure that they are accompanied by sufficiently rigorous privacy and accountability protections.*
10. *Eternal vigilance will be required to secure our fundamental rights, including the right to personal privacy in relation to all public spaces, including those found online and in other virtual spaces.*



Commissioner's Foreword

As we all adjust to the tragic bombings at the Boston Marathon, followed by the thwarted plot to derail a VIA Rail passenger train travelling between Toronto and New York, and the flurry of terrorism-related charges that ensued, it is critical that citizens of free and democratic societies raise their voices in support of those committed to achieving both security and privacy.

In this climate, the authorities in multiple jurisdictions, including the United States, will be under enormous pressure to overreact. Some officials are already arguing that they need "an enhanced ability to monitor public places."[2] Others have even suggested that, post-Boston, "privacy is overrated."[3] Of course, reasonable proposals to achieve real improvements in public safety should be welcomed, but the notion that we should somehow dispense with privacy protections is clearly excessive.

Proposals to obtain security at any cost must be resisted. In the drive for unattainably perfect security, we will invariably experience the real loss of privacy and freedom. As Benjamin Franklin, one of the founding fathers of the United States, wisely observed, "They that can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."[4]

I believe we must continue to seek measures designed to provide both security and privacy, in an accountable and transparent manner. Whether the issue is one relating to cybersecurity legislation or surveillance technologies ranging from CCTV cameras to biometrics, to automatic licence plate recognition to drones, we must reject the dated zero-sum, either/or, win/lose approach. By shifting to a positive-sum mindset focused on win-win solutions, we will be able to accommodate multiple legitimate interests, thereby avoiding unnecessary trade-offs and false dichotomies.

Introduction

> [I]n this era of explosive technology, can it be long before a device is developed that will be able to track our every movement for indefinite periods even without visual surveillance? … This is the time to begin regulating the use of electronic tracking devices while they are still in their infancy and before the law enforcement authorities begin routinely using them as part of their work habits.
>
> (*R. v. Wise*, 1992, Supreme Court of Canada Justice Gérard La Forest)

Governments around the world have long used technology to help prevent serious harm and prosecute wrongdoing. Periodically, however, in order to protect our fundamental right to privacy, lawmakers have had to respond by imposing controls on the use of intrusive new surveillance techniques. The purpose of this paper is to assist lawmakers, law enforcement, and the broader public in understanding and protecting our fundamental right to privacy, particularly with respect to state surveillance of our activities in public spaces using new technologies.

By state surveillance, we mean surveillance carried out by the law enforcement agencies responsible for investigating, prosecuting, and preventing serious harm. In the discussion that follows, we will be referring to these agencies using the terms law enforcement, the police, and the state interchangeably. As a regulator with oversight over law enforcement institutions, we have the greatest respect for the important work they do. At the same time, as Justice Jackson of the United States Supreme Court "pointed out in [a case dating back to 1948], law enforcement is a competitive enterprise in which government agents will naturally seek any strategic advantage available to them. Pursuit of that advantage naturally impels government agents, acting with the best of intentions, toward broader and more intrusive forms of surveillance."[5]

Twenty years have passed since the Supreme Court of Canada first grappled with the police use of a primitive "beeper" to track a suspect's car in *R. v. Wise*;[6] nearly 10 years since the Court looked at police surveillance from an airplane using an unsophisticated infrared radar camera in *R. v. Tessling*.[7] In the meantime, we have seen a significant increase in the state's capacity for intrusive surveillance. One emerging issue that raises substantial privacy concerns is the state's use of drones for domestic surveillance. Others include law enforcement's use of geolocational tracking and

Internet-based surveillance. Left unchecked, such surveillance will have considerable implications for the future of freedom and liberty.

Now, more than ever, it is critical that we revisit the way we supervise the state's use of new surveillance technologies. Neither a "wait and see" nor an individual "case by case" approach will suffice. Legislative rules, independent oversight, policy guidance, and administrative and technical controls can all contribute to the protection of privacy. To secure our right to privacy in an era of explosive new technologies, however, requires a proactive approach that emphasizes the right to informational privacy owed to all citizens.

The right to informational privacy or data protection includes the individual's right to exercise a significant measure of control over the collection, use, and disclosure of one's own personal information. In the context of state surveillance, individuals frequently do not have sufficient knowledge and power to effectively control the collection, use, and disclosure of their own personal information by law enforcement. Instead, the right to informational privacy must be protected by both: (i) the implementation of *Privacy by Design*[8] principles in the design and operation of legitimate state-deployed surveillance; and (ii) the insistence on legal rules and norms as found in systems of prior judicial authorization and other systems of independent oversight and accountability. The latter rules and norms are the primary focus of this paper. While special attention will be given to the Canadian context, we also look farther afield at developments in the United States (U.S.) and beyond.

Before considering some of the current challenges and emerging technologies, let us first recall the important role privacy plays in a free and democratic society, and look back at the emergence of FIPs-based[9] public sector privacy legislation and how we came to regulate some of the early and still-evolving surveillance techniques.

Part I – The Importance of Privacy

The protection of privacy is essential to safeguard the "type of society which Canadians, by the adoption of the Charter, have elected to live in." The constitutional restraints imposed on government limit its power to "pry into the lives of the citizen [and] go to the essence of a democratic state." Privacy rights and the legal rules supporting them are designed to increase government accountability while leaving individuals secure in the knowledge that "information collected by government institutions is relevant to their legitimate programs and operations."[10]

The right to privacy, which has its origins in the recognition of the inherent worth of the individual, plays a central role in the promotion of "respect for individual dignity and autonomy" and the "preservation of a free and democratic society."[11]

Privacy includes the right to exercise control over one's own person, personal spaces, and personal information. It preserves an "essential space for the development of ethically grounded citizens capable of engaging in the critical functions of public citizenship."[12] In shielding dissidents and human rights advocates, it supports and facilitates freedom of speech and freedom of association. It also helps to ensure freedom from interference and repression.

What of the right to privacy in public? "While the expectation of privacy in public spaces may be lower than in private spaces, it is not entirely eliminated."[13] We must remember that the right to privacy "protects people, not places."[14] In a 2012 case discussing the right to "public privacy" — a privacy right closely associated with our right to informational privacy — the Ontario Court of Appeal stated that "personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society."[15] Indeed, in the information and technology era we live in, the protection of our right to informational privacy is increasingly critical to the preservation of our rights to life, liberty, and security of the person — in essence, our freedom.

Properly understood, informational privacy protects our ability to live as both private and social beings, secure in the knowledge that the state will not access our personal information or seek to identify us, let alone record and retain our conversations, communications, movements, or activities, without just cause. These rights are guaranteed under section 8 of the *Charter of Rights and Freedoms* (the *Charter*), which provides that "Everyone has the right to be *secure* against unreasonable search or seizure."[16] This right to be secure is not the security or safety interest frequently invoked as a value weighing against or overriding privacy rights. Like its antecedent in the Fourth Amendment to the U.S. *Bill of Rights*, the constitutional concept of security that animates section 8 of the *Charter* was born of "the conviction that certain kinds of searches and seizures [are] intolerable."[17]

Today, both section 8 of the *Charter* and the Fourth Amendment recognize that everyone has a right to be secure against the use of unreasonable state powers in the form of unjustifiable and intrusive searches or seizures. As a general rule, this constitutionally mandated security can only be provided by ensuring that intrusive powers are subject to timely, exacting, and independent scrutiny.

In addition, privacy legislation such as Ontario's *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)[18] ensure that people "have a right to expect the following: that their personal information will only be collected for legitimate, limited and specific purposes; that the collection of their personal information will be limited to the minimum necessary for the specified purposes; and that their personal information will only be used and disclosed for the specified purposes."[19] In our view, these general principles apply to all public space surveillance systems.

Of course, in addition to privacy and freedom, people require safety and security. Benjamin Franklin's resounding cry from 1775 bears repeating: "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety." This declaration is as relevant today as it was then; we believe it is essential that we strive to have both together. We recognize that freedom must be preserved from both terrorism and tyranny.

And the public clearly recognizes this too. In the *aftermath* of the Boston Marathon bombings, a Time Magazine poll shows that 61 per cent of Americans are more concerned about the government enacting new antiterrorism policies that will excessively restrict civil liberties than they are about government going soft on security. Not surprisingly, at a time when private security cameras and personal cellphone cameras are always rolling (and considering their role in the quick identification and capture of the suspected bombers), Americans' tolerance for video surveillance in public places has spiked to a post-9/11 high (81 per cent are now in favour of increased cameras, up from 63 per cent). However, there are also indications that there is wariness about *enhanced* video surveillance. Two weeks *after* the bombings, support for use of facial recognition technology to scan public events has *declined* from a September 2001 high of 86 per cent to 79 per cent. More telling is the fact that "Americans are warier than ever about government monitoring of their cell phone and email communications, with 59 per cent opposed to such actions." In fact, only 38 per cent of Americans favour increased powers with respect to the monitoring of these communications, *down* from 54 per cent.[20]

Fortunately, we are not faced with the unpalatable and impractical choice of trying to prohibit the state from using emerging technologies for public safety purposes. By adopting a *Privacy by Design* framework and imposing legal, administrative, and technical controls to ensure that the use of such technologies is appropriate and accountable, we can accommodate all legitimate interests and objectives in a positive-sum, *win-win* manner, not the dated *zero-sum* model of *win/lose, either/or*. In this context, it is critical to recall that our approach to wiretapping, video surveillance and other forms of surreptitious electronic surveillance has allowed for necessary and effective law enforcement while securing the public interest in a reasonable expectation of privacy. Success in achieving a constitutionally appropriate regulatory framework has taken considerable time and debate, but the lessons learned point to the continuing need for a principled approach in order to sustain not only "peace, order and good government,"[21] but freedom and liberty.

Part II – Looking Back

Securing Privacy in Government's Information-Handling Practices

> [A] privacy protection policy intended to preserve informational privacy would therefore attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives and would attempt to maximize the control that individuals are able to exert over subsequent use and dissemination of information surrendered to institutional records keepers.[22]

In the years following the adoption of the *Charter* in 1982, comprehensive FIPs-based public sector privacy legislation was enacted across Canada. In one jurisdiction after another, federal and provincial Parliaments established rules restricting the collection, retention, use, and disclosure of personal information by institutions at all levels of government. These privacy rules also provided for rights of access and correction, complaint mechanisms, and other means of ensuring government compliance with and accountability for privacy requirements. The institutions bound by these rules include police services and a range of other institutions that carry out law enforcement functions. Independent Privacy Commissioners and ombudsmen were established to oversee compliance with privacy requirements.

The public concerns that motivated this wave of legislative activity focused on the fact that, in many circumstances, individuals were unlikely to have an effective choice to refuse to supply their personal information to the state, information holdings were becoming increasingly extensive, and there was public anxiety about government agencies sharing their holdings of personal information and building comprehensive files on individuals.

As with criminal law safeguards provided for by prior judicial authorization, FIPs-based privacy legislation was drafted with the intention of preventing privacy harms before they occur. Data minimization forms a critical component of privacy harm prevention. This principle instructs government not to collect, retain, use, or disclose any more personal information than is reasonably necessary to meet well-defined, legitimate social objectives.

Like the *Criminal Code of Canada* (*"Criminal Code"*)[23] rules providing for public reporting and after-the-fact notice with respect to wiretapping, compliance with FIPs-based privacy legislation ensures a commitment to openness and accountability. For example, government is generally required to be open about its data-handling practices, ensure the accuracy of its information holdings, and provide individuals the right to access and request a correction of their personal information. In addition, Privacy Commissioners have a role to play in recommending improved information-handling practices to ensure compliance with privacy requirements. Many may also order an institution to comply with privacy requirements.

The resulting framework of privacy statutes is not based on a confidentiality analysis in which privacy is only protected with respect to information that has been kept secret. Privacy statutes generally apply to all personal information collected by government, whether captured on the street or the Internet.[24] Moreover, a government institution's authority to collect personal information for one purpose does not entitle it to use that same information for a secondary purpose. In addition, while law enforcement officials have been granted exemptions from certain privacy rules,[25] their authority to collect, use, and disclose personal information must nonetheless fall within the scope of their law enforcement duties and powers as circumscribed in legislation, under the common law, and by the *Charter*.

The crucial principles to emerge with the rise of privacy legislation: *Data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate societal objectives, and subjected to controls over its retention, subsequent use, and disclosure. The state should be open and accountable for its information-handling practices. Compliance with privacy rules and restrictions should be subject to independent scrutiny.*

Further consideration will be given to the role of FIPs-based privacy legislation, as well as *Privacy by Design*, in Part IV of this paper. In the meantime, let us turn to consider how we came to regulate some of the early and evolving surveillance techniques.

Securing Privacy in Private Communications and Activities

> The right to privacy implies not just freedom from unreasonable search and seizure, but also the ability to identify and challenge such invasions, and to seek a meaningful remedy.
>
> (*R. v. Tse*, 2012, Supreme Court of Canada Justice Rosalie Abella)

There is a longstanding relationship between emerging technologies, police surveillance tactics, and the means by which we secure our right to privacy. Throughout this relationship, privacy has shown itself to be resilient, yet not to be taken for granted, even with respect to privacy in activities such as speaking on the telephone at home. Periodically, we face the challenge of law enforcement wanting a free hand in the use of new or evolving surveillance technologies. In response, we must ensure the proper supervision of their use of powerful new, evolving, and often undetectable surveillance technologies.

Consider, for example, that in Ontario in 1972, the decision to authorize audio surveillance of telephone conversations was made, not by a court, but by the police. At the same time, wiretapping technology had "advanced so rapidly" that the Ontario High Court of Justice recognized that:

> The apparatus used in snooping devices have been developed in such miniature and deceptive form that it has become difficult to detect that one is being subjected to its secretive observation or attention. Such listening is not now confined to apparatus directly connected with the telephone or with wires leading to one's residence. Devices have been developed that permit listening in to conversations in a room without any apparatus being installed in the premises whatsoever.[26]

While the High Court of Justice identified "a pressing need for legislation in Canada providing protection to the individual … and regulating the area within which such devices may be lawfully used," it nonetheless found that, at that time, a person had "no legally enforceable right to the privacy of his conversation even if held on the telephone." In this context, the Court was reluctant to "interfere with the judgment of the … Police [authority] as to the methods which it feels essential to meet the task of retaining law and order and suppressing crime."

Since this ruling, the public, governments, and Parliament, as well as the Courts, have given careful consideration to the police use of electronic surveillance in the course of their duties, and to the individual's right to privacy. Beginning in 1974 and with periodic updates over the ensuing decades, Parliament has laid down a detailed set of rules to both protect privacy in private communications and allow for necessary surveillance by the police. Now found in Part VI of the *Criminal Code*, these rules signal Parliament's appreciation that "as a general proposition, surreptitious electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under [section] 8 of the *Canadian Charter of Rights and Freedoms*."[27]

In Canada, this means the "presumed constitutional standard for searches or seizures in the criminal sphere" is judicial authorization: "a prior determination by a neutral and impartial arbiter, acting judicially, that the search or seizure is supported by reasonable grounds, established on oath[.]"[28]

In the early 1990s, this principle-based approach to protecting privacy was extended to video surveillance as well as to "all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future." In concluding that all such surveillance must be carefully regulated, the Supreme Court of Canada emphasized that:

> [T]here is an important difference between the risk that our activities may be observed by other persons, and the risk that agents of the state, in the absence of prior authorization, will permanently record those activities on videotape … To fail to recognize this distinction is to blind oneself to the fact that the threat to privacy inherent in subjecting ourselves to the ordinary observations of others pales by comparison with the threat to privacy posed by allowing the state to make permanent electronic records of our words or activities.[29]

As a result, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally requires prior judicial authorization wherever its use would intrude upon a person's reasonable expectation of privacy.[30]

The crucial principle to emerge over the two decades spanning 1972 – 1992: *the police power to deploy any form of intrusive surveillance must be supervised under a system of prior judicial authorization.*

The importance of this point cannot be overemphasized. Are there exceptions to this principle? What about in "genuine emergencies?"[31] If there must be an exception to the warrant requirement in emergencies, how can we ensure that the state remains accountable for the use of such an extraordinary power?

In an April 2012 case called *R. v. Tse*, the Supreme Court of Canada ruled that the state's statutory power to engage in warrantless wiretapping in an emergency was unconstitutional. The Court gave Parliament one year to amend the relevant provision in the *Criminal Code* (section 184.4). The fact that the nearly 20-year-old power includes strict statutory conditions to help ensure that warrantless interceptions are only available in exigent circumstances to prevent serious harm was found to be insufficient. What was missing was an effective means for ensuring accountability. In this context, the Court understood that:

> Unless a criminal prosecution results, the targets of the wiretapping may never learn of the interceptions and will be unable to challenge police use of this power. There is no other measure in the *Code* to ensure specific oversight of the use of s. 184.4. For s. 8 purposes, bearing in mind that s. 184.4 allows for the highly intrusive interception of private communications without prior judicial authorization, we see that as a fatal defect.[32]

In recognizing after-the-fact accountability as a critical privacy protection required under the *Charter*, the Court emphasized that its ruling would protect privacy rights without impairing important police functions:

> The obligation to give notice to intercepted parties would not impact in any way the ability of the police to act in emergencies. It would, however, enhance the ability of targeted individuals to identify and challenge invasions to their privacy and seek meaningful remedies.[33]

As the deadline for complying with the Court's order to ensure notice loomed, Parliament passed Bill C-55, the *Response to the Supreme Court of Canada Decision in R. v. Tse Act*.[34] Not only did the bill amend the *Criminal Code* to provide that a person who has been the object of an emergency wiretap must be notified of the interception within a specified period, it went further. The federal Minister of Public Safety and provincial Attorneys General are now required to issue annual public reports on the number of interceptions made under section 184.4. In addition, the wide range of officials previously permitted to conduct electronic surveillance under Part VI of the *Criminal Code* has been restricted to police officers. Mayors, bailiffs, prison guards, and other officials no longer have access to this extraordinary power.[35]

The Court's analysis in *Tse* and Parliament's legislative response provide an excellent example of the power of positive-sum thinking. The resulting regulatory framework achieves the goal of both enabling law enforcement functions and protecting privacy, demonstrating that it is as possible as it is desirable to have both.

The key principles to emerge from Tse: *Even where genuine emergencies make it impracticable for the police to obtain judicial authorization before they employ surveillance measures, the state must remain transparent and accountable for its use of intrusive powers through subsequent timely, exacting, and independent scrutiny of their use. The authority to employ intrusive surveillance powers should generally be restricted to limited classes of individuals such as police officers. A positive-sum approach to designing a regulatory framework governing state surveillance can avoid false dichotomies and*

unnecessary trade-offs, demonstrating that it is indeed possible to have both effective public safety and rigorous privacy protections.

Given the bewildering rate at which new, complex technologies and services continue to emerge, how can we continue to ensure the preservation of our right to privacy?

The Supreme Court of Canada decided a case raising these kinds of issues in March 2013. *TELUS v. The Queen* was initiated by a communications service provider determined to protect the privacy of its texting customers. Canadians communicate with one another through millions of text messages sent every day. As part of its standard business practices, TELUS briefly preserves records of such conversations, solely for the purpose of "troubleshooting customer problems."[36]

In the course of conducting a criminal investigation, the police may need to see a suspect's text message conversations. TELUS was faced with production orders requiring it to provide the police with access to anticipated *future* strings of text messaging conversations shortly after they are created and recorded. These court orders are easier to obtain and come with fewer safeguards than Part VI wiretap warrants. Protections provided under Part VI — but missing from a production order — include limits on: which officers can apply to conduct intrusive surveillance; when they can apply (only as a "last resort"); and whose privacy will be invaded, where, and in what manner. The protections also include accountability controls in the form of requirements that the authorities provide: notice to the surveillance target(s) within certain timeframes; and annual reports to Parliament concerning the number of applications made for authorizations under Part VI and the details thereof.

TELUS successfully questioned whether the police should have too-ready access to the ongoing conversations of Canadians simply because of the technical and customer service arrangements facilitating their effective delivery. We applaud TELUS for challenging the routine collection of such information by the police.

Faced with an emerging pattern of police applying for and obtaining hundreds of less onerous production orders requiring TELUS to provide police with future access to strings of such conversations, the Supreme Court of Canada observed that "technical differences inherent in new technology should not determine the scope of protection afforded to private communications."[37] The Court held that when the police seek to seize an anticipated stream of text messages, they must observe the same rigorous privacy and accountability protections governing the interception of other live or ongoing electronic communications, such as voice calls. In so ruling, the Court recommitted itself to the proposition that "the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 [of the *Charter*] is meant to keep pace with technological development … to ensure that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take."[38]

The key principles to emerge from TELUS: *Close attention must be paid to the privacy impact of new technologies, business practices, and police tactics if we are to continue to ensure strong principle-based privacy protections. Surveillance practices that intrude upon privacy by leveraging new technological platforms or transmission processes must be scrutinized to ensure that they are accompanied by sufficiently rigorous privacy and accountability protections.*

Part III – Current Challenges

Securing Privacy in the Online and Digital World

> [I]n Canadian society people can reasonably expect that they can move about on public highways [or while "participating in activities on the Internet"] without being identified and continually monitored by the state. If the state chooses to engage in that kind of invasive conduct, it must be able to meet the constitutional requirements of s. 8. … [W]hile the public nature of the forum in which an activity occurs will affect the degree of privacy reasonably expected, the public nature of the forum does not eliminate all privacy claims.
>
> (*R. v. Ward*, 2012, Ontario Court of Appeal Justice David Doherty)

In 2012, in a case concerning the ability of the police to pierce online anonymity by obtaining information linking an Internet Service Provider (ISP) customer to an Internet Protocol (IP) address associated with a criminal offence conducted online,[39] the Ontario Court of Appeal held that: "Anonymity 'to some degree at least' is a feature of much Internet activity ... Depending on the totality of the circumstances, [a person's] anonymity may enjoy constitutional protection under s. 8 [of the *Charter*]."[40] In this context, the Court affirmed that the right to privacy includes the concept of "public privacy." In particular, the Court's reasoning clarified that public privacy is the right to seek and find freedom from identification and surveillance with respect to activities engaged in within public spaces, including on the street and on the Internet.[41] In coming to this conclusion, the Court held that:

> Personal privacy is about more than secrecy and confidentiality. Privacy is about being left alone by the state and not being liable to be called to account for anything and everything one does, says or thinks.[42]

In reaching this conclusion, the Court gave careful attention to the implications of new technologies and business practices, as well as the relationship between the police, ISPs, and ISP customers.

While the Court rejected the notion that law enforcement should be able to "unilaterally, and without restraint, gather information [from third parties] to identify individuals engaged in public activities of interest to the state," it recognized that ISPs can, in the appropriate circumstances, exercise their discretion to disclose the personal information of a customer to the police for the purpose of assisting an active criminal investigation.[43] In this further example of the power of positive-sum thinking, the Court's reasoning allows for the maintenance of law and order and the protection of fundamental rights.

Contemporaneously, in Canada, the U.S., and the United Kingdom (U.K.), Legislators have been asked to authorize very significant changes to the relationship between ISPs and other communications service providers and the state. With these kinds of changes, communications service providers would be much more tightly controlled by the state, particularly through legislative proposals that would require the retention and warrantless disclosure of personal information to law enforcement and security agencies. If adopted, such proposals threaten our right to digital privacy and the related right to move about and participate in activities in social spaces without the risk of being identified and monitored by the state. Fortunately, the latest developments suggest that elected officials are becoming increasingly sensitive to the concerns their constituents have about state surveillance and the right to personal privacy. Consider the fate of three such bills: the U.K. *Communications Data Bill*; the U.S. *Cyber Intelligence Sharing and Protection Act*, and Canada's Bill C-30, the *Protecting Children from Internet Predators Act*.

In the United Kingdom

The U.K. government's July 2012 draft *Communications Data Bill* seeks to extend the range of information that communications service providers will have to store for up to 12 months. It would include — for the first time — communications traffic data related to messages sent on social media, by webmail, text, tweet, and instant messaging, in voice calls over the Internet and while gaming, in addition to emails and telephone calls. This data is capable of showing who was involved in what digital activity, and when and where. Pursuant to current U.K. law, a number of investigative bodies would have warrantless access to this data, namely the police, intelligence agencies, and revenue and customs authorities. They would not need the permission of a judge to see details of the time and place of digital messages, provided that they were investigating an offence or protecting national security. The bill would, however, place restrictions on warrantless access to the data by other public bodies, including local authorities.

The draft *Communications Data Bill* was subject to substantial scrutiny by a joint committee of the House of Commons and the House of Lords, which made its final report to Parliament in December 2012. The report was highly critical of the draft bill. In response to this criticism, the British government indicated that it will rewrite the legislation. As hinted at in the Queen's May 8th, 2013 Speech to the Throne, the new draft is expected shortly. However, many remain concerned about the risks associated with mandatory data retention. In this challenging context, many key questions remain. For example, will the retention requirements and access powers be clearly spelled out in the bill? Will they be justified and proportionate? Will the data be stored securely? Will law enforcement access be properly supervised? Under what circumstances, if any, should the state be allowed to have direct access to communications network traffic, for example, by way of automated inspection tools capable of sifting through all network traffic? Answers to these questions may dictate the state of digital privacy in the U.K. for years to come.

Meanwhile, the European Union Data Directive that requires European governments like that in the U.K. to enact data retention legislation is being reviewed. And, in the background, European Courts continue to declare provisions of some of the transposing national laws unconstitutional. As observed in rulings from countries such as Romania and Germany, sweeping communications data retention requirements expose people to the potential for arbitrary state action and generate a perception of surveillance which — on its own — may impair the free exercise of fundamental rights. In addition, those Courts have indicated that such laws may not be necessary, efficacious, or appropriate given that criminals may be able to sidestep a data retention regime through the use of offshore service providers and anonymous SIM cards. Sooner or later, the European Court of Justice will likely have to determine whether the broad mandatory retention of communications data comports with the "right to a private life" guaranteed in the European Convention on Human Rights.[44]

In the United States

In February 2013, the proposed *Cyber Intelligence Sharing and Protection Act* (*CISPA*) was reintroduced before the U.S. Congress. It passed the House of Representatives in mid-April, 2013. If such a bill were enacted, it would authorize broad information-sharing between government agencies and private sector companies (including of the content of communications) and provide the private sector with substantial immunity from civil and criminal proceedings. At the same time, *CISPA* provides for a degree of post-disclosure oversight by the Inspector General and Congress.

Supporters of *CISPA* see it as a means of helping companies and government share information to catch "bad actors" who breach networks to steal information or sabotage systems. Critics worry it will trump existing privacy laws, and

allow information about the mobile activities and Internet communications of Americans to go directly to law enforcement and intelligence agencies without effective checks and balances. Given that companies are already permitted to disclose personal information to the authorities in a range of related circumstances,[45] it appears that *CISPA* sets the stage for unjustified and overbroad information-sharing.

Meanwhile, President Barack Obama's February 2013 Executive Order, "Improving Critical Infrastructure Cybersecurity," has been praised for focusing on cybersecurity solutions that do not negatively impact civil liberties. That Order directs federal departments and agencies to use their existing authorities to provide better cybersecurity, with an emphasis on increased information-sharing by government and the private sector, while adhering to "Fair Information Practice Principles, and other applicable privacy and civil liberties frameworks and polices."[46]

In this context, it is expected that cybersecurity proposals will face close scrutiny in the Senate in the months ahead, particularly in view of President Obama's April 16th, 2013 statement that he will veto an insufficiently privacy-protective *CISPA*. Indeed, at the end of April, the Senate signalled that protecting privacy will be critical to its efforts to strengthen cybersecurity. Media reports also indicate that while the Senate may yet introduce a different information-sharing bill at some point, the House version will not be advanced any further.[47] Coming up with a good plan to protect cybersecurity is, of course, essential, as is respect for privacy.

Meanwhile, on May 15th, 2013, U.S. Attorney General Eric Holder signalled that the U.S. Justice Department supports privacy protections requiring the government to obtain a probable cause warrant in order to access emails and other content stored in the Cloud. This provides further reason to be hopeful for a comparable privacy-protective approach to cybersecurity legislation.

In Canada

In Canada, proposed legislative changes introduced before Parliament in February 2012 represented the most significant attempt to rewrite the rules governing electronic surveillance since the 1970s. Unfortunately, the bill's drafters appeared to misconceive how Canadians interact with new communications technologies and significantly underestimated the sensitivity of the personal information involved. As a result, Bill C-30 amounted to a sweeping proposal for new surveillance powers without adequate attention to necessary privacy protections.

In particular, the bill would have significantly increased the state's surveillance capacity by: (i) allowing for warrantless access to subscriber information identifying and linking customers to both their online and offline, mobile and desktop activities; (ii) expanding, simplifying, and accelerating court-supervised avenues for law enforcement access to and monitoring of other sensitive digital information and activity; and (iii) giving the state significant control over the design of communications systems and software. Privacy Commissioners, civil society groups, and a wide variety of citizens spoke out forcefully against the privacy-invasive bill. While acknowledging that it contained some positive elements, we warned that it "represented a looming system of 'surveillance by design.'"[48]

An engaged public recognized the risks the bill posed to privacy in digital communications and joined together to call on their elected representatives to reject the proposed surveillance powers. To their credit, Members of Parliament and the government listened to the enormous public outcry against overbroad and warrantless access and withdrew the bill in February 2013. Together we demonstrated that the true value of privacy must be recognized — and ideally enhanced, not diminished — in any effort to modernize law enforcement powers.

With citizens calling on government to withdraw or at least rewrite controversial privacy-intrusive legislative proposals, now more than ever, it is crucial that we deepen our commitment to work together to help ensure that: (i) first and foremost, *Privacy by Design* is built into new communications systems and other technologies; and (ii) new surveillance and information-sharing regimes do not undermine the independently-supervised rules and procedures which secure our shared rights to privacy, freedom, and security of the person. Intrusive surveillance tools without adequate safeguards are a recipe for disaster.

Even if such disasters appear remote or hypothetical, history teaches us that injustice and tyranny are preceded by a rising tide of intrusions on the privacy and dignity of ordinary citizens. In the meantime, even in free and democratic societies, sophisticated and readily available technologies add a whole new dimension to the state's power to subject its citizens to surveillance. In the words of U.S. Supreme Court Justice Brennan, "[t]hey make [surveillance] more penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient, and police omniscience is one of the most effective tools of tyranny."[49] The time to maintain and strengthen democratic safeguards is now, while we enjoy a strong consensus about respect for human rights and the rule of law.

People everywhere expect and deserve privacy in their online and digital activities. The protection of both public safety and fundamental rights requires careful attention to the implications of the relationship between law enforcement agencies and communications service providers. Law enforcement's power to gather information from third parties to identify individuals engaged in activities of interest to the state must be subject to timely, exacting, and independent scrutiny in the form of the appropriate combination of prior judicial authorization and/or subsequent notice, reporting, and accountability requirements.

The preceding three principles may be particularly relevant to the emerging debate about Big Data, Data Analytics, and online privacy. ***The key principles that have emerged from recent legislative controversies and related criminal cases which we will consider in this paper are that:*** *We can and must have both effective law enforcement and rigorous privacy protections. Eternal vigilance will be required to secure our fundamental rights, including the right to privacy in relation to all public spaces, including those found online and in other virtual spaces.*

Part IV – Meeting the Future Head On

Securing the Right to Privacy in Public Spaces

> … a moment's reflection will confirm that as we go about our daily business many, if not the majority, of our activities are inevitably carried out in the plain view of other persons. The prospect that the agents of the state should be free, on account of this fact alone, to make it their business to electronically track all our comings and goings is simply an unthinkable prospect in a free and open society such as ours.
>
> (*R. v. Wise*, 1992, Supreme Court of Canada Justice Gérard La Forest)

It is one thing to be *seen* in public. It is another to be *tracked* by the state. Public spaces facilitate a range of vital, everyday activities in a democratic society: transportation, recreation, shopping, socializing, and artistic performance. "They are places in which political movements … make themselves visible" and in which the individual is able to merge into the "situational landscape."[50] Similar things can be said about tracking people in open fields and woods — spaces which facilitate solitary walks, intimacy and romance, as well as group worship.[51] Warrantless surveillance that facilitates the sustained tracking or monitoring of people engaging in everyday activities in public and open spaces is, in Supreme Court Justice La Forest's words, "an unthinkable prospect in a free and open society such as ours."

Unthinkable as it may be, the prospect of close and continuous surveillance is no longer simply the stuff of science fiction. Increasingly sophisticated surveillance technologies are being deployed by the state. Miniature surveillance drones, unseen digital recognition systems, and surreptitious geolocational monitoring are readily available, making long-term surveillance relatively "easy and cheap."[52] Unfettered law enforcement access to surveillance technologies that are capable of facilitating indiscriminate monitoring risks intruding upon our right to a reasonable expectation of privacy, particularly where that monitoring may be close and continuous.[53] After all, the right to privacy is of concern, not only to accused persons, "but to the general … public who have every right to go about their law-abiding business without being the subject of random police

searches …"[54] As previously indicated, we are not faced with the unpalatable and impractical choice of trying to prohibit the state from using emerging technologies altogether, but simply of imposing legal, administrative, and technical controls to ensure that their use is appropriate and accountable.

The Supreme Court of Canada faced the issue of the right to personal privacy in public spaces in 1992, in a case concerning the warrantless and non-consensual use of an unsophisticated tracking device — a "beeper" — installed under a car by the police. In *R. v. Wise*, the Court determined that police monitoring or tracking of a person's movements on public roads intrudes on the reasonable expectation of privacy, even if that expectation is a reduced or diminished one. Since this decision, in Canada, the use of a tracking device has required a warrant.

The U.S. Supreme Court only faced this issue head on 20 years later, in 2012, in a case involving GPS (or global positioning system) tracking.[55] In *U.S. v. Jones*, the entire Court held that the government's warrantless use of a GPS tracking device violated an individual's Fourth Amendment right to be free from unreasonable searches and seizures by the state. While the Court was divided on whether the violation resulted from the government's physical intrusion on the individual's vehicle in installing the device to monitor his movements on public streets (the view of five justices), or from a violation of the individual's reasonable expectation of privacy from long-term GPS monitoring of his movements (the view of four justices), both views recognize society's privacy interests in public places as a factor in any future Fourth Amendment analyses. This is significant given future cases will likely involve new technologies like remote location tracking technologies that do not require a physical trespass for their activation.

While both Canadians and Americans can take some comfort that they have a constitutional right to a degree of privacy in public spaces, it is critical that lawmakers and the public begin to think more proactively about the relationship between emerging technologies, police practices, and our right to privacy in public. As indicated at the outset, we live in the era of explosive new technologies.

Governments now have access to technologies capable of facilitating broad programs of continuous and indiscriminate monitoring — technologies that are increasingly precise, scalable, affordable, and widely available. Unfettered use of these technologies by law enforcement and security agencies raises the spectre of a true surveillance state.

At the same time, new technologies can provide increased efficiencies for law enforcement and safety. How can democracies ensure that the public receives the benefits associated with these new technologies, while continuing to provide strong privacy protections?

The answer to this critical question lies in the key principles and lessons that have emerged during the course of our look back, from past to present. These are summarized here as follows:

In the remainder of this paper, we will consider the application of these principles to the way we supervise law enforcement's use of a number of surveillance technologies: automatic licence plate

Privacy Principles in Public Spaces

1. *Data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate social objectives, and subjected to controls over its retention, subsequent use, and disclosure.*
2. *The state should be open and accountable for its information-handling practices.*
3. *Compliance with privacy rules and restrictions should be subject to independent scrutiny.*
4. *The authority to employ intrusive surveillance powers should generally be restricted to limited classes of individuals such as police officers.*
5. *The police power to deploy any form of intrusive surveillance must be supervised under a system of prior judicial authorization.*
6. *Even where genuine emergencies make it impracticable for the police to obtain judicial authorization before they employ surveillance measures, the state must remain transparent and accountable for its use of intrusive powers through subsequent, timely, and independent scrutiny of their use.*
7. *A positive-sum approach to designing a regulatory framework governing state surveillance can avoid false dichotomies and unnecessary trade-offs, demonstrating that it is indeed possible to have both public safety and personal privacy. We can and must have both effective law enforcement and rigorous privacy protections.*
8. *Close attention must be paid to the privacy impact of new technologies, business practices, and police tactics if we are to continue to ensure strong, principle-based privacy protections.*
9. *Surveillance practices that intrude upon privacy by leveraging new technological platforms or transmission processes must be scrutinized to ensure that they are accompanied by sufficiently rigorous privacy and accountability protections.*
10. *Eternal vigilance will be required to secure our fundamental rights, including the right to personal privacy in relation to all public spaces, including those found online and in other virtual spaces.*

recognition systems, video surveillance cameras and CCTV, geolocational tracking, and drone-based surveillance. The approach outlined here builds on the constitutionally appropriate regulatory framework required to secure our right to privacy and provide for effective law enforcement. It does so by combining a *Privacy by Design* approach with a modern appreciation of our right to informational privacy.

Automatic Licence Plate Recognition Systems

Automatic Licence Plate Recognition ("ALPR") technology is used to take digital pictures of vehicle licence plates in order to recognize and record vehicle licence plate numbers. It employs optical licence plate detection software to seek out and recognize the presence of licence plates in view of an ALPR camera. Once an ALPR system recognizes the presence of a licence plate, the plate number is automatically extracted, at which point it can be recorded. ALPR systems can also leverage GPS technology to record the date and time, as well as relative location of all recorded images.

While ALPR systems generally do not film vehicle occupants — their focus is on the licence plates of vehicles — associated cameras could be configured to capture images of all drivers and passengers, as well as vehicle licence plates. ALPR systems — whether they are focused on licence plates or enhanced to create a more detailed record of a vehicle and its occupants — may be deployed openly from a stationary platform such as a pole, or mounted on a vehicle such as a marked police cruiser. Nonetheless, in many circumstances, they may operate in an opaque manner that may go unnoticed by much of the affected public.[56]

In Ontario, basic ALPR systems are currently being used for valid law enforcement purposes — in particular, those related to road safety. However, the use of enhanced ALPR systems to maintain a detailed accounting of every licensed vehicle that passes along a stretch of road, clears a check-point or enters into a park, town or city, 24 hours a day, seven days a week, would obviously have grave implications for privacy. So too could their use to track and monitor the comings and goings of political activists or anyone on a vaguely-defined "person of interest" watch list. Such surveillance could intrude upon a reasonable expectation of privacy — even if it were not conducted surreptitiously.

At the same time, a proactive, positive-sum approach allows for the accountable, limited, and justifiable deployment of an ALPR system. In taking this approach, we can avoid unnecessary trade-offs and demonstrate that it is indeed possible to have both public safety and personal privacy on public roads.

In this context, it is significant to note that driving is a regulated activity and some surveillance and supervision of vehicles and their drivers is expected. Surveillance of drivers, however, must be reasonable. As discussed above, Canadians have a legally-recognized "privacy interest in automobile travel" and the use of surveillance technologies in public spaces may violate section 8 of the *Charter*.[57] In this regard, police roadside and highway operations may interfere with

the "fundamental right to move about in the community."[58] As such, they must be designed and operated in a manner consistent with legislation, the common law, and the *Charter*.

Even if ALPR surveillance only results in roadside stops in a small percentage of cases, the system effects a digital identity check of drivers and their vehicles, typically for the purpose of identifying whom to stop or subject to further surveillance. *FIPPA*, which sets out rules governing the collection, use, and disclosure of *personal information* by government institutions in Ontario, permits the police to collect personal information where it is to be "used for the purposes of law enforcement."[59] Section 2 of *FIPPA* defines *personal information* as "recorded information about an identifiable individual" and "law enforcement" to include "policing."[60] Consistent with the overarching legal framework, our office has determined that the words *used for the purposes of law enforcement* require a policing institution to demonstrate that a collection of *personal information* is to be used by police acting within the scope of their law enforcement powers.[61] And, as indicated, in Ontario, ALPR systems are currently being used for valid law enforcement purposes.

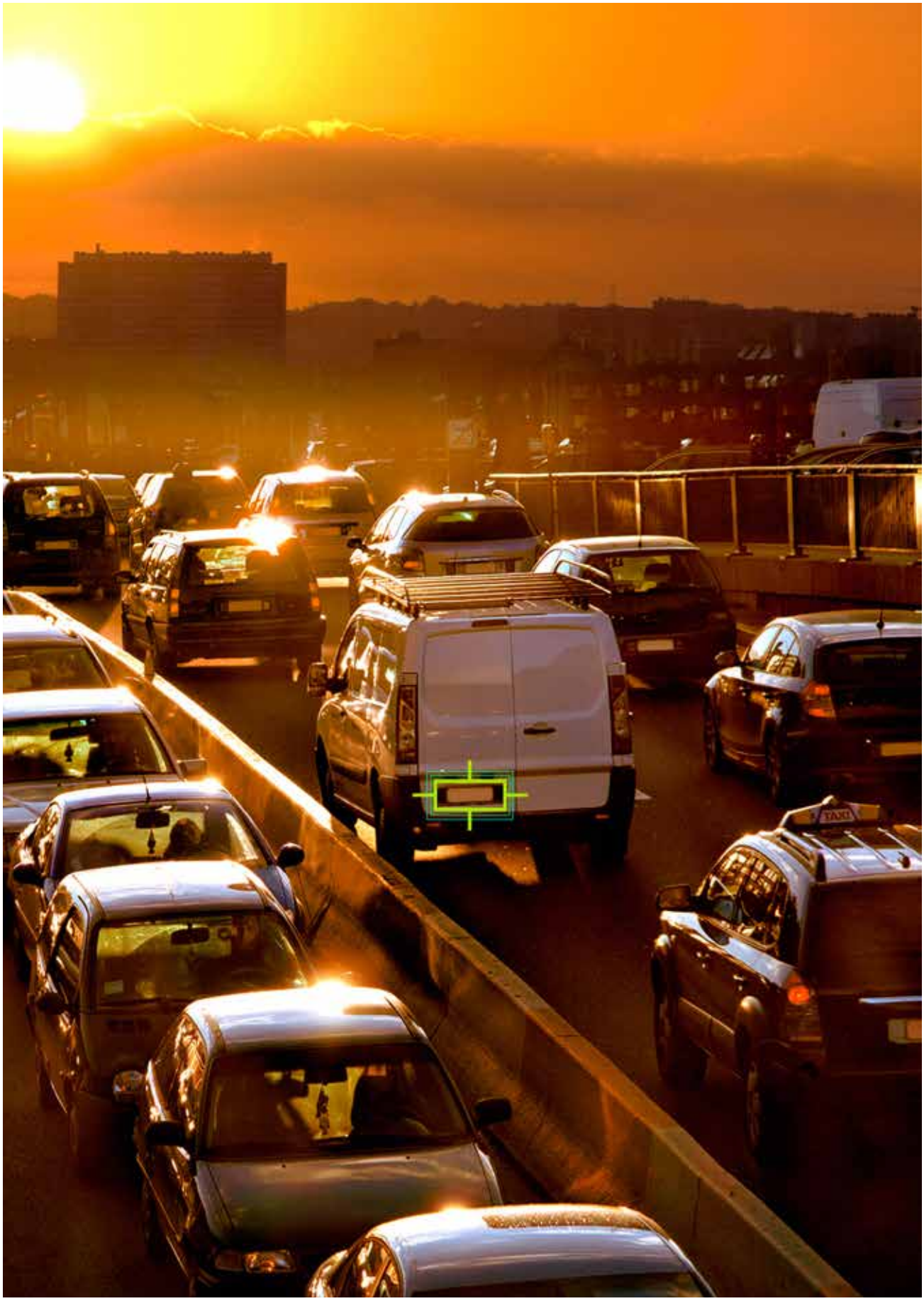
In this context, we note that, in considering the scope of law enforcement powers at the roadside and in highway operations, the Courts have consistently determined that the powers granted to the police for the purpose of enforcing the highway traffic laws, while significant, are nonetheless limited. For example, in 1992, the Supreme Court of Canada held that:

> [Highway safety] programs are justified as a means aimed at reducing the terrible toll of death and injury so often occasioned by impaired drivers or by dangerous vehicles. The primary aim of the [roadside stop] program is thus to check for sobriety, licences, ownership, insurance and the mechanical fitness of cars. The police use of check stops should not be extended beyond those aims. Random stop programs must not be turned into a means of conducting either an unfounded general inquisition or an unreasonable search.[62]

While a legitimate police interest beyond highway safety concerns need not taint the lawfulness of an otherwise valid exercise of a police power, road and highway safety concerns do "not provide the police with a means to pursue objects which are themselves an abuse of the police power or otherwise improper."[63] In this context, the Supreme Court of Canada has observed that a random stop program "designed as a 'comprehensive check for criminal activity' … was … fatally flawed from the outset."[64]

To date, ALPR surveillance systems have been used by Canadian police for purposes such as recovering stolen vehicles and licence plates, enforcing rules prohibiting driving under a suspended licence, and identifying "persons of interest" to law enforcement. Licence plate information collected by police-operated ALPR systems is recorded and compared against other information retained in police databases.

Concerned Privacy Commissioners have conducted investigations and reviews and engaged in consultations with police about their use of ALPR systems. To their credit, the police have responded by indicating their commitment to comply with Commissioner recommendations. As a result, we understand that ALPR systems are now generally only being used by police to vet vehicles against defined and appropriate *hit-lists* without retaining any data on law-abiding, *non-hit* vehicles or their occupants.


TAXI

Getting to this point has taken a positive, collaborative, but vigilant approach. Over the course of the last 10 years, the Privacy Commissioner of Canada, as well as the Information and Privacy Commissioners of British Columbia and Ontario have cautioned that, without significant controls, ALPR systems are capable of subjecting law-abiding Canadians to excessive and improper surveillance.

Beginning in 2003, our office accepted the use of mobile ALPR systems for valid law enforcement purposes (such as the location and retrieval of stolen vehicles), but cautioned against their use to continuously track and record the movements of law abiding citizens. In the intervening years, we have worked with the Ontario Provincial Police (OPP) to ensure that the personal information of law-abiding drivers — *non-hit* data — is deleted immediately after the ALPR system determines that there is no match with data on a properly-controlled highway safety-related *hit-list*. Similarly, the Privacy Commissioner of Canada has vigorously engaged the Royal Canadian Mounted Police (RCMP) over their retention of *non-hit* information, describing their initial practices as "ubiquitous surveillance of law-abiding Canadians who had committed no infraction." In 2012, she reported that "the RCMP agreed to stop retaining the *no-hit* information for the present."[65]

At the end of 2012, the Information and Privacy Commissioner of British Columbia wisely determined that "collecting personal information for law enforcement purposes does not extend to retaining information on the suspicionless activities of citizens, just in case it may be useful in the future."[66] In addition to recommending that police delete *non-hit* data immediately after the system determines that it is not a match to licence plates linked to an RCMP alert list, she recommended that the police limit their collection to reducing auto theft and motor vehicle violations. She also recommended that the municipal police work with the RCMP to amend their alert list to restrict it to addressing unlicensed drivers, driver-related court orders, and stolen vehicles.[67]

Bearing in mind the restrictions and recommendations described above, and applying our principled framework to law enforcement's use of ALPR systems, leads us to the following conclusions about the deployment of ALPR systems.

ALPR surveillance practices that intrude on privacy by leveraging new technologies must come with rigorous privacy and accountability protections. With those privacy requirements built into the technological, administrative, and legal controls, the public can be satisfied that the fair and efficient enforcement of highway safety is accomplished in a positive-sum manner.

In this regard, the deployment of ALPR systems should be restricted to circumstances where its use is necessary to meet legitimate social objectives, such as the identification of stolen vehicles or suspended drivers on a properly controlled *hit-list*. The resulting data collection should be subject to strict controls to limit the retention and subsequent use and disclosure of any personal information of law-abiding Canadians. *Non-hit* data should be deleted and destroyed immediately after the system has determined that it does not match the data on the *hit-list*.

Recalling that ALPR systems may operate in a manner that may frequently go unnoticed by much of the affected public, police services should provide the public with annual reports on their use of ALPR surveillance. In order to ensure that law enforcement remains transparent and accountable for its use of ALPR systems, such reports could, for example, provide:

- A detailed description of the times and locations at which ALPR surveillance is used;
- The purposes for which it is used;
- Whether it is deployed in a covert, overt, or opaque manner;
- How the applicable highway safety-related *hit-lists* are defined;
- How many *hits* are recorded; and
- The number of *non-hits* that are observed.

Each report could also:

- Include a declaration confirming that all *non-hits* were purged, deleted, or destroyed immediately after the system determined that they did not match data on the applicable *hit-list*(*s*) and that they were purged, deleted, or destroyed in such a manner that the *non-hit* data cannot be reconstructed;
- Indicate how many ALPR deployments have occurred that, for operational reasons associated with the need to protect the integrity of ongoing police investigations, cannot be described in detail in the report; and
- In the event that any *non-hit* data has been preserved, list the number of instances where such data has been retained, and the length, purpose, and justification for its retention.

Finally, we must not lose sight of the issue of ALPR systems being used surreptitiously or covertly. In our view, the authority to employ a covert ALPR surveillance system should be restricted to the police. In addition, the police power to deploy ALPR surveillance surreptitiously or for purposes other than those related to highway safety — such as to monitor the comings and goings of a suspect or person of interest — should be carefully supervised under a system of prior judicial authorization. Even where a genuine emergency makes it impracticable for the police to obtain judicial authorization before they employ such surveillance, the state can and must remain transparent and accountable for its use of such powers through subsequent timely, exacting, and independent scrutiny of their use — facilitated, for example, by notification and reporting requirements.

Video Surveillance and CCTV Cameras

Historically, pervasive video surveillance has posed a threat to privacy and our constitutional rights. When controlled by government departments, video surveillance can provide the government with massive amounts of personal information about the activities of law-abiding citizens, simply going about their daily lives. When individuals know they are being watched, this may have a chilling effect on their freedom to speak, act, and associate with others. Since individuals may censor their own activities when they are aware of being watched, video surveillance may also be perceived as a means of enforcing social conformity.

Privacy and the right of individuals to go about their daily activities in an anonymous fashion not only protects freedom of expression and association, but also protects individuals from intrusions into their daily lives by the government. Accordingly, when government organizations wish to use surveillance technology in a manner that will impact the privacy of all citizens, there must be clear justification for doing so. Specifically, the benefits of the technology should justify any invasion of privacy.[68]

The appropriate deployment of video surveillance can also provide significant benefits. In the aftermath of the April 2013 acts of terrorism in Boston and the alleged terrorist plot to bomb a VIA Rail passenger train travelling between Toronto and New York, it is not surprising that many have urged the deployment of increased video surveillance, including in public spaces, with CCTV cameras controlled by the police. As stated at the outset, however, the need for security must not come at the expense of privacy. Instead, we must consider achieving both goals — privacy **and** security.

With respect to surreptitious video surveillance, recall that, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally

requires prior judicial authorization wherever its use would intrude upon a person's reasonable expectation of privacy.

As Justice La Forest observed in an opinion he provided to the Privacy Commissioner of Canada regarding public space video surveillance in 2002:

> [S]ome may be tempted to conclude that there can be no reasonable expectation of privacy in what is by definition public space.
>
> Such a conclusion, however, would be far too facile. Section 8 protects personal privacy in a host of situations. It does not demarcate rigid, formalistic borders between private and public spatial domains. As I stated for the Court in *R. v. Dyment*, "the spirit of s. 8 must not be constrained by narrow legalistic classifications." Determining whether individuals have a reasonable expectation of privacy in a given context is a nuanced, contextual, and fundamentally normative enterprise. As Justice Dickson held in *Hunter*, in each case "an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement." This assessment must be made in the light of all the circumstances.[69]

Decisions dealing with public space video surveillance illustrate that we have a reasonable expectation of privacy in the confines of a public washroom cubicle. As one Ontario Court judge expressed it in 1995, "it would be difficult ... to find many 'public' places where there is more 'reason' for an 'expectation of privacy' than in the closed cubicle of a public washroom."[70]

A 2010 decision of the British Columbia Supreme Court dealing with the criminal prohibition against making a voyeuristic visual recording of a person in circumstances that give rise to a reasonable expectation of privacy indicates that we "maintain a reasonable expectation of some privacy" in public settings such as a park:

> One can conceive of many examples where a person, sitting in a park, has his or her privacy interests interfered with. A person, sitting on a park bench, who reads or writes in her diary does not reasonably anticipate that someone may, with a telephoto lens, be reading that diary. A person sitting on a park bench with a friend does not expect that their conversation may be overheard and recorded with sophisticated eavesdropping equipment. A woman who lies on a blanket in a park does not anticipate a person can, with a telephoto lens, peer up her skirt.
>
> In each of these cases, though the person in question sits or lies in a public setting, they continue to maintain a reasonable expectation of some privacy. The person's expectation is certainly lower and different than if they were in their own home, but it nevertheless exists and can be violated.[71]

In this case, the Court concluded that we have a reasonable expectation that — while we may be observed by others or incidentally captured in a third party's photograph or video — we will not be surreptitiously filmed with the zoom feature of a camera, particularly for a voyeuristic purpose. In reaching this conclusion, the Court was mindful of "the quality and nature of the information or interest at issue" and that:

> … the use of technology can transform what is reasonably expected and intended to be a private setting into something that is completely different [and that] through the use of technology [it is possible] to not only see or hear more acutely but to create a recording and to capture and preserve an image or communication.[72]

In reaching these conclusions, the British Columbia Supreme Court commented on an observation made by Justice Binnie in *R. v. Tessling*. Drawing on a number of Supreme Court of Canada decisions dealing with physical rather than technology-driven searches, in *Tessling*, Justice Binnie observed that "it is true that a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place."[73] This is a form of "risk analysis" (e.g., that when we are in public, we take the risk of being exposed). Taking note of other Supreme Court decisions dealing directly with electronic surveillance in which the Court clearly rejected the application of such a risk analysis, the British Columbia Supreme Court ruled that "the suggestion that because a person is in a location which is ostensibly public they can no longer continue to have any reasonable expectation of relative privacy is not tenable. … [T]he assessment and interpretations of privacy expectations must keep pace with technological developments. The failure to do so would lead to the inevitable erosion of [the] normative standards that are central to reasonable privacy expectations."[74]

Of course, surreptitious public space surveillance by law enforcement brings additional considerations to bear and the case law reflects this. Courts have determined, for example, that law enforcement may,

in the course of conducting an investigation, take pictures and videos of people at a shopping complex or walking from their front door to their garage from a publicly accessible adjacent roadway.[75] As Justice La Forest put it in 2002:

> We cannot reasonably expect the police to refrain from observing or overhearing persons they consider to be suspicious. To require the police to have cause or obtain authorization for such surveillance would unjustifiably limit their ability to investigate and prevent crime. Indeed, it may be permissible for the police to use a video camera to observe and record a particular suspect's movements in public spaces. For this type of targeted surveillance, the relatively minor intrusion into privacy may possibly be balanced by the state's interest in effective law enforcement.

In contrast, Justice La Forest then observed that "comprehensive and continuous video surveillance is a very different matter:"

> It permits the police to systematically observe, often at high resolution and across a broad spatial expanse, everyone present within the camera's or cameras' range. This type of video surveillance is equivalent to having individual police officers closely follow, 24 hours a day, every person within a certain geographical space. That would be a police state, not a free society. We may not have a reasonable expectation that the police will never observe our activities in public spaces, either incidentally or as part of a targeted investigation. But surely it is reasonable to expect that they will not always do so.

We agree. In our view, unfettered law enforcement use of, or access to, video surveillance technologies that are capable of facilitating indiscriminate monitoring, particularly where that monitoring may be close and continuous, is likely to intrude upon our right to a reasonable expectation of privacy, whether those technologies are employed overtly or covertly. In light of the expanding use of video surveillance technologies, not to mention the increasing sophistication of sensoring devices, biometrics, and facial recognition systems, the future of privacy may well lie in ensuring that the necessary protections are built right into the design of surveillance systems.

With respect to covert video surveillance, recall that, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally requires prior judicial authorization whenever its use would intrude on a person's reasonable expectation of privacy. How are we to ensure a constitutionally appropriate regulatory framework with respect to overt video surveillance?

Fortunately, we grappled with this issue first-hand in 2007 during our mass transit system investigation concerning the use of video surveillance cameras by the Toronto Transit Commission (TTC) in buses, streetcars, and subways, as well as on subway platforms and other transit property.[76] Our investigation report (the "*TTC Report*") brought to the fore questions about personal privacy in public spaces. In public spaces, law-abiding people may be visible and audible to others,[77] but they should reasonably expect that they will generally be able to go about their lives without being tracked and identified.

Video surveillance is often implemented in public spaces because of an expectation that it will deter crime. Aside from research suggesting that some video surveillance may deter crimes like

car theft in "hot spots," this does not appear to be supported by the research.[78] However, as was demonstrated in Boston, cameras — including privately owned and operated cameras — can serve as an effective tool in the detection, arrest, and prosecution of offenders. When an incident occurs in the presence of video surveillance cameras, the authorities can respond quickly and appropriately. In this context, the value of surveillance technologies to law enforcement appears to be clear. At the same time, given its inherently invasive nature, privacy must be considered right from the outset, wherever and whenever surveillance technologies are contemplated.

While there is "evidence to suggest that the general public recognizes that video surveillance may be justifiable in certain high risk locations,"[79] the public may be significantly less tolerant of more widespread surveillance — for example, on residential streets — or of routine, active, real-time monitoring. In addition, the public may not view a *degree* of video surveillance as unreasonable if the resulting video recordings are routinely destroyed, in a reasonably short time frame. At the same time, all legal privacy requirements must be met.

In this context, in Ontario, the state must be able to demonstrate that the collection of personal information is in accordance with the statutory privacy rules in *FIPPA* and *MFIPPA*. In general terms, the collection should be restricted to that which is reasonably necessary to meet legitimate societal objectives, and subjected to controls over retention and subsequent use and disclosure. The state should also be open and accountable for its information-handling practices.

It follows that, even where the deployment of video surveillance cameras is justified — for example, for compelling safety and security purposes, law-abiding individuals are still entitled to the privacy afforded by the ability to merge into the "situational landscape." Accordingly, necessary public spaces video surveillance must be restricted to ensure that:

- Personal information will only be collected for legitimate, limited, and specific purposes;
- The collection of personal information will be limited to the minimum amount necessary for the specified purpose(s);
- Personal information will only be used and disclosed for the purpose(s) specified; and
- Personal information will be deleted pursuant to precise and appropriately limited retention schedules and in such a manner that the personal information cannot be reconstructed.

With respect to the TTC — having found that its video surveillance program was justified — our report rejected a "privacy versus security" paradigm in favour of a positive-sum, *Privacy by Design* model. Under this model, privacy and security coexist through the use of Privacy-Enhancing Technologies (PETs) and strong procedural controls.

PETs refer to information and communications technologies that incorporate measures to protect privacy by eliminating or minimizing the collection, retention, use, and disclosure of personal information. This is often referred to as "data minimization," and increasingly represents a vital component of privacy protection. An example of a PET described in the *TTC Report* is object-based encryption that can be used to obscure the images of individuals captured by video surveillance. Where an incident takes place requiring further investigation, the images may be decrypted, but only by authorized parties. When deployed successfully, this technology reduces the risk of

random, invasive, and unlawful surveillance of individuals, while permitting the use of images for legitimate safety and security purposes — a doubly-enabling, positive-sum solution.

Beyond the effective implementation of PETs, *Privacy by Design* calls for privacy to be built proactively into an organization's information practices, by default. In the *TTC Report*, we recommended that, among other things, the TTC:

- Install accessible signage providing clear notice of collection to all passengers;
- Require all employees accessing or using the video surveillance system to sign a written agreement with the TTC regarding their duties and obligations in respect of video surveillance, including a strong undertaking of confidentiality;
- Retain *used* surveillance images (i.e., those viewed for incident-driven, law enforcement purposes) for a maximum of one year;
- Only retain *unused* images for a maximum of 72 hours (with surface vehicles — buses, streetcars — overwriting unused footage every 15 hours);
- Keep abreast of research on emerging PETs and adopt these technologies, whenever possible;
- Implement a two-signature sign-off protocol for police requests for incident-driven remote access to images recorded by the TTC surveillance system, with the Police Chief or his designate being the second sign-off; and
- Undertake comprehensive privacy audits on an annual basis.

Consistent with the TTC's policy of limiting law enforcement access to recorded images to the investigation of specific incidents, the two-signature sign-off protocol is critical to ensuring that privacy is strongly protected when providing the police with remote access to captured information for law enforcement purposes. The TTC provided a copy of a Memorandum of Understanding between the TTC and the Toronto Police Services Board (TPSB) addressing the police's remote access to and use of recorded images from TTC surveillance cameras. Incident-driven remote access would take place from a computer, located within police headquarters, connected to the TTC's surveillance system through a fibre-optic cable. To ensure proper oversight of remote access, the TTC and TPSB agreed on a double sign-off request protocol. This protocol requires that any requests from the police to the TTC for access to images captured by video surveillance be signed off both by the police officer requesting access, and by the Chief of Police, or his or her designate. This additional protection against any unauthorized access to and use of surveillance images is an excellent example of *Privacy by Design* in action, and has been working very effectively since being put into place.

The recommendations in the *TTC Report*, as well as in our *Guidelines for the Use of Video Surveillance Cameras in Public Places* (the *Guidelines*), still resonate today.[80] Once an appropriate decision has been made to deploy an overt video surveillance system, a *Privacy by Design* approach will ensure that surveillance is implemented in a privacy-protective manner that meets multiple legitimate needs — a positive-sum approach.

The application of *Privacy by Design* to surveillance technologies is not confined to video surveillance in mass transit systems. *Privacy by Design* principles may be applied to virtually any surveillance technology in a positive-sum manner, to achieve both the protection of privacy and the security of the public. We know that video surveillance technologies present a particular challenge for privacy due to their extraordinary potential for data capture and retention. Recent events serve to remind us that there are legitimate uses for some degree of surveillance in high-risk locations. The challenge is to rein in, as tightly as possible, any potential surveillance-driven erosion of privacy. We can do this by ensuring that strong controls are in place, through the implementation of appropriate legal rules and administrative policies and procedures, the use of independent audits and other measures to ensure strong oversight and accountability, and the continued development and implementation of innovative PETs to preserve privacy, while effectively providing security in public spaces.

Geolocational Tracking

Every day, millions of people move about while making use of location-enabled portable computing devices and services. Many of us are inseparable from our cellphones, smartphones, and other mobile devices and enjoy their associated location-related functionalities. More and more of our cars and trucks feature GPS-assisted mapping and roadside assistance services. However, these enormously useful tools come with a downside — they allow our movements and activities to be tracked. Indeed, this surreptitious technology is sophisticated enough in its current form to be configured to "track our every movement for indefinite periods … without visual surveillance."[81]

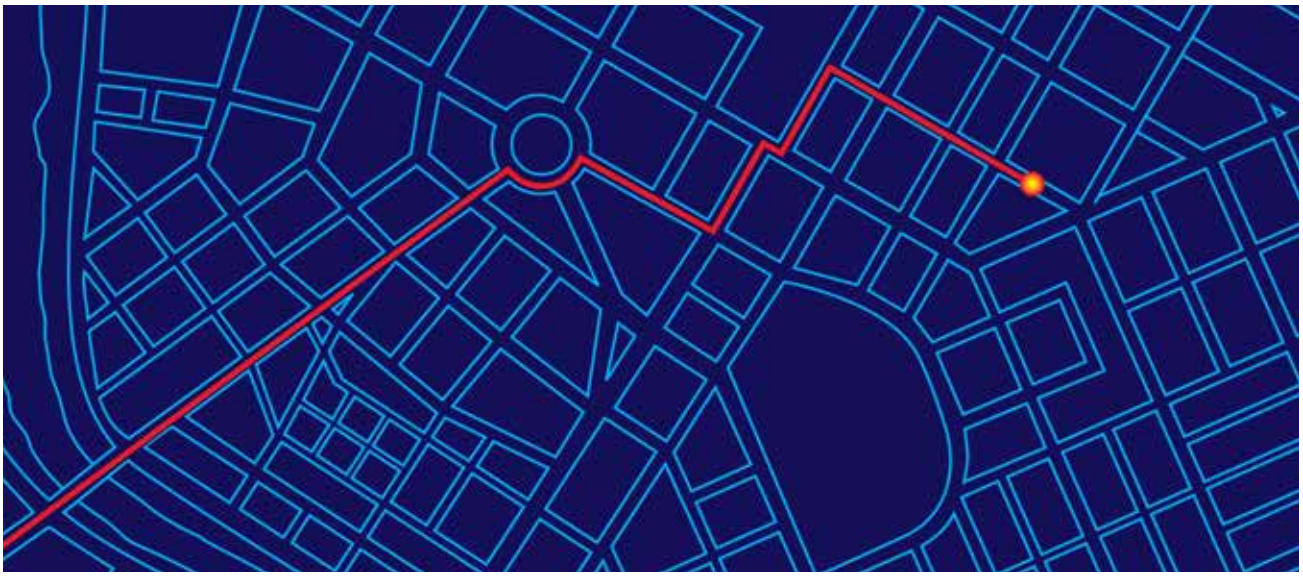
Geolocational monitoring by the state may sometimes involve a police officer having to physically install a GPS tracking device on, for example, a person's vehicle. Alternatively, this functionality can be activated remotely — for example, on a GPS-enabled device already in the possession of a person of interest. Such remote activation may require the cooperation of a third party such as a communications service provider. Geolocational tracking may also be effected by the police deploying a "stingray" (or "IMSI catcher") to trick nearby mobile phones and other wireless communications devices into connecting to the surveillance device rather than a legitimate communications tower. When devices unwittingly connect to the police, the stingray can see and record their unique device ID numbers and traffic data, as well as information that points to their precise location.

Close attention to the technical capacities and potential uses and abuses of this technology tells us that such monitoring is a form of intrusive surveillance that should generally require supervision under a system of prior judicial authorization. After all, geolocational tracking allows for close and continuous surveillance. The privacy implications of GPS-facilitated locational monitoring were described by U.S. Supreme Court Justices Sotomayor and Alito in *U.S. v. Jones*. Justice Sotomayor focused on the wealth of information collected through even short-term use of this powerful tracking technology:

> GPS monitoring generates a precise comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations … "Disclosed in GPS data … will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrists, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and so on." The Government can store such records and efficiently mine them for information for years into the future. … And because GPS monitoring is cheap in comparison to conventional surveillance techniques and by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility."[82]

Justice Alito expanded on the implications for future police practices, pointing to the possibility of more frequent resort to the use of such sophisticated and intrusive GPS surveillance in a wider array of investigations:

> The surveillance at issue in this case — constant monitoring of the location of a vehicle for four weeks — would have required a large team of agents, multiple vehicles, and perhaps aerial



> assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.[83]

In view of the facts of the case before it, however, and out of respect for the limited role assigned to the judiciary in a democracy, the majority of the U.S. Supreme Court was only prepared to declare that the Fourth Amendment requires a probable cause warrant where police installation of a GPS tracking device involves a trespass on a suspect's property. Other "vexing problems," the majority said, should be left to be resolved as future cases required.[84] At the same time, the Court appeared to appreciate that the regulation of this form of surveillance may properly move elected officials to enact a constitutionally appropriate regulatory framework.[85] Such legislative protections may be necessary to ensure the protection of privacy and freedom. As Justice Sotomayor expressed it, "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse [and] may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[86]

As indicated above, the use of a tracking device has long required a warrant in Canada. To obtain permission to install, maintain, and use a tracking device on anything, including a thing carried, used, or worn by a person, the police must first satisfy a justice of the peace or judge that there are reasonable grounds to *suspect* an offence has been or will be committed and the tracking device will provide relevant information about that offence. The terms of the relevant *Criminal Code* provision, section 492.1, would appear to capture GPS or any other electronic monitoring of the location of a person's mobile device or vehicle, whether that monitoring is activated remotely or first requires that the authorities gain physical access to a person's cellphone or car. However, in addition to incorporating a lower suspicion-based rather than belief-based threshold, the warrant regime does not require notice to individuals that they have been subject to tracking, or reports to Parliament on how frequently and in what circumstances such tracking is conducted. The same shortcomings apply with respect to section 487.11, the *Criminal Code* provision for warrantless use of a tracking device in exigent circumstances — it too lacks notice and reporting safeguards.

We believe that a positive-sum regulatory framework governing electronic locational surveillance must allow for some necessary electronic locational surveillance, while securing our right to privacy. It must ensure that a warrant is generally required, irrespective of how that surveillance is activated (e.g., *via* a trespass or remotely) or whether, in any particular case, it is used for brief periods or in a prolonged or continuous sweep. In addition, it must also provide for much greater transparency and accountability. In other words, it must also provide for appropriate post-use notice to those targeted for tracking. As the Supreme Court of Canada recognized in *R. v. Tse*, such privacy protections would not impact the ability of the police to investigate offences or "act in emergencies." It would, however, "enhance the ability of targeted individuals to identify and challenge invasions to their privacy and seek meaningful remedies."[87]

In view of the foregoing, legislative changes appear to be required in Canada (as well as in the U.S.) to ensure proper supervision and accountability in the use of this sophisticated form of surveillance technology. Recalling the principles that guide our review of law enforcement uses of new surveillance technologies, it is our view that, in addition to the existing warrant requirement, the authority to employ geolocational tracking should generally be restricted to limited classes of state actors such as police officers. Moreover, in order to ensure that law enforcement remains transparent and accountable for its use, police services should, as a matter of routine, provide the public with periodic reports on their use of geolocational tracking. Finally, and, as indicated, the authorities should provide appropriate notice to those targeted for geolocational tracking.

DRONES: Drone-based Surveillance

The word "surveillance" comes from the French word for "watching over." "Sur" means "from above" and "veiller" means "to watch." In this context, it is easy to appreciate that drone technology represents the "cold technological embodiment of observation."[88]

Drones, also referred to as remotely piloted aircraft (RPAs) and unmanned aerial vehicles (UAVs), present unique privacy challenges, due to their ability to carry a variety of sensors and to gather information from virtually any vantage point — often for long periods, and on a continuous and covert basis. Regarded as effective, low-cost alternatives to manned aircraft, drones can also sustain a greater amount of G-force, allowing for more complex flight manoeuvring. Indeed, improvements in navigation and sensor technology have made drones more reliable in terms of flight control, while advanced telecommunications technologies permit control at high altitudes, over considerable distances.[89]

Drones have attracted enormous controversy for their deadly use by the Central Intelligence Agency and the U.S. military in Pakistan, Afghanistan, and other countries. Meanwhile, in February 2013, U.S. President Barack Obama signed the *FAA Modernization and Reform Act* into law. The *Act* explicitly allows the Federal Aviation Administration (FAA) to permit the domestic use of unarmed drones, but fails to address the privacy of Americans. Transport Canada has been issuing Special Flight Operation Certificates allowing the use of drones in Canada since 2007.

Of course, drones may be deployed in a myriad of contexts, for a wide range of purposes. And, like so many technologies, drone-based surveillance can be properly deployed to provide enormous benefits. Drones may assist with fighting fires and protecting remote critical infrastructure like hydroelectric lines and oil and gas pipelines. They may also be used by law enforcement agencies in search and rescue operations, at hostage-taking incidents and other emergencies, and to document crime scenes and accidents. But drones may also be used to record people's lawful participation in events such as political protests, as well as to conduct sustained, intrusive, and surreptitious surveillance of persons of interest.

Indeed, in the hands of law enforcement, drones may be equipped with sophisticated zoom cameras, infrared thermal imagers, radar, location-based tracking tools, communication interception and listening devices, and other surveillance technologies that can record and transmit digital data to ground control systems. These technologies have become cheaper and more sophisticated, allowing data capture at greater distances, with greater resolution and granularity. Advanced video analytics can apply artificial intelligence to collecting and processing considerable amounts of video data. When combined with facial recognition software, this could be used to continuously track individuals in public, as well as in private spaces (e.g., through windows or perhaps even walls). Moreover, since they can provide effective aerial surveillance at a fraction of the cost of manned vehicles such as helicopters, it follows that drones could also facilitate a substantial increase in intrusive surveillance.

Meanwhile, the use of drones is expected to rise. In the U.S., the FAA has issued 1,428 licences to police, universities, and federal agencies between 2007 and the beginning of 2013. Of these, 327 were still listed as active in February 2013.[90] The FAA has estimated that as many as 30,000 drones could be in use domestically in the U.S. by 2020, spurred on by the Department of Homeland

Security and other government agencies. That estimate includes commercial and government drones, but not private drone hobbyists or the peeping Toms already popping up in media reports. For example, on May 29th, 2013, it was reported that, earlier that month, a Seattle woman looked out of her upper-floor window to find an aerial drone hovering outside! "On the sidewalk next to her house ... she found the man operating the drone [who] claimed that he was doing research and that what he was doing was 'perfectly legal.'"[91] Whatever the purported justification for this kind of intrusive activity, it should not go unregulated because it was on public property. Whether acting on their own behalf, or on behalf of the state, citizens' privacy must be protected.

In addition, the FAA recently announced that it has "achieved the first milestone included in the 2012 FAA reauthorization — streamlining the process for public agencies to safely fly [drones] in the nation's airspace," by: (i) developing "an automated, web-based process to streamline" the authorization process; (ii) creating "expedited procedures ... to grant one-time [authorizations] for time-sensitive emergency missions such as disaster relief and humanitarian efforts;" and (iii) "[c] hanging the length of authorization[s] from the current 12-month period to 24 months."[92]

The FAA is now working to select six drone test sites. Drone testing, however, will be focused on ensuring that drones do not "collide with planes or endanger people or property on the ground." And, while the FAA has announced a public consultation directed at protecting privacy interests associated with test site operations, the chief of the FAA's Unmanned Aircraft Systems Integration Office has acknowledged that "the FAA has no authority to make rules or enforce any rules relative to privacy."[93] That responsibility appears to lie primarily with Legislators and the Courts.

Between January 2007 and January 2012, Transport Canada issued 293 Special Flight Operation Certificates for drone operations. These certificates do not address privacy. The "ultimate goal" of Transport Canada's UAV program is stated as being "to 'normalize' UAV operations within civil airspace, [but] the industry technology is not mature enough, and the regulatory structure is not in place, to support routine operations."[94] In our view, the challenges are, however, not limited to

immature collision avoidance systems for drones operating beyond the visual range of their human pilots — privacy issues must also be addressed, directly and explicitly.

Legislation to provide for a constitutionally appropriate regulatory framework for the domestic use of aerial drones is moving ahead — in the U.S. Faced with mounting privacy-related concerns from American citizens, we are delighted to see lawmakers at the municipal, state, and federal levels taking a proactive, privacy-protective stance. In this context, it should come as no surprise that as of May 28th, 2013:

- Cities and towns such as Charlottesville, Virginia, St. Bonifacius, Minnesota, and Seattle, Washington have moved to restrict drone use in their communities;
- Twenty-eight state Legislators are actively considering passing drone legislation, most to require law enforcement to get a probable cause warrant before using a drone in an investigation;[95]
- Five states — Florida, Idaho, Montana, Tennessee, and Virginia — have already enacted laws restricting the use of drones by either imposing warrant requirements or moratoriums;[96]
- The Department of Homeland Security has set up a working group to study the impact of government UAVs on civil liberties and civil rights, as well as other legal and policy issues; and
- A comprehensive bipartisan drone bill was introduced before the U.S. House of Representatives in February by Ted Poe (R-Texas), Trey Gowdy (R-S.C.), and Zoe Lofgren (D-Calif.). Since referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, H.R. 637, the *Preserving American Privacy Act of 2013* (*PAPA*), would significantly restrict the use of drones. Like similar bills from the last session of Congress (where it was first introduced),[97] under *PAPA*, court authorization would be required for government and law enforcement drone-based surveillance, with exceptions for exigent circumstances, consent-based surveillance, and surveillance for the purpose of U.S. border control. *PAPA* would also prohibit the arming of drones and make the intentional *private* use of drone surveillance *unlawful* if it invades an individual's reasonable expectation of privacy in a "highly offensive" manner, regardless of whether there is any trespass.[98]

In contrast, it appears that, for the time being, Canadians may have to rely on the prudence of law enforcement and the oversight provided by Privacy Commissioners and the Courts. Canadian Legislators have yet to grapple *directly* with the emerging privacy issues associated with drone use. The reason may be that, thus far, the public perceives drones to be a largely American phenomenon. However, while they may not yet be in widespread use by police in Canada, the RCMP have a fleet of approximately 20 drones. Meanwhile, in Ontario, the OPP and the Halton Police Service are actively using drones. In addition to using them for purposes related to search and rescue operations, hostage-taking incidents, and other emergencies, as well as the documentation of crime scenes and accidents, the police appear to have used drones to investigate drug offences.[99]

In this context, it is time for a proactive public discussion of the issues. The key is to ensure that we receive the benefits associated with drone-based technologies, while continuing to provide strong

privacy protections, *including* in public spaces. Once more, we turn to the principles and lessons that emerged during the course of our retrospective. They will instruct us as to how to ensure a constitutionally appropriate regulatory framework with respect to drone-based surveillance.

And, once again, we recall that, in Canada, the police use of any device or investigative technique, including a television camera or similar electronic device, generally requires prior judicial authorization wherever its use would intrude on a person's reasonable expectation of privacy. Moreover, recalling our discussion of ground-based video surveillance, we join with our Canadian Courts in asserting that Canadians "maintain a reasonable expectation of some privacy" on public roads and other public settings such as parks, public squares, plazas, and playgrounds.

This conclusion is consistent with the weight of the case law dealing with manned aerial video surveillance by the police over occupied and unoccupied private land, as well as over Native reserves. As affirmed by Courts in New Brunswick,[100] Ontario,[101] Saskatchewan,[102] and British Columbia,[103] "an expectation of privacy, which society is prepared to recognize is reasonable, can exist in respect of unoccupied lands," as well as occupied lands, particularly with respect to individuals entitled to be present on those lands. This body of law tells us that even low-tech manned aerial surveillance of open private spaces generally requires a warrant, especially when that surveillance is conducted at low altitudes.[104]

In one of the two cases where a Provincial Court would have permitted warrantless aerial video surveillance of open spaces, the Supreme Court of Canada effectively set that finding aside, explicitly leaving the critical issue of the constitutionality of "open-space searches" to a more appropriate future case.[105] In the remaining case, the Court determined that the police may conduct some aerial surveillance from an airplane flying over adjacent private land at an altitude in excess of the minimum altitude for permissible aircraft flyovers (over 500 feet for rural areas, over 1,000 feet for built-up areas), where they used a commonly available zoom lens camera.[106]

In our view, an analysis that places too much emphasis on the altitude, angle, or availability of surveillance tools and tactics must be rejected. The key question is whether the surveillance provides a *close or penetrating gaze*. In this regard, we join with Justice Drapeau, writing for the Court of Appeal of New Brunswick, where he states that:

> For my part, I reject the suggestion that the application of s. 8 to [open spaces in an occupied residential lot] is contingent on the presence of view-proof walls or roofs. Such an approach would deny s. 8 rights to most open spaces in residential properties, and it would limit s. 8 rights to the few who can afford such privacy shields. As a rule, lawful occupants have an expectation of privacy in all open spaces within their residential lots that is qualitatively sufficient to invest them with s. 8 protection against unlawful aerial as well as terrestrial searches.[107]

As the Saskatchewan Court of Queen's Bench said in 2008, "there has been no determination by the Supreme Court of Canada regarding the right to privacy on open, privately owned land."[108] That remains the case to date. What of the Supreme Court of Canada's 2004 ruling in *R. v. Tessling*? In that decision, the Court determined that police did not need a warrant to conduct surveillance of the patterns of heat distribution on the external surfaces of a private residence from an airplane using an unsophisticated infrared radar camera (FLIR). In reaching this conclusion, the Court's focus

was squarely on "the quality of information that [*existing*] FLIR imaging can actually deliver."[109] The Court was careful to remind us that:

> If, as expected, the capability of FLIR *and other technologies* will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist.[110]

While the intrusiveness of a drone operation will depend on its surveillance 'payload,' as well as the circumstances, manner, and length of its deployment, it is self-evident that drone-facilitated surveillance has the capacity to facilitate close, continuous, and indiscriminate monitoring.

Bearing in mind our 2012 paper, *Privacy and Drones*, as well as the approach emerging out of U.S. Legislatures, we make the following further recommendations about the constitutionally appropriate governance of the state's use of drone-based surveillance.

As indicated throughout this paper, data-gathering by the state should be restricted to that which is reasonably necessary to meet legitimate social objectives, and subjected to controls over its retention and subsequent use and disclosure. The state should be open and accountable for its information-handling practices. Compliance with these rules and restrictions should be subject to independent scrutiny. In particular, we recommend that the authority to employ intrusive drone-based surveillance powers should generally be restricted to limited classes of state actors such as police officers. Barring any genuine urgencies, the police should secure a warrant before conducting any sophisticated drone-facilitated surveillance that targets one or more individuals, including people participating in political activities including speeches, demonstrations, picket lines or other forms of non-violent protests. The police should also be required to provide appropriate post-use notice to those targeted for any drone surveillance.

At the same time, not all drone-facilitated police surveillance will be intrusive of privacy interests. Like geological inspections or environmental surveys, police surveillance of a remote piece of

energy infrastructure will rarely intrude upon the privacy of any member of the general public. In such circumstances, a warrant may not be necessary. Of course, any personal information collected by law enforcement through such uses of drones will generally be governed by applicable privacy legislation and should not be used for secondary law enforcement purposes.[111]

Other law enforcement uses of drone-based surveillance in search and rescue operations, at hostage-taking incidents, and to document crime and accident scenes also call for a different approach. Drone use in geographically-confined, time-limited, emergency situations of these kinds may not require a warrant. However, to ensure that the state remains transparent and accountable, all drone use should be subject to additional restrictions, as well as subsequent, timely, and public scrutiny. In particular, the decision to deploy a drone should be made by a senior officer. In all cases, images of identifiable individuals captured by drone-based surveillance technologies should not be retained longer than one year following their collection — or shared with third parties at all — unless there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.

Moreover, clear written policies and procedures governing the use of aerial surveillance technologies should be adopted and made available to the public. To help ensure necessary transparency and accountability, law enforcement agencies should also be required to issue annual public reports on their use of drones. This will help both lawmakers and the public understand how drones work in practice. Such reports could, for example, indicate:

- The purpose for which drones have been used and the circumstances under which their use has been authorized, and by whom (i.e., a Court or a senior officer);
- The specific kinds of information that the drone(s) have collected about individuals;
- The length of time for which the information will be retained;
- The possible impact on individuals' fundamental rights including the right to privacy;
- The specific steps the police service takes to mitigate the impact on individuals' privacy, including protections against unauthorized use and disclosure; and
- An individual point of contact for citizen complaints and concerns.

Throughout, any move to regularize drone use — for example, within a municipality — should be preceded by a full public discussion. Consultations should be conducted with all relevant stakeholders to examine the necessity of any proposed drone program and the policies required for a justified and proportionate program that is acceptable to the public.

Finally, we must make a commitment to proactively embed privacy into the design of these new technologies. By adopting a *Privacy by Design* framework, we can limit the negative impacts that may otherwise be produced. The prospect of having our every move monitored, and possibly recorded, raises profound privacy and civil liberty concerns. We must avoid, as many privacy scholars and regulators have cautioned, "sleepwalking into a surveillance society."[112] Instead, we encourage law enforcement authorities to take a proactive *Privacy by Design* approach to developing and operating a drone program which truly respects privacy.

Privacy by Design principles should be adopted into all aspects of drone operations, particularly in any circumstances where personal information may be collected, retained, used, disclosed, and/or disposed of. Where possible, the collection of personally identifiable information should be

avoided. Drone operators should ensure that they are transparent with respect to any collection of personal information. In addition, consideration should be given to employing object-based encryption to obscure any images of individuals that are captured by drone-based surveillance. Under this approach, where an incident takes place requiring further investigation, the images may be decrypted, but only under the authority of two authorized officials. If deployed successfully, this technology could reduce the risk of random, invasive, and unlawful surveillance of individuals, while permitting the use of images for legitimate safety and security purposes. In addition, access to drone data recordings would be restricted to authorized personnel only. Logs would be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail. Where records are maintained electronically, the logs should also be electronic. Such measures would ensure that the proposed design and operation of a drone system strictly limits privacy intrusions to those which are absolutely necessary to achieve required, lawful goals.

Conclusions

In a free and open society such as ours, privacy plays a critical role. It is a constitutional right "integral to an individual's relationship with the rest of society and the state."[113] Legislatures, Courts, and Privacy Commissioners continue to provide further instruction and guidance on how to protect this fundamental right. A *Privacy by Design* approach is central to designing a regulatory framework governing state surveillance, whether we are considering the use of video surveillance, an ALPR system, geolocational tracking, drones, or any other new surveillance technology.

Now more than ever, calls for increased public surveillance must be vigorously questioned. Technologies capable of facilitating broad programs of continuous and indiscriminate monitoring must be subject to strict controls. As Justice Ian Binnie stated in 2004:

> Efforts to counteract terrorism are likely to become part of our everyday existence for perhaps generations to come. … The danger in the "war on terrorism" lies not only in the actual damage the terrorists can do to us but what we can do to our own legal and political institutions by way of shock, anger, anticipation, opportunism or overreaction.[114]

The same cautions apply in respect of any proposal to obtain "a little temporary safety" at any cost. Excessive surveillance is anathema to freedom and liberty, and must thus be opposed.

In the words of Justice Binnie's colleagues, Justice Iacobucci and Justice Arbour, however, "we must not forget that the legislative and executive branches also desire, as democratic agents of the highest rank, to seek solutions and approaches that conform to fundamental rights and freedoms."[115] Fortunately, it is our experience that, where the use of a particular surveillance technology is justified, proportional, and effective at delivering public safety **and** privacy, a proactive, *win-win*, *positive-sum* approach is available that will ensure that privacy, accountability, and transparency are embedded into the legal and technical design specifications of any proposed surveillance system.

While eternal vigilance is required to secure our fundamental rights, including the right to personal privacy, we remain confident that we can have both public safety and personal privacy in public spaces. There is neither reason, nor need, to settle for anything less.

Endnotes

1 *R. v. Wise*, [1992] 1 S.C.R. 527 at para 82.

2 Phil Mattingly, "Boston Police Chief Urges Surveillance Increase After Attack," *Bloomberg*, (9 May 2013) online: <http://www.bloomberg.com/news/2013-05-09/boston-police-chief-urges-surveillance-increase-after-attack-1-.html>.

3 Richard A. Posner, "Privacy is Overrated," *New York Daily News*, (28 May 2013) online: <http://www.nydailynews.com/opinion/privacy-overrated-article-1.1328656> . See also Commissioner Ann Cavoukian Letter to the Editor, *New York Daily Times* (1 May 2013) online: <http://www.nydailynews.com/opinion/2-school-lunch-privacy-ed-article-1.1332648?pgno=1>.

4 Benjamin Franklin, *Memoirs of the Life and Writings of Benjamin Franklin* (London: Henry Colburn, 1818) at 270.

5 Danielle Citron and David Gray, "A Technology-Centered Approach to Quantitative Privacy," (14 August 2012) at 4. See also Danielle Citron and David Gray, "The Right to Quantitative Privacy" (2013) 98 *Minnesota Law Review* at 4.

6 *Supra* note 1.

7 *R. v. Tessling,* [2004] 3 S.C.R. 432.

8 An important means of achieving proper privacy is through the *Privacy by Design* (*PbD*) approach. *PbD*'s approach is to embed privacy in the design specifications of information technologies and systems, accountable business practices, and physical design and networked infrastructures, as the default, right from the outset. *PbD* principles accommodate all legitimate interests and objectives in a positive-sum, *win-win* manner. *PbD* avoids the pretense of false dichotomies, such as privacy versus security, demonstrating that it is possible, and far more desirable, to have both. *PbD* represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches after the fact. *PbD* requires an evolution in the way that private organizations and government institutions think about privacy — moving from a reactive mode to a proactive one. Similarly, enshrining a *PbD* approach in statutes, regulations, administrative codes, and best practices may require an evolution in how policy and lawmakers approach privacy rule-making. For example, surveillance-related rule-making should ensure that surveillance is accountable, limited, and transparent.

9 FIPs refers to the *Fair Information Practice Principles*, online: < http://www.priv.gc.ca/resource/tool-outil/english/fair-info-practices.asp>.

10 *R. v. Patrick*, [2009] 1 S.C.R. 579 at para 20. See also *R. v. A.M.*, [2008] 1 S.C.R. 569 at paras 35 and 36; *R. v. Dyment*, [1988] 2 S.C.R. 417 at pp. 427-428; and *H.J. Heinz of Canada Ltd. v. Canada* (*Attorney General*), [2006] 1 S.C.R. 441 at para 22.

11 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 at para 71, per La Forest J. dissenting in the result; and *Lavigne v. Canada (Commissioner of Official Languages)*, [2002] 2 S.C.R. 773 at paras 24-25.

12 *Supra* note 5 ("A Technology-Centered Approach to Quantitative Privacy") at 17.

13 Office of the Information and Privacy Commissioner of Ontario, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report — Privacy Investigation Report MC07-68* (3 March 2008) at 2.

14 *Hunter et al. v. Southam Inc.,* [1984] 2 S.C.R. 145.

15 *R. v. Ward* 2012 ONCA 660.

16 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11. ss. 8 and 24(1).

In the majority of section 8 cases, search and seizure issues arise in the context of criminal proceedings where the primary focus is on a specific factual context of a particular police investigation, the rights of the accused, the admissibility of evidence, and the application of the section 8 and 24(1) tests. While these issues are obviously important, they are not the focus of this paper. Our focus is on ensuring the privacy rights of the public at large in the face of increasingly sophisticated surveillance technology.

17 Jed Rubenfeld, "The End of Privacy," (2008) 61:1 *Stanford Law Review* 121.

The Fourth Amendment provides that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

18 *Freedom of Information and Protection of Privacy Act* R.S.O. 1990, Chapter F.31 (*FIPPA*); *Municipal Freedom of Information and Protection of Privacy Act* R.S.O. 1990, Chapter M.56 (*MFIPPA*).

19 *Supra* note 13.

20 Massimo Calabresi and Michael Crowley, "Homeland Insecurity; Do we need to sacrifice privacy to be safer?" *Time Magazine* (13 May 2013) at 28.

21 *Constitution Act*, *1867*, 30 & 31 Vict, c.3, (U.K.) reprinted in RSC 1985, App II, No 5., s. 91.

22 *Cash Converters Canada Inc. v. Oshawa (City)* 2007 ONCA 502 at paras 30-31, quoting the *Williams Commission Report (Public Government for Private People: The Report of the Commission on Freedom of Information and Protection of Individual Privacy* (1980) 3) at 504-505, the report that led to the enactment of Ontario's public sector privacy legislation.

23 *Criminal Code*, R.S.C., 1985, c C-46.

24 At the same time, note that, for example, under s. 21(1)(c) of *FIPPA* and s. 14(1)(c) of *MFIPPA*, the privacy protective rules regulating the handling of "personal information" by Ontario public sector institutions do not apply to a narrow

class of "personal information" that is maintained "for the express purpose of creating a record available to the general public." (The fact that an individual has disclosed the information to the public, for example, via the press, does not render it public within the meaning of these provisions. See *Investigative Report I94-011P* quoted in *MO-1366 [2000] O.I.P.C. No. 203* at para 44 and *I95-24M [1996] O.I.P.C. No. 80* at para 13. Further, note that our office has determined that: "Other institutions cannot claim the benefit of the exclusion for the same personal information unless they, too, maintain the information for the purpose of making it available to the general public. In our view, this interpretation is not only reasonable, but also in keeping with one of the fundamental goals of the Act, namely 'to protect the privacy of individuals with respect to personal information about themselves held by institutions.' … Information contained in police daily arrest sheets (*Order M-849*), dockets listing daily matters being heard under the *Police Services Act* (*Order M-1053*), a list of all doctors registered with the College of Physicians and Surgeons of Ontario (*Order P-1635*) and a list of the names and addresses of all persons licensed to drive in the province of Ontario (*Order P-1144*) have all been found to not satisfy the requirements of ss. 14(1)(c) and 21(1)(c)." [*MO-1366* at para 45].

25 For example, s. 39(3) of *FIPPA* provides certain law enforcement-related exemptions from the general duty to provide all affected individuals notice of indirect collections of their personal information.

26 *Copeland and Adamson*, [1972] 3 O.R. 248 (OHCJ).

27 *R. v. Tse* 2012 SCC 16 at para 17, quoting Justice La Forest in *R. v. Duarte*, [1990] 1 S.C.R. 30.

28 *Ibid* at para 16.

29 *Supra* note 1, at para 69 (quoting the majority in *R. v. Wong*, [1990] 3 S.C.R. 36) and para 81.

30 *R. v. Wong*, [1990] 3 S.C.R. 36. See also *Supra* note 23, s. 487.01, but note *Supra* note 7 at 30.

31 *Supra* note 27, at para 28.

32 *Supra* note 27, at para 85.

33 *Supra* note 27, at para 98.

34 Bill C-55, *An Act to Amend the Criminal Code (Response to the Supreme Court of Canada Decision in R. v. Tse)*,1st Sess, 41st Parl, 2013.

35 Note that, in *R. v. Tse* (*supra* note 27) at para 57, the Supreme Court signalled that it had strong "reservations about the wide range of people who, by virtue of the broad definition of 'peace officer,' can invoke the extraordinary measures permitted under s. 184.4 [of the *Criminal Code*]."

The definition of "peace officer" includes "mayors and reeves, bailiffs engaged in the execution of civil process, guards and any other officers or permanent employees of a prison, and so on." Without ruling on the point, the Court stated that the emergency warrantless wiretap powers "may be constitutionally vulnerable" for this additional reason (see paras 55-57).

In addition, at para 89 the Supreme Court had welcomed rather than required "added safeguards, such as the preparation of reports for Parliament." The Court did observe that, as a "matter of policy, a reporting regime that keeps Parliament abreast of the situation on the ground would seem to make good sense."

36 *R. v. TELUS Communications Co.* 2013 SCC 16 at para 58.

37 *Ibid* at paras 75 and 5.

38 *Supra* note 36 at para 33.

39 *Supra* note 15.

40 *Supra* note 15 at para 75.

41 *Supra* note 15 at paras 72-74.

42 *Supra* note 15 at para 71.

43 *Supra* note 15 at paras 74, 95-109.

44 See, for example, Lukas Feiler, "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection" *European Journal of Law and Technology*, Vol 1, No 3 (2010). Online: <http://ejlt.org/article/view/29/75> and EC, *Commission Directive 2006/24/EC* of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

45 As indicated in letters from various private sector entities supporting *CISPA*, U.S. companies are already engaged in some critical infrastructure protection-related information-sharing. Online: <http://intelligence.house.gov/hr-3523-letters-support>.

46 U.S. Presidential Exec Order, "Improving Critical Security Infrastructure" (12 February 2013).

47 Chris O'Brien, "Senate Indicates it Won't Consider CISPA," *LA Times* (29 April 2013) online: <http://www.latimes.com/business/technology/la-fi-tn-senate-cispa-20130429,0,357666.story>.

48 Ann Cavoukian, "The Issue," online: RealPrivacy < http://www.realprivacy.ca/issue>.

49 Malvin Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" (1988) 39 *Syracuse Law Review* at 647. See also *United States v. White* 401 U.S. 745. And see the discussion of "Project Champion" in Pete Fussey and Jon Coaffee, "Urban spaces of surveillance," The Routledge Handbook of Surveillance Studies, edited by Kirstie Ball, David Lyon, Kevin Haggerty. Routledge: New York (2012) at 207-208.

50 Jason W. Patton, "Protecting privacy in public? Surveillance technologies and the values of public places," *Ethics and Information Technology* (2000) 2: 3 at 183; and Alan F. Westin, *Privacy and Freedom* (New York: Athenum, 1967) at 31.

51 *R. v. Poncelet,* [2008] SKQB 157 at para 27.

52 *United States v. Jones* 625 F. 3d 544 at 3.

53 *Supra* note 5 ("A Technology-Centered Approach to Quantitative Privacy").

54 *R. v. Kang-Brown*, [2008] 1 S.C.R. 456 at paras 79 and 104.

55 As discussed in *Supra* note 52, in U.S. Supreme Court cases from the 1980's, the use of a beeper was effected with the consent of the original owner of the vehicle or container being tracked. See *U. S. v. Knotts*, 460 U.S. 276 [1983] and *U. S. v. Karo*, 486 U.S. 705 [1984].

56 Office of the Information and Privacy Commissioner of British Colombia *Investigation Report F12-04: Use of Automated Licence Plate Recognition Technology by the Victoria Police Department* (15 November 2012) online: <http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF12-04.pdf>.

57 *Supra* note 1 at para 14.

58 *Brown v. Durham (Regional Municipality) Police Force*, [1998] 116 O.A.C. 126 at paras 67, 77.

59 *Supra* note 18 (*FIPPA*) at s. 38(2). See also *Supra* note 18 (*MFIPPA*) at s. 28(2).

60 *Supra* note 18 (*FIPPA*) at s. 2(1). See also *supra* note 18 (*MFIPPA*) at s. 2(1).

61 *IPC Investigation I94-048M: A Regional Police*, [1994] O.I.P.C. No. 428 at 2-3.

62 *R. v. Mellenthin*, [1992] 3 S.C.R. 615 at 624.

63 *Supra* note 58 at para 38.

64 *R. v. Ladouceur* 2002 SKCA 73 at paras 43, 54.

65 Office of the Privacy Commissioner of Canada, *2011-2012 Annual Report to Parliament on the Privacy Act: The Privacy Act 1982-2012 — Three Decades of Protecting Privacy in Canada* (October 2012), at 19 online: <http://www.priv.gc.ca/information/ar/201112/201112_pa_e.pdf>.

66 *Supra* note 56 at 3.

67 *Supra* note 56 at 6 and 28.

68 *Supra* note 13 at 2.

69 Justice Gérard La Forest, Opinion (5 April 2002) online: <http://www.priv.gc.ca/media/nr-c/opinion_020410_e.asp>.

70 *R v. Silva,* [1995] O.J. No. 3840 at para 46. See also *R. v. Baker,* [1998] B.C.J. No. 1854; but also see *R. v. LeBeau,* [1988] O.J. No. 51 where the Ontario Court of Appeal determined the accused had no reasonable expectation of privacy in the circumstances.

71 *R. v. Rudiger* 2011 BCSC 1397 at paras 91-92.

72 *Ibid* at paras 101, 93, 98.

73 *Ibid* note 71 at para 40.

74 *Ibid* note 71 at paras 113 and 117.

75 *R. v. Hounsell,* [1994] N.J. No. 319 and *R. v. Bryntwick* [2002] O.J. No. 3618.

76 *Supra* note 13.

77 *Supra* note 1.

78 *Supra* note 13 at 3-10. And see John Papazian, "The Lens of Law Enforcement: A Geospatial Statistical Program Evaluation of Denver's HALO Camera Surveillance System," 2013 *Sanford Journal of Public Policy* 4 at 109, online: <http://sites.duke.edu/sjpp/files/2013/04/Papazian-The-Lens-of-Law-Enforcement.pdf>; and Rajiv Shaha and Jeremy Braithwaite, "Spread too thin: analyzing the effectiveness of the Chicago camera network on crime," *Police Practice and Research: An International Journal* (2012) online: <http://www.tandfonline.com/doi/abs/10.1080/15614263.2012.670031#.UaYP6kA4tBl>.

79 *Supra* note 13 at 26. And see Charles Farrier, "Civil Liberties and CCTV Camera Surveillance. Landmark Court Decision in Australia," *Global Research* (9 May 2013) online: <http://www.globalresearch.ca/civil-liberties-and-cctv-camera-surveillance-landmark-court-case-in-australia/5334423>.

80 The *Guidelines* are intended to assist organizations in determining whether the collection of personal information by means of overt video surveillance is lawful and justifiable as a policy choice, and if so, how privacy-protective measures may be built into the system. Before deciding whether to use overt video surveillance, the *Guidelines* recommend that organizations consider the following:

- A video surveillance system should only be adopted after other measures to protect public safety or to deter, detect, or assist in the investigation of criminal activity have been considered and rejected as unworkable. Video surveillance should only be used where conventional means (e.g., foot patrols) for achieving the same law enforcement or public safety objectives are substantially less effective than surveillance or are not feasible, and the benefits of surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.
- The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- An assessment should be made of the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects may be mitigated.
- Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public.
- Organizations should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

Once a decision has been made to deploy overt video surveillance, the *Guidelines* set out the manner in which video surveillance cameras should be implemented in order to minimize their impact on privacy.

81 *Supra* note 1 at para 75.

82 *Supra* note 52 at 955-956.

83 *Supra* note 52 at 963-963.

84 *Supra* note 52 at 954.

85 *Supra* note 52 at 962, 964, per Alito J.; 956 per Sotomayor J.

86 *Supra* note 52 at 956.

87 *Supra* note 27 at para 98.

88 Calo, R. (2011), "The drone as privacy catalyst." 64 *Stan. L. Rev*. 29 online: <http://www.stanfordlawreview.org/online/drone-privacy-catalyst>.

89 At present, there are three main types of drones: micro and mini drones, tactical drones, and strategic drones. Micro drones, weighing as little as 100 grams (about 3.5oz), fly at low altitudes (below 300 metres, or approximately 1,000 feet). Mini drones, which weigh up to 30 kilograms (approximately 66 pounds), fly at altitudes between 150 and 300 metres (approximately 500 and 1,000 feet). Tactical and strategic drones are considerably larger and heavier (from 150 to 1,500 kilograms and up to 15,000 kilograms, or from approximately 330 to 3,300 pounds and up to 33,070 pounds, respectively) and fly at much greater altitudes (from 3,000 to 8,000 metres, or approximately 10,000 to 26,250 feet) and up to 20,000 metres (approximately 66,000 feet), respectively, and for longer periods of time (35 to 40 hours or more). Tactical and strategic drones are associated predominately with military applications.

90 See Brian Bennett and Joel Rubin, "Drones are taking to the skies in the U.S.," *LA Times* (15 February 2013) online: <http://articles.latimes.com/2013/feb/15/nation/la-na-domestic-drones-20130216>.

91 See Ben Wolfgang, "FAA chief says drones will force change at agency," *The Washington Times* (7 August 2012) online: <http://www.washingtontimes.com/news/2012/aug/7/faa-chief-says-drones-will-force-change-at-agency/>. And see Matt Hickey, "Is Seattle Being Buzzed By Drone-Equipped Peeping Toms?" *Forbes*, 29 May 2013, online: <http://www.forbes.com/sites/matthickey/2013/05/28/is-seattle-being-buzzed-by-drone-equipped-peeping-toms/>.

92 See "FAA Makes Progress with UAS Integration," Federal Aviation Administration (page last modified 14 May 2012) online: <http://www.faa.gov/news/updates/?newsId=68004>.

93 *Supra* note 91 and see "Unmanned Aircraft Systems (UAS) – Online Session on UAS Test Site Privacy Policy," Federal Aviation Administration online: <http://www.faa.gov/about/initiatives/uas/>.

94 See Alexandra Gibb, "Privacy concerns hover over RCMP drones in British Columbia," *TheThunderbird.Ca* (29 March 2012) online: <http://thethunderbird.ca/2012/03/29/privacy-concerns-hover-over-rcmp-drones-in-british-columbia/>; "Unmanned Air Vehicle (UAV)," Transport Canada online: <http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm>.

95 See Allie Bohm, "Status of Domestic Drone Legislation in the State," *American Civil Liberties Union* online: < http://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states>.

96 *Ibid*.

97 *The Preserving American Privacy Act* was first introduced by Republican Reps. Poe and Gowdy in 2012 as H.R. 6199. Like two other comparable drone bills from the last session of Congress (Sen. Rand Paul's (R-Kentucky) S.3287, *The Preserving Freedom from Unwarranted Surveillance Act of 2012*, and Rep. Ed Markey's (D-Mass) H.R. 6676, *The Drone Aircraft Privacy and Transparency Act of 2012*), H.R. 6199 died when the session concluded. All 3 bills set warrants as the general rule for most law enforcement drone-based surveillance.

98 See progress of H.R. 637 at: <http://thomas.loc.gov/cgi-bin/query/z?c113:H.R.637.IH>. And see Senator Rand Paul's comparable bill, S. 1016, *The Preserving Freedom from Unwarranted Surveillance Act of 2013*, introduced before the Senate on 22 May 2013, which aims to protect individual privacy against unwarranted governmental intrusion through the use of drones by imposing a warrant requirement with exceptions for the patrol of national borders, imminent danger to life or a high risk of a terrorist attack.

99 "Not just for modern warfare: RCMP to expand use of drone mini-helicopters," Douglas Quan, Postmedia News, 13/01/27, <http://news.nationalpost.com/2013/01/27/not-just-for-modern-warfare-rcmp-to-expand-use-of-drone-mini-helicopters/ …> "RCMP expands its drone fleet as watchdogs worry Canadians may face aerial snoops", Steve Mertl, Daily Brew, Jan. 28, 2013 <http://ca.news.yahoo.com/blogs/dailybrew/rcmp-expands-drone-fleet-watchdogs-worry-canadians-may-211447954.html ...> "Police drones sparks debate over personal privacy," Jennifer Quinn, Feb. 5, 2013, <http://www.thestar.com/news/world/2013/02/05/privacy_vs_security_when_does_the_use_of_drones_cross_the_line.print.html>.

100 *R. v Kelly,* [1995] N.B.J. No. 98 (C.A.) at 49-50.

101 *R. v. Lauda* 121 O.A.C. 365 AT 60-72, and see [1998] 2 S.C.R. 683. While *Lauda* is not an aerial surveillance case, in it, the Ontario Court of Appeal held that there may be a reasonable expectation of privacy in an open field, a finding not overturned by the Supreme Court of Canada.

102 *Supra* note 51 at paras 14-32.

103 *R. v. Douglas* 2000 BCPC 9 at paras 101-111.

104 In view of the Supreme Court of Canada's decision in *R. v. Boersma,* [1994] 2 SCR 488, a case dealing with a physical, on-the-ground search on Crown lands, it is not clear whether an individual would have a reasonable expectation of privacy with respect to drone surveillance over such lands.

105 *R. v. Patriquen,* [1994] N.S.J. No. 573 (CA), [1995] 4 S.C.R. 42 (SCC) at para 1.

106 *R. v. Kwiatkowski* 2010 BCCA 124 at paras 40-41.

107 *Supra* note 100 at para 50.

108 *Supra* note 51 at para 24.

109 *Supra* note 7, at para 28.

110 *Ibid* at para 29.

111 Note that the collection of personal information by a drone operator in the course of commercial activity is likely to be regulated under the *Personal Information Protection and Electronic Documents Act (PIPEDA)* S.C. 2000, c.5., as well as comparable legislation in British Columbia and Alberta. While the collection of personal information for personal or domestic purposes as well as for journalistic, artistic or literary purposes may not be covered by *PIPEDA*, in Ontario, any egregious, drone facilitated violation of privacy may attract civil litigation under the new tort of intrusion upon seclusion. See also *Jones v. Tsige* 2012 ONCA 32.

112 Comments of the then-UK Information Commissioner Richard Thomas, as reported in BBC News, "Britain is 'surveillance society'" (2 November 2006) online: <http://news.bbc.co.uk/2/hi/uk_news/6108496.stm>.

113 *Jones v. Tsige* 2012 ONCA 32 at para 39.

114 *Application under s.83.28 of the Criminal Code (Re)* 2004 SCC 42 at paras 115-116.

115 *Ibid* at para 8.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca
Telephone: 416-326-3333
Fax: 416-325-9195

June 2013

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, September 3, 2015

Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators

Increased Privacy Protections and Higher Legal Standards to Be Required

The Justice Department today announced a new policy for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard and increase privacy protections in relation to law enforcement's use of this critical technology.

The policy, which goes into effect immediately and applies department-wide, will provide department components with standard guidance for the use of cell-site simulators in the department's domestic criminal investigations and will establish new management controls for the use of the technology.

"With the issuance of this policy, the Department of Justice reaffirms its commitment to hold itself to the highest standards as it performs its critical work to protect public safety," said Deputy Attorney General Sally Quillian Yates. "Cell-site simulator technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations and complicated narcotics cases. This new policy ensures our protocols for this technology are consistent, well-managed and respectful of individuals' privacy and civil liberties."

Cell-site simulators are just one tool among many traditional law enforcement techniques and are deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, when the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.

Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

While the department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department components will be required to track and report the number of times the technology is deployed under these exceptions.

To ensure that the use of the technology is well managed and consistent across the department, the policy

requires appropriate supervision and approval.

15-1084

Office of the Deputy Attorney General

Download DOJ Cell-Site Simulator Policy 9-3-15

Updated September 3, 2015

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

PARLIAMENTARY OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE EUROPEAN UNION

STUDY

EN

2011

PARLIAMENTARY OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE EUROPEAN UNION

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

PARLIAMENTARY OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE EUROPEAN UNION

STUDY

Abstract

This study evaluates the oversight of national security and intelligence agencies by parliaments and specialised non-parliamentary oversight bodies, with a view to identifying good practices that can inform the European Parliament's approach to strengthening the oversight of Europol, Eurojust, Frontex and, to a lesser extent, Sitcen. The study puts forward a series of detailed recommendations (including in the field of access to classified information) that are formulated on the basis of in-depth assessments of: (1) the current functions and powers of these four bodies; (2) existing arrangements for the oversight of these bodies by the European Parliament, the Joint Supervisory Bodies and national parliaments; and (3) the legal and institutional frameworks for parliamentary and specialised oversight of security and intelligence agencies in EU Member States and other major democracies.

PE 453.207 EN

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHORS

Aidan WILLS, Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Mathias VERMEULEN, European University Institute (EUI)

Hans BORN, Project Leader, DCAF
Martin SCHEININ, Project Leader, EUI
Micha WIEBUSCH, Research Assistant, DCAF

Ashley THORNTON, Language Consultant

RESPONSIBLE ADMINISTRATOR

Andreas HARTMANN
Policy Department C: Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Bruxelles
E-mail: andreas.hartmann@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its newsletter please write to:
poldep-citizens@europarl.europa.eu

Manuscript completed in June 2011.

This document is available on the Internet at:
http://www.europarl.europa.eu/activities/committees/studies.do?language=EN
http://www.ipolnet.ep.parl.union.eu/ipolnet/cms

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

AAI	*Autorités Administratives Indépendantes* (France)
AFET	Committee on Foreign Affairs, Fundamental Rights and Common Security and Defence Policy (EU)
AFSJ	Area of Freedom, Security and Justice (EU)
AIC	Australian Intelligence Community
AISE	External Information and Security Agency (Italy)
AISI	Internal Information and Security Agency (Italy)
ANAO	Australian National Audit Office
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
AWFs	Analysis Work Files
BfV	*Bundesamt für Verfassungsschutz*/Federal Office for the Protection of the Constitution (Germany)
BND	*Bundesnachrichtendienst*/Federal Intelligence Service (Germany)
BNDG	*Gesetz über den Bundesnachrichtendienst*/Federal Intelligence Service Act (Germany)
BVerfSchG	*Bundesverfassungsschutzgesetz*/Federal Protection of the Constitution Act (Germany)
BUDG	EP's Committee on Budgets
CATS	Article 36 Committee (EU)
CBO	Congressional Budget Office (USA)
CCSDN	*Commission consultative du secret de la défense nationale* (France)
CEPOL	European Police College
CFSP	Common Foreign and Security Policy (EU)
CIA	Central Intelligence Agency (USA)
CIC	Civilian Intelligence Cell (EU)

CIS	Customs Information System
CISR	Inter-Ministerial Committee for the Security of the Republic (Italy)
CJEU	Court of Justice of the European Union
CMS	Case Management System
CNCIS	*Commission nationale de contrôle des interceptions de sécurité* (France)
CNI	National Intelligence Centre (Spain)
CNIL	*Commission nationale de l'informatique et des libertés* (France)
ComCen	Communications Unit (EU)
CONT	Committee on Budgetary Control (EU)
COPACO	Parliamentary Control Committee (Italy)
COPASIR	Parliamentary Committee for the Security of the Republic (Italy)
COSAC	Conference of national parliaments' European Affairs Committees
COSI	Standing Committee on Operational Security (EU)
CPC	Commission of Public Complaints (Canada)
CRS	Congressional Research Service (USA)
CSDP	Common Security and Defence Policy
CSIS	Canadian Security Intelligence Service
CTIVD	Dutch Review Committee on the Intelligence and Security Services
CUTA	Coordination Unit for Threat Assessment (Belgium)
CTIVD	Intelligence and Security Services Review Committee (Netherlands)
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DCRI	*Direction centrale du renseignement intérieur* (France)
DGPN	French National Police
DGSE	*Direction générale de la sécurité extérieure* (France)

DHS	Department of Homeland Security (USA)
DIGO	Defence Imagery and Geospatial Organisation (Australia)
DIO	Defence Intelligence Organisation (Australia)
DIS	Department of Security Intelligence (Italy)
DPO	Data Protection Officer (EU)
DPR	*Délégation parlementaire au renseignement* (France)
DSD	Defence Signals Directorate (Australia)
EASO	European Asylum Support Office
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EIRAN	European Intelligence Review Agencies Knowledge Network
EP	European Parliament
EPP	European Public Prosecutor's Office
ESDP	European Security and Defence Policy
ETA	*Euskadi Ta Askatasuna* (Spain)
EU	European Union
EUCI	European Union Classified Information
EUI	European University Institute
EURODAC	European Dactyloscopy (fingerprint database)
Eurojust	EU's Judicial Cooperation Unit
Europol	European Police Office
FBI	Federal Bureau of Investigation (USA)

FRA	Defence Radio Establishment (Sweden)
Frontex	European agency for the coordination of operational cooperation at the external borders of the EU
FUD	Defence Intelligence Court (Sweden)
G10	*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*/Article 10 Act (Germany)
GAO	Government Accountability Office (USA)
GCHQ	Government Communications Headquarters (UK)
GG	*Grundgesetz*/the Basic Law (Germany)
GISS	General Intelligence and Security Service (Netherlands)
GISS	General Intelligence and Security Service of the Armed Forces (Belgium)
GOU	General Operations Unit (EU)
HB	Herri Batasuna (Spain)
IGIS	Inspector-General of Intelligence and Security (Australia)
ISA	Intelligence Services Act 1994 (UK)
IPEX	Interparliamentary EU Exchange Information Network
IPT	Investigatory Powers Tribunal (UK)
IS	Europol Information System
ISC	Intelligence and Security Committee (UK)
ITAC	Integrated Threat Assessment Centre (Canada)
JHA	Justice and Home Affairs
JITs	Joint Investigation Teams (EU)
JSB	Joint Supervisory Body (EU)
JTAC	Joint Terrorism Analysis Centre (UK)
JuU	Committee on the Administration of Justice (Sweden)
KU	Committee on the Constitution (Sweden)

LIBE Committee on Civil Liberties, Justice and Home Affairs (EU)

MI5 Security Service (UK)

MI6 Secret Intelligence Service (UK)

MAD *Militärischer Abschirmdienst*/Military Counterintelligence Service (Germany)

MADG *Gesetz über den Militärischen Abschirmdienst*/Military Counterintelligence Service Act (Germany)

MEP Member of the European Parliament

MISS Defence Intelligence and Security Service (Netherlands)

MP Member of Parliament

NATO North Atlantic Treaty Organization

NCTb National Coordinator for Counterterrorism (Netherlands)

NICC National Intelligence Coordination Committee (Australia)

NPB National Police Board (Sweden)

NSC National Security Committee (Hungary)

NSA National Security Agency (USA)

NSB National Supervisory Body (EU)

NSC National Security Committee of the Department of Prime Minister and Cabinet (Australia)

OCHA Office for the Coordination of Humanitarian Affairs

OC Organised Crime

OCTA Organised Crime Threat Assessment (EU)

OCTA-WA Organised Crime Threat Assessment on West Africa (Europol)

OLAF European Anti-Fraud Office

ONA Office of National Assessments (Australia)

PDA Police Data Act (Sweden)

PJCIS Parliamentary Joint Committee on Intelligence and Security (Australia)

PKGrG	*Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes*/Parliamentary Scrutiny of Federal Intelligence Activities Act (Germany)
RCMP	Royal Canadian Mounted Police
RIPA	Regulation of Investigatory Powers Act 2000 (UK)
ROCTA	Organised Crime Threat Assessment on Russia (Europol)
RoP	Rules of Procedure
SAKINT	Swedish Committee on Security and Integrity Protection
SCAN	Europol's Scanning, Analysis & Notification System
SDECE	*Service de documentation extérieure et de contre-espionnage* (France)
SEDE	Committee on Foreign Affairs Sub-Committee of Defence (EU)
SIN	Commission on Security and Integrity Protection (Sweden)
SIRC	Security Intelligence Review Committee (Canada)
SIS	Schengen Information System
SIS II	Second generation Schengen Information System
Sitcen	Situation Centre (EU)
SIUN	Defence Intelligence Inspection (Sweden)
SNE	Seconded National Experts
SOCTA	Serious and Organised Crime Threat Assessment
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TDIP	Temporary Committee on the alleged use of European countries by the CIA for the transport and illegal detention of prisoners
TESAT	Terrorism Situation and Trend Reports (EU)
TFEU	Treaty on the Functioning of the European Union
TFTP	EU Terrorist Finance Tracking Programme
ToR	Terms of Reference
UMP	Union for a Popular Movement

UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on Drugs and Crime
VIS	Visa Information System

LIST OF TABLES

EXECUTIVE SUMMARY

The European Parliament's Directorate-General for Internal Policies mandated the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the European Union Institute (EUI) to carry out a study on *'parliamentary oversight of intelligence agencies in relevant EU Member States and other major democracies'. This study was expected to 'identify democratic standards and best practice as well as a proper balance between the demands of secrecy and the need for scrutiny which can be used by the European Parliament (EP) when it sets up its own oversight body'.* Following consultations with the EP's Directorate General for Internal Policies, it was decided to interpret this mandate against the backdrop of four important trends and developments which have prompted a discussion on how the EP can strengthen oversight of the EU's AFSJ agencies, as well as the European Union's Situation Centre (Sitcen)[1] which plays a role in the Area of Freedom Security and Justice (AFSJ):

(1) The Treaty of Lisbon gives the EP and national parliaments a mandate to strengthen their oversight of two AFSJ bodies: Europol and Eurojust. It explicitly provides for the new regulations on Europol and Eurojust to include provisions on parliamentary 'scrutiny' (in the case of Europol) and 'evaluation' (in the case of Eurojust). Within the next two years, the Commission will put forward proposals for these regulations; the EP will have the opportunity to ensure that this legislation includes appropriate provisions on parliamentary oversight. In addition, the fact that the Area of Freedom, Security and Justice is now subject to the standard legislative procedure means that the EP is now better placed to ensure that new or revised legal frameworks for the AFSJ agencies include provisions on parliamentary oversight. Indeed, it has already done so in a draft regulation on Frontex, which, at the time of writing, was under discussion.

(2) The EP may have some opportunities to address the work of Sitcen, which performs a number of functions pertaining to internal security, because it is now part of the European External Action Service (EEAS). While the EEAS (and thus Sitcen) falls under the Common Foreign and Security Policy (CFSP), which is an intergovernmental policy area, the Treaty of Lisbon gives the EP some new powers in this area.

(3) There have been important developments in the area of access to information, which are intrinsically linked to strengthening oversight of the AFSJ bodies. In 2010, the EP and Commission concluded a new inter-institutional agreement, which significantly improves the EP's access to information from the Commission. In addition, the EP is currently considering the revision of the EU's legislation on access to information, as well as the possibility of a new inter-institutional agreement with the Council, which would include provisions on parliamentary access to classified information. The trajectory of these ongoing discussions will have profound implications for the EP's oversight of AFSJ bodies.

(4) More generally, over the past decade, the EP has developed a growing interest in both national security agencies and AFSJ bodies. This has been evidenced by its strong interest in the development of the new regulation on Frontex, the Europol and Eurojust decisions, as well as two temporary committees that examined the activities of national security agencies and made important recommendations in regard to oversight.

[1] This study uses the term 'AFSJ bodies' to refer to the AFSJ agencies (Europol, Eurojust and Frontex) and the European Union's Situation Centre (Sitcen).

On the basis of this interpretation of the mandate, the primary aim of this study is to provide a comparative assessment of the oversight of intelligence agencies in European Union member states and other democracies, with the aim of identifying good practices that can inform the debate on strengthening oversight of the AFSJ bodies by the European Parliament.

This study focuses on Europol, Frontex and Eurojust as well as Sitcen. Broadly speaking, the role of these AFSJ bodies is to facilitate, coordinate and strengthen cooperation between national authorities with the aim of promoting security and justice within the EU. Arguably the defining feature of the national intelligence agencies[2] is their power to use what are known as 'special powers' to collect information, such as the powers to intercept communications, conduct covert surveillance, use secret informants, and even enter dwellings surreptitiously. The AFSJ bodies do not possess such powers, and when juxtaposed alongside this description, it is evident that the EU's AFSJ bodies are not intelligence agencies in the way that they are conceptualised at the national level. In view of the fact the EP is interested in strengthening oversight of these bodies, a mandate to study and draw lessons from the oversight of national 'intelligence agencies' may appear to be an unusual choice.

Nevertheless, the AFSJ bodies and national intelligence agencies share a number of characteristics. They perform 'intelligence functions' of national intelligence agencies, albeit not necessarily in the same way or for the same purpose. Notably, they collect (though without recourse to special powers), analyse and disseminate information to a range of decision makers. Another important similarity between the AFSJ bodies and national intelligence agencies is that they too receive, produce and disseminate classified information. This has important implications for oversight because overseers need access to classified information in order to scrutinise the work of agencies whose activities are 'classified' and/or entail the use of classified information, which is an area where the EP can learn much from national systems of oversight. We should, however, remain cautious about the 'portability' of oversight models and practices from the national to the EU level given that national overseers and the EP scrutinise agencies with very different mandates and powers. Oversight has to be understood in the context of the organisations which are being overseen.

This study is comprised of five chapters. The first discusses the aims, mandate and methodology of the study. The second chapter provides an overview of the legal basis, mandate and current powers of Europol, Eurojust, Frontex and Sitcen, and identifies several areas of these bodies' work that might raise concerns from the point of view of oversight. The third chapter anaylses the EP's existing role and powers for overseeing the AFSJ bodies, as well as the scope of its access to information from (and pertaining to) these bodies. This chapter also examines the role of national parliaments in overseeing the AFSJ bodies, as well as the role of the Joint Supervisory Bodies (JSBs) of Europol and Eurojust in scrutinising these agencies' use of personal data. Chapter four provides a detailed

[2] The term 'intelligence agency' generally refers to a state body that collects, analyses and disseminates information—on threats to national security or other national interests—to policy-makers and other executive bodies. Intelligence agencies may perform these 'intelligence functions' exclusively outside of their state's territorial jurisdiction (e.g., the UK's Secret Intelligence Service), exclusively within their state's territory (e.g., Germany's Federal Office for the Protection of the Constitution), or both inside and outside their territory (e.g., the Dutch General Intelligence Service or AIVD). In a few states (e.g., in Sweden and Denmark), these bodies may also possess police powers and are therefore sometimes called 'police security services'. For reasons of consistency, this study uses the term 'intelligence agency' to refer to organisations which are variously labelled as 'security services', 'domestic intelligence agencies' or 'intelligence services'.

comparative assessment of how parliamentary and specialised non-parliamentary oversight is organised and carried out on a national level. This section will pay particular attention to access to information by parliamentary and non-parliamentary oversight bodies. The final chapter of the study outlines a series of options for consolidating and strengthening oversight of Europol, Eurojust, Frontex and Sitcen by the European Parliament. This executive summary will focus on providing an overview of this chapter, including its twenty-two recommendations to the European Parliament.

Recommendations for strengthening the European Parliament's oversight of the AFSJ bodies

This study provides detailed recommendations which might be useful for the forthcoming debate on how the European Parliament's oversight of the AFSJ bodies could be strengthened. Some of these recommendations apply to the EP's oversight of all AFSJ bodies discussed in this study (i.e. Europol, Eurojust, Frontex and Sitcen); however, most focus exclusively on the AFSJ agencies (i.e. Europol, Eurojust, Frontex). This is because the EP has an explicit treaty mandate to oversee Eurojust and Europol, and will be a co-legislator for new regulations on these agencies and Frontex. The development of parliamentary oversight of the Sitcen will have to proceed along a different track because Sitcen falls under the Common Foreign and Security Policy (CFSP), an area in which the EP has fewer powers. The recommendations pertain to the oversight of the AFSJ bodies as they exist in May 2011. It is essential that oversight arrangements are developed in tandem with any changes to the mandates and powers of these bodies, and should remain commensurate with the activities being overseen.

In developing legal and institutional frameworks for parliamentary oversight of the AFSJ bodies the EP and other relevant stakeholders should remain mindful that oversight arrangements should not have the effect of dissuading member states from using these bodies to cooperate in the AFSJ. Most EU member states are now convinced of the added value that agencies such as Europol and Eurojust can have in supporting their own work. Yet, there is a risk that if oversight arrangements place too great a burden on the AFSJ bodies and/or national authorities, some member states may simply revert to bilateral channels of cooperation, which are less heavily regulated and perhaps not subject to the same levels of scrutiny. Any moves in this direction would undermine the capacity of the AFSJ bodies to contribute successfully to promoting freedom, justice and security in the EU.

Recommendation 1: The European Parliament should ensure that any new arrangements for the oversight of the AFSJ bodies do not serve to dissuade member states from using these bodies as platforms for cooperation.

Limitations on the scope of the European Parliament's oversight of the AFSJ bodies

This study highlights several factors which should serve to limit the scope of the EP's oversight of the AFSJ bodies. These primarily relate to oversight of the AFSJ bodies' operational activities. Firstly, the intergovernmental nature of the AFSJ bodies and the relationship between actions of the AFSJ bodies and Member States has important implications for oversight. Member States' police, prosecutorial, border (and to a much lesser extent) intelligence agencies are both the principal suppliers and the main customers

of the AFSJ bodies. The AFSJ bodies function primarily on the basis of information provided by national agencies and their principal output is information and analysis that is sent to these agencies. National agencies may take action, including the use of coercive powers, on the basis of such information, including within the context of operations coordinated by an AFSJ body such as Europol or Frontex. As is discussed in chapter two of the study, such action remains the exclusive responsibility of national authorities. The implication of this is that both the inputs to AFSJ bodies and actions taken on the basis of the outputs of these bodies are regulated by national law and should be overseen by appropriate national authorities. It is generally accepted inside the EP and in Member States that it is not the prerogative of the EP to oversee how national agencies collect information that might be shared with AFSJ bodies and/or action undertaken on the basis of information provided by AFSJ bodies.

Secondly, the AFSJ bodies consist of a mix of personnel seconded by the Member States and EU staff members. National liaison officers at Europol, national border guards that participate in a Frontex-coordinated operation, or seconded intelligence officers at Sitcen are paid by Member States and cooperate with the agencies in accordance with national laws. As such, their cooperation with and contributions to an AFSJ body are more appropriately overseen by national oversight mechanisms. This intergovernmental element of the AFSJ bodies requires that the EP works closely with national parliaments in ensuring that appropriate oversight arrangements are in place.

Thirdly, Europol and Eurojust are authorised to process, store and transfer personal data within the parameters of their mandates. These are activities which interfere with the right to privacy and may serve as the basis for use of coercive or special powers—which have particularly significant human rights implications—by member or third states' authorities. In view of this, these activities clearly need to be subject to oversight by an independent body. Accordingly, the EU has established specialised non-parliamentary oversight bodies—the Joint Supervisory Bodies (JSBs) of Europol and Eurojust—for this purpose. The JSBs have access to all files and premises related to the processing of personal data and are in a strong position to ensure that any practices which violate data protection regulations are corrected. In our view, the JSBs are an appropriate oversight mechanism for scrutinising the use of personal data by the AFSJ agencies. Accordingly, their activities do not need to be duplicated by the EP. Equally, the EP would not need to oversee Frontex's future role in processing personal data because it is envisaged that the European Data Protection Supervisor would perform a similar function to the JSBs.

There are several other arguments against involving the EP in the oversight of the AFSJ bodies' operational activities on an ongoing basis. First, as is noted in chapter four, this is extremely time consuming and requires specialised expertise and resources which many parliaments do not possess. A number of the MEPs and staffers interviewed for this study indicated that the EP would not have the time, resources, or inclination to scrutinise the operational activities of the AFSJ bodies. Oversight can be conducted more effectively by a 'professional' oversight body, such as the JSBs, that focuses exclusively on the oversight of an agency's operational activities. Second, giving the EP a mandate to oversee information processing would require the parliament to have access to personal data in these files, which would raise significant privacy concerns. Finally, parliamentary scrutiny of the operational aspects of the AFSJ bodies' work might adversely impact upon the effectiveness of these bodies. This is because many states are opposed to giving the EP a role in this regard and may reduce information sharing with the AFSJ bodies if the EP was given such a role.

The European Parliament's oversight mandate and functions

There was widespread agreement among our interlocutors at various EU institutions and bodies that the EP should play a role in overseeing the AFSJ bodies. Oversight of the AFSJ bodies by parliament and bodies created by parliament is important for reasons that are outlined in chapters one and four. Perhaps most importantly, the EP is now a co-legislator in the AFSJ and will have a pivotal role in defining the future mandate and powers of the AFSJ agencies in particular. Therefore, it is essential that the EP plays a role in ensuring that these agencies fulfil their mandates effectively and in a manner which complies with relevant legislation. In addition, the AFSJ agencies are funded to a large extent with EU funds that are appropriated to them by the EP. As the budgetary authority, the EP must have a role in ensuring that such money is used both correctly and efficiently.

These rationales for parliamentary oversight of the AFSJ agencies do not, however, imply that the EP should play a role in their management. When discussing the EP's role in the oversight of AFSJ bodies, we should remain mindful of the separation of powers and responsibilities in this regard. This is particularly important in relation to Eurojust because it works with judicial bodies. Oversight of the AFSJ bodies should also not be conflated with controlling or co-managing an agency—this is not the role of a parliament. The AFSJ bodies are meant to serve as repositories of expertise which exist to provide a professional service to the EU and its Member States. It is not the role of parliamentarians to meddle in the management of this work; such functions are primarily the prerogative of the agencies' directors and their management boards. Meanwhile, the Commission and/or Council provide political direction to AFSJ bodies and assume political responsibility for them. For these reasons, the involvement of the EP in matters such as the appointment of management board representatives, or even as part of the management boards of the AFSJ agencies is not recommended. Indeed, the involvement of the EP in these decision-making processes would obfuscate its oversight functions, making it extremely difficult to subsequently review independently the actions of agencies and their management boards.

Recommendation 2: The European Parliament should not be part of the management boards of Europol or Frontex, or of the College of Eurojust.

In chapter four we argue that it is difficult to advocate a 'best' approach or practice in regard to the subject(s) of an oversight body's mandate. Ultimately, what matters is that all dimensions of an intelligence agency's work are overseen by a body which is independent from the agencies and the executive. In the case of the EU, this means independent from the AFSJ bodies, the Council and the Commission. Chapter four of the study illustrates that the 'subject' of oversight can be broadly divided into four areas: operations, policy, administration and finance. In view of the foregoing comments on the role of the JSBs and national authorities in overseeing the operational activities of the AFSJ bodies, it is clear that the EP should focus on overseeing the policies, administration and finance of these bodies. This is, however, without prejudice to the EP's powers of inquiry (discussed in chapter three), under which the EP could, of course, examine allegations that any activities of these agencies violate EU law.

Recommendation 3: The European Parliament's oversight of the AFSJ agencies should focus on their policies, administration and finance.

Oversight of the finances of the AFSJ agencies

The EP can make better use of its budgetary appropriation and discharge powers in its oversight of the AFSJ agencies by ensuring a continued link between the oversight of agencies' policies and administration and the approval and discharge of the agencies' budgets. The entire budget cycle requires close cooperation between the LIBE Committee (or any newly created body with a mandate to oversee the AFSJ agencies), the Committee on Budgets (BUDG) and the Committee on Budgetary Control (CONT. There are four main ways in which the EP can effectively continue and improve the use of its budgetary oversight powers in this regard. First, the EP needs to continue to strengthen the cooperation between CONT, BUDG and the LIBE Committee throughout the budget cycle to ensure that there are links between the oversight of the AFSJ agencies' finances and other areas of their work. Second, some members of the LIBE Committee need to be made more aware of the formidable budgetary and discharge powers at the EP's disposal and how LIBE can work with the BUDG and CONT committees to more effectively use these powers in the fulfilment of its mandate. Third, the powers of the purse (both the reserve procedure and the power to withhold or delay discharge of a budget) can be used as a tool for requesting a change in the policies, procedures or activities of the AFSJ agency concerned. Finally, as we mentioned in chapter three, the reserve procedure may, in some exceptional circumstances, be used as a tool to persuade an AFSJ agency to disclose information in any area that is financed from the EU budget. This should not, however, be necessary if a new legal framework for access to classified information by the EP is adopted (see below).

Recommendation 4: The European Parliament should ensure its budgetary appropriation and discharge functions are fully linked to other aspects of its oversight of AFSJ agencies.

Keeping the European Parliament informed about security threats

The European Parliament needs to be informed about threats to the security of the EU and its member states in order to fully evaluate the measures that are needed to counter such threats. Without this information, it is hard for the EP to fully assess whether the AFSJ bodies may, for example, need new powers (i.e., requiring legislative amendments), additional resources or new cooperation agreements with particular third states. Indeed, this is an excellent example of an area in which the EP should ensure that there is a close relationship between its role as a legislator, budgetary authority and overseer. Making the EP aware of pertinent threats may also be in the interests of the agencies because in this way they can make MEPs aware of their need for additional legal powers or resources; MEPs may be useful allies in this regard (see chapter four). The EP could, for instance, be provided risk assessments and threat analyses from Frontex, the full version of Europol's Organised Crime Threat Assessment, or terrorist threat assessments from the Sitcen (see chapter two). Such assessments are classified and would therefore, need to be provided to the body within the EP designated to receive classified information. In this context, the responsible body could hold in camera discussions with relevant officials from the AFSJ bodies.

Recommendation 5: The European Parliament should receive threat assessments from the AFSJ bodies. This would enable Parliament to better assess whether these bodies have the necessary legal mandate, powers and financial resources to address such threats.

The European Parliament's relationship with the Joint Supervisory Bodies

The EP currently has very limited engagement with the two JSBs. Closer engagement with the JSBs could begin with inviting their chairpersons to discuss their biennial and thematic reports with the relevant body within the EP (see below). This dialogue would allow the chairs of the JSBs to express any concerns about their mandate, powers or the resources available to them. Meetings between the EP and JSBs could also serve as a forum to discuss the implementation of JSBs' recommendations. On this basis, the EP could use its political clout to raise any concerns with agency directors or management boards, and it could use its budgetary powers to address such matters. More regular engagement with the JSBs could also benefit MEPs in the carrying out of their work. The JSBs are repositories of significant amounts of knowledge and expertise which could benefit MEPs when, for example, preparing for hearings with agency directors or drafting own-initiative or legislative reports on Europol and Eurojust. MEPs and their staffers may benefit from this expertise not only through periodic hearings but also by reviewing the JSBs' reports and holding informal discussions with members of the JSBs and their secretariat.

In the context of closer engagement between the EP and the JSBs (or any other specialised non-parliamentary oversight bodies that are created), a body of MEPs may need to be given access to the inspection reports of the JSBs. What the EP will not need is access to data inputted into Europol's databases or Eurojust's CMS, and/or personal data shared with national authorities or third states. Access to this data would give rise to serious privacy concerns. If, in the context of its oversight functions, the EP does have access to documents which contain personal data, personal data should be deleted from these documents, as is foreseen under Annex Two of the 2010 Framework Agreement between the Commission and the Parliament.

The EP could consider adopting the practice used in some Member States whereby parliament can request a non-parliamentary oversight body to examine a particular matter (see chapter four). This is a more direct means by which a parliament can take advantage of both the expertise and independence of a non-parliamentary oversight body in order to examine particular aspects of an agency's work. To our knowledge, the EP cannot currently make such requests to the JSBs. Any provisions of this nature would need to be carefully formulated to ensure that the independence of a non-parliamentary oversight body, such as the JSBs, could not be compromised by such requests from the EP. Accordingly, much can be learned from the good practice on a national level, namely that non-parliamentary oversight bodies have the final decision on whether or not they will examine an issue at the request of parliament or any other entity (see chapter four).

Recommendation 6: The European Parliament should engage in regular dialogue with the Joint Supervisory Bodies (JSBs) of Europol and Eurojust, and should make use of the reports and expertise of the JSBs in its own oversight of the AFSJ agencies.

Standardisation of the European Parliament's right to summon the directors of AFSJ agencies

The EP currently has the power to require the Director of Europol and the Chairperson of the Europol Management Board to appear before it. This power should be extended to Frontex (the Director and Chair of the management board) and Eurojust (the Administrative Director and President of the college). While the European Parliament does not have these powers with respect to Eurojust and Frontex, it needs to be stressed that, in practice, directors of the AFSJ agencies often appear before the parliament upon its request and are aware that refusing to appear before parliament would make for bad publicity.

The power to summon agency directors and chairpersons of the management boards/college could be particularly useful outside the context of agency directors presenting an agency's annual report. It would, for example, enable the EP to require the appearance of a director in the event of a particular problem or scandal coming to light. However, the right to summon the director of an AFSJ body may be of limited value unless the MEPs involved have the right to discuss classified matters. Under existing procedures, directors cannot or choose not to answer questions which would entail disclosing classified information. This further illustrates the need to formulate a proper framework for parliamentary access to classified information before developing other oversight mechanisms (see below).

We have opted to confine this recommendation to the AFSJ agencies, i.e., not to include the director of Sitcen. It is difficult to envisage how this formal power could be extended to the director of Sitcen because it is not an autonomous agency. The EP can, however, request the High Representative for Foreign and Security Policy, under whom Sitcen falls, to appear before it.

Recommendation 7: The European Parliament's power to summon the director of Europol and the chairperson of the Europol Management Board should be extended to the equivalent persons at Eurojust and Frontex.

Oversight of the appointment of agency directors

Currently, the EP does not play any role in the appointment of AFSJ agency directors or the director of Sitcen. Yet, the EP has long expressed a desire to be involved in the appointment of directors of these bodies. Chapter four's survey of the role of national parliaments in the appointment of directors of intelligence agencies demonstrates that the majority of parliaments are not involved in the appointment of the directors of intelligence agencies.

There are a number of drawbacks associated with involving the EP in the appointment of directors; these are broadly similar to arguments relating to the role of national parliaments in this regard, outlined in chapter four. First and foremost, involving the EP in the appointment of directors risks politicising the work of agencies which are meant to be non-political. This concern would be magnified if parliament's role in the appointment of directors were to include the power to approve or reject a nominee. Secondly, the current process for selecting the directors/president of Europol, Frontex and Eurojust is already protracted and cumbersome because it involves representatives of 27 Member States seeking to find a compromise candidate. Adding the EP to this process would serve to

further complicate and drag out an already lengthy process. Moreover, the fact that 27 states are already involved in the selection of directors ensures that there are inbuilt checks and balances, which prevent any single party appointing a director to promote their interests. This removes one of the main reasons for which national parliaments are involved in the appointment of the directors of intelligence agencies: to prevent the incumbent government appointing someone to promote and protect partisan political interests.

All things considered, the authors are not persuaded that the European Parliament should be given a role in the appointment of directors of the AFSJ bodies. The parliament should, however, be kept informed regarding appointment processes. This should include information on the identity and credentials of proposed candidates.

Recommendation 8: The European Parliament should not be given a role in the appointment of the directors/president of the AFSJ bodies.

A role for the European Parliament in providing assessments on the human rights records of AFSJ bodies' cooperation partners

While the JSBs provide an opinion on the legal and institutional frameworks for data protection in third states, they do not examine the broader human rights record of particular foreign partners, such as a police agency in a third state. There is, therefore, no independent assessment of whether or not agencies with which AFSJ bodies share information use techniques which violate human rights. As is discussed in chapter four, this is relevant to both incoming and outgoing information. Foreign partners may collect information through e.g., torture or arbitrary detention and then share this information with AFSJ bodies. Equally, they may use information provided by AFSJ bodies as part of activities which violate human rights. These concerns are primarily relevant to the sharing of personal data.

Although the AFSJ bodies' own due diligence processes should prevent this from happening, it is good practice for an independent oversight body to provide some form of human rights assessment of the general human rights record/compliance of partner agencies in third states. There is precedence for this at the national level (see chapter four) and this is a role which could be performed by the EP or another independent body. If the EP were to assume this role, it would make sense to involve the AFET Committee's Sub-Committee on Human Rights, which has expertise in examining human rights matters outside the European Union. Such assessments would not be binding but could serve to inform the Council and AFSJ agencies' management boards in the context of entering into information sharing agreements with third states.

Recommendation 9: The European Parliament should ensure that either a (sub)committee of parliament or a specialised non-parliamentary body provides independent assessments of the general human rights records/compliance of agencies in third states with which the AFSJ bodies cooperate. Such assessments could take place before an information sharing or other cooperation agreement is signed with a third state, and during the implementation of these agreements.

A role for the European Parliament in reviewing the AFSJ bodies' information sharing agreements and memoranda of understanding

Information sharing agreements are an important part of agencies' policy and should therefore, be subject to review by the EP. Indeed, it is important that the EP is aware of the terms upon which the AFSJ bodies cooperate with each other, and with foreign entities. In our view, the EP should not play a role in the formulation or approval of agency to agency information sharing agreements or memoranda of understanding (which are distinct from agreements between the EU and third states, such as the SWIFT agreement). However, a designated body of parliament should be able to review, ex post, agreements that have been concluded and to raise questions or concerns regarding, inter alia, the content and implementation of such agreements. It is not sufficient for the EP to be simply made aware that such agreements exist. Accordingly, the AFSJ bodies should be required to forward agreements and memoranda of understanding to relevant bodies in parliament, even if such agreements are considered to be classified.

Recommendation 10: The European Parliament should have access to information sharing agreements and other memoranda of understanding concluded between AFSJ bodies within the European Union, as well as between AFSJ bodies and third states or organisations.

Access to and the protection of classified information by the European Parliament

As this study's analysis of oversight of intelligence agencies at the national level demonstrates, information is the oxygen that sustains oversight; a mandate to oversee an agency's work is of limited use unless it is accompanied by access to the relevant information. It will be extremely difficult to strengthen parliamentary oversight of the AFSJ bodies without clear and predictable rules and procedures for the EP to access relevant information from these bodies, the Commission and the Council. While access to relevant information is fundamental to oversight, the professional handling of this information by overseers is also crucial for effective oversight. Accordingly, improved access to classified information by the EP will need to be accompanied by the development of appropriate procedures for the protection of this information, as well as an ongoing commitment from MEPs to handle classified information in a professional manner.

Improving the European Parliament's access to classified information in the AFSJ

The development of an appropriate legal and institutional framework for parliamentary access to classified information is of fundamental importance to strengthening the EP's oversight of the AFSJ bodies. The discussion of the EP's access to classified information must take place alongside deliberations on the evolution of the EP's mandate to oversee the AFSJ bodies; indeed, we have argued throughout this study that an oversight body's information needs are inextricably linked to its mandate. Yet, regardless of which aspects of the AFSJ bodies' work the EP wishes to oversee and which institutional mechanism is chosen to carry out this oversight (see below for a discussion of these mechanisms), access to relevant classified information will be crucial. This is because various aspects of the work of AFSJ bodies are classified and/or involve the processing or creation of classified information.

Parliamentary access to classified information is currently being discussed in the context of deliberations regarding the revision of Regulation 1049—legislation which is ostensibly

about public access to information from EU entities. The EP's rapporteur on this matter, Michael Cashman, has opted to include provisions on parliamentary access to information in the broader draft legal framework for public access to EU documents. This approach has several advantages. First, it is aimed at ensuring that there is a general framework for the EP's access to classified information from all EU entities and across all policy domains. This may be preferable to a fragmented legal framework for parliamentary access to information based on inter-institutional agreements across different fields. The effects of this current framework are that the EP has access to classified information from, e.g., the Council, in some fields but not others and that different modalities apply to access classified information in different policy domains. Second, the inclusion of provisions on the EP's access to classified information as part of broader legislation on public access to information could help to ensure that these rules have the status of legislation rather than being enshrined in inter-institutional agreements, which are of a subordinate legal status.

In spite of these advantages, we are of the view that parliamentary access to classified information should be decoupled from provisions on public access to information. This is supported by practice on the national level, where freedom of/access to information laws are separated entirely from regulations on parliamentary access to information. Parliamentary access to classified information implies access to the specific categories of information which are justifiably exempt from public access, e.g., information regarding the work of intelligence agencies. It is precisely because such information is beyond the reach of public access that it must be available to certain parliamentarians and institutions established by parliaments for overseeing, inter alia, intelligence agencies. In almost every state analysed in this study, parliaments have privileged access to classified information to, among other things, enable to them oversee intelligence activities. This is premised on the notion that parliamentarians are elected by a population to hold governments and their agencies to account. In order to do this, they require privileged access to information which is not necessarily available to members of the public. Therefore, rules governing parliamentary access to classified information are set out in law and are disconnected for general freedom of/access to information laws.

Recommendation 11: New regulations on the European Parliament's access to classified information should be decoupled from legislation on public access to information.

The legal basis for access to information by the European Parliament

The EP could pursue a number of options with regards to developing a new legal framework for parliamentary access to classified information in the AFSJ and beyond. First, provisions on parliamentary access to classified information could be integrated in the new regulations on Europol, Eurojust and Frontex. Such provisions would be developed alongside regulations on parliamentary oversight of these agencies, thus ensuring that the EP's access to classified information from and relating to each agency is clearly tied to its oversight mandate and functions with regards to each agency. It is important to note that these regulations would need to extend to the EP's access to classified information from the Council because the Council has 'ownership' of a significant amount of information relating to the AFSJ agencies.

Second, the EP could attempt to negotiate a specific inter-institutional agreement with the Council covering the AFSJ. An agreement with the Council covering the AFSJ could help to ensure a uniform set of regulations on parliamentary access as well as one mechanism for such access (e.g., the special committee or sub-committee options discussed in chapter

five). It is not clear, however, whether an agreement with the Council could extend to parliamentary access to information from the agencies themselves. There may therefore be a need for some form of agreement between the EP and each of these three agencies regarding parliamentary access to information. This would likely require some form of amendment to the existing legislation on each agency, which is unlikely to happen given that the legislative basis for all three agencies is due to change within the next three years.

Third, as noted above, the EP's access to classified information in all policy areas could be regulated by overarching legislation that also deals with public access to EU documents. Under the current proposals, the EP could request access to classified information through, inter alia, the chair of the committee with responsibility for a given subject, e.g., LIBE for the AFSJ. If granted, the information would be made available to a special committee composed of seven members appointed by the EP's Conference of Presidents. The membership of the committee could consist of a core—comprised, for instance, of the leaders of the political groups—but it would not be a committee with a fixed membership. The merits of this particular institutional mechanism are discussed in more detail below. However, for reasons stated above, regulations on the EP's access to classified information should not be included in legislation on public access to information.

Recommendation 12: New legislation on the AFSJ agencies (Europol, Eurojust and Frontex) should include provisions on the European Parliament's access to classified information from and pertaining to these agencies. Such provisions should be anchored to the EP's mandate to oversee these agencies, which will be outlined in the same legislation.

In chapter three, it is argued that the legal framework regulating the EP's access to information relating to the Sitcen needs to be examined separately. This is because—in spite of Sitcen performing some functions which are relevant to the AFSJ—it falls in a different policy domain (the CFSP) in which the EP has fewer powers. Unlike the AFSJ agencies, it does not have its own legislative basis and there are no plans to 'Lisbonise' its legal basis.

The EP's existing special committee for the CSFP field may be able to access information pertaining to Sitcen but, to our knowledge, has never made use of this opportunity. The 2002 inter-institutional agreement between the Council and EP will probably need to be re-negotiated in view of the fact that the Lisbon Treaty has made profound changes to the CSFP field. For the purposes of this study, the most relevant change is that Sitcen is no longer exclusively a creature of the Council because it now falls under the EEAS structure. While the High Representative has declared that the existing inter-institutional agreement between the Council and EP, which regulates the EP's access to classified information in the CFSP field, will continue to apply, the modalities of the EEAS are so different that it seems likely there will be a need for a new agreement between the EP and EEAS, which would include provisions on parliamentary access to classified information. Yet, in view of the inter-governmental character of Sitcen, the Council may continue to be the gatekeeper to any parliamentary access to information regarding this body. Hence, the existing 2002 agreement between the EP and Council or an updated version thereof may continue to apply.

Recommendation 13: The European Parliament should consider negotiating an inter-institutional agreement with the European External Action Service, which would include provisions on parliamentary access to classified information.

The scope of the European Parliament's access to classified information from the AFSJ agencies

Rather than enumerating a specific list of the types of information the EP could have access to, it would be preferable for legislation to grant the EP a general right to request access to classified information which it deems to be relevant to its (new) oversight mandate and functions. In chapter four it is argued that this is a common good practice on the national level and helps to ensure that the responsibility for determining what information is relevant should, in the first instance, be the prerogative of the overseer. In the context of the EP's oversight of the AFSJ agencies, classified information would be requested by and made available to one of the institutional mechanisms outlined below. Access to classified information on the basis of requests would, however, be subject to appropriate limitations such as those outlined in Annex Two of the 2010 Framework Agreement between the EP and the Commission.

Recommendation 14: Legislative provisions on the oversight of the AFSJ agencies by the European Parliament should include a general right for a designated body of Parliament to access classified information it deems to be relevant to its oversight mandate and functions.

While the EP needs a general right to request access to classified information relevant to its mandate to oversee the AFSJ agencies, access to relevant information may be better ensured by requirements for the agencies to make proactive disclosures of particular categories of information. On the basis of what is advocated in chapter five, the following types of information could, for example, be subject to proactive disclosure:

- Annual work plans of the AFSJ agencies
- Threat assessments produced by the agencies
- Cooperation and information sharing agreements between the AFSJ agencies.=
- Cooperation and information sharing agreements between the AFSJ agencies and third states
- All information pertaining to budgeting and past expenditure

The proactive disclosure of these types of information is broadly in line with similar provisions which apply to proactive disclosures to oversight bodies on the national level (see chapter four).

Recommendation 15: New legislative provisions on the oversight of the AFSJ agencies by the European Parliament should enumerate specific categories of information, including classified information that must be proactively disclosed to a designated body of parliament.

The protection of information handled by the European Parliament

Improved access to classified information by the European Parliament will have to be accompanied by the concomitant development of rules and procedures pertaining to the protection of classified information handled by the EP.

Chapter four outlines three principal mechanisms used to ensure that members of oversight bodies do not disclose classified information without proper authorisation. The EP may wish

to consider each of these. Firstly, measures need to be taken to ensure that appropriate persons are selected for positions in which they will have access to classified information. One very simple way of doing this, which can be applied within the EP, is by group leaders carefully selecting MEPs to be members of bodies with access to classified information. The EP could follow the practice used in some national parliaments whereby members of committees that have access to classified information are selected by their peers, thus ensuring cross-party support (see chapter four). There is however, no precedent for this at the EP.

Vetting and security clearance processes are also used by some oversight bodies. While EP staffers should certainly be subject to security clearance before being granted access to classified information, the situation for MEPs is more complex. Chapter four illustrates that in the majority of (but not all) EU states, MPs are not subject to vetting and security clearance processes. This divergence in national practices has posed a problem for the EP because security clearance processes (of MEPs) have to be conducted by national authorities and, in many EU states, parliamentarians cannot be subject to security clearance. For this reason, the 2010 Framework Agreement between the EP and Commission left some scope for divergent Member State practices by inserting the phrase 'appropriate personal security clearance'. In view of the sensitivities associated with security clearing parliamentarians, it would be advisable for the EU institutions to follow this approach in developing the legal framework for access to classified information by MEPs from other EU institutions and bodies. However, it should be stressed that security clearance can be seen as a confidence building measure which can make it easier for overseers to gain access to classified information. In view of this, MEPs who are part of bodies that have access to classified information may wish to consider obtaining a security clearance, even when MPs in their state are not normally subject to security clearance processes.

Secondly, most states criminalise unauthorised disclosure of classified information by MPs and other overseers. At the EU level, penalties for unauthorised disclosure are complicated by the fact any prosecution of an MEP would have to take place under national law. The EP does, however, have its own disciplinary procedures which could be used in the event of an MEP making unauthorised disclosures of classified information. An assessment of the adequacy of these procedures is beyond the scope of this study. Indeed, more research is required on whether or not these procedures are effective, as well as on how national criminal law provisions would apply to unauthorised disclosures of classified information by MEPs or staffers. Ideally, there should be pan-EU consistency in this regard, in order to avoid the problem that MEPs are treated differently depending on their nationality.

Finally, physical protection measures and procedures play an important role in ensuring that classified information is not disclosed either accidentally or deliberately. At the time of writing, in May 2011, an EP working group was drafting new security procedures which will enable the EP to receive and handle classified information. This is taking place within the context of the implementation of Annex Two of the 2010 Framework Agreement between the EP and the Commission. While the development of these security procedures has been driven by an agreement that will facilitate the EP's access to classified information from the Commission, these procedures could be applied to information received from the Council, EEAS and AFSJ bodies. Given the highly technical nature of information protection procedures, the EP may benefit from discussions with national parliaments and non-parliamentary oversight bodies with experience in dealing with these matters.

It is important to note that these procedures alone will not be sufficient to persuade the AFSJ bodies, the Council, Commission and Member States that the European Parliament can be trusted with classified information. A relationship based on trust will need to gradually develop over time and will be greatly assisted by MEPs demonstrating that they will not disclose information without proper authorisation.

Oversight mechanisms

In chapter five we put forward different options regarding the mechanisms or bodies within parliament that could undertake the oversight functions discussed here. These are also the mechanisms through which the EP should be able to access classified information in the AFSJ.

It is preferable for the body that is given primary responsibility for the oversight of the AFSJ agencies to be the same body which has access to classified information in the AFSJ. Chapter four demonstrates that on the national level, specialised oversight committees are almost always one of the bodies (or the only body) in parliament that have access to classified information in the security domain (see Table 3). Having one mechanism for parliament to access information relating to AFSJ agencies and a separate body—without the same level of access to such information—for overseeing such bodies would seriously undermine oversight of these agencies. The reasons for this are self evident: bodies with a mandate to conduct oversight need access to relevant information, and bodies that have access to information relating to particular agencies but no clear mandate to oversee such agencies cannot make effective use of their privileged access to information.

Recommendation 16: The European Parliament body responsible for the oversight of the AFSJ agencies should also be the body of Parliament which has access to classified information in the Area of Freedom, Security and Justice.

It would be preferable for the EP to have one body (e.g., the LIBE Committee or a newly created sub-committee) that plays the lead role in the parliament's oversight of the AFSJ agencies. In order to ensure that the EP takes a coherent and coordinated approach to the oversight of the AFSJ agencies, there should be one body which has primary responsibility for all oversight functions vis-à-vis all AFSJ agencies. This responsibility should include not only the EP's own oversight mandate and functions but also cooperation with national parliaments and non-parliamentary oversight bodies such as the JSBs. An important exception to this is the financial oversight of the agencies which will, of course, remain the responsibility of the Budgets and Budgetary Control Committees. Nevertheless, whichever body has primary responsibility for the oversight of the AFSJ agencies should be closely involved in the work of the BUDG and CONT committees with respect to these agencies. It should be stressed that the 'body' discussed in this paragraph cannot be given primary responsibility for the oversight of Sitcen because it is situated in the Common Foreign and Security Policy field, under the High Representative.

Recommendation 17: The European Parliament should ensure that there is *one* body within parliament that has primary responsibility for the oversight of the Area of Freedom, Security and Justice (AFSJ) agencies.

The performance of additional oversight functions by the LIBE Committee

The development of a new body or mechanism within the EP is likely to be a complex and protracted process requiring the agreement of numerous other actors. Depending on which type of mechanism the EP opts to establish, it may not be possible until new legislation on Europol and Eurojust is drafted and there is a legal framework in place which regulates the EP's access to classified information in the AFSJ area. In view of this, it is necessary for the LIBE Committee to develop procedures that make it better suited to serving as a forum for the oversight of AFSJ agencies, at least on an interim basis.

One relatively straightforward option is for the bureau of the LIBE Committee to hold off-the-record briefings with directors/president of the AFSJ agencies and/or representatives of the management board (in the case of Europol & Frontex) and the College (in the case of Eurojust). This option could be utilised to permit MEPs to discuss sensitive matters with these individuals in small, private meetings. Matters under discussion could include anything which falls within the broader mandate of the LIBE Committee. For example, directors could use such meetings to brief bureau members on sensitive strategic issues or problems in the operation of their agency. During the course of our interviews, it became clear that some MEPs and the directors of the agencies would welcome the opportunity for more confidential meetings when particularly sensitive matters need to be discussed. Such meetings could be initiated at the request of the chair of the LIBE Committee, by directors/president of the AFSJ agencies, and/or by relevant figures from the management boards/college. While small, off-the-record meetings could be a useful option for ad hoc discussions on some issues, they could not serve as a mechanism for many of the oversight functions discussed above.

Recommendation 18: The European Parliament's LIBE Committee should develop procedures that make it better suited to serving as a forum for the oversight of AFSJ agencies, at least on an interim basis. For this purpose, the LIBE Committee could use off-the-record meetings between its Bureau and directors (or president in the case of Eurojust) of the AFSJ agencies and/or representatives from the agencies' management boards (or the College of Eurojust) to address sensitive issues which cannot be discussed in meetings of the full committee.

Special committee options for the Area of Freedom, Security and Justice (AFSJ)

Chapter three of the study examines the role of the European Parliament's 'Special Committee'—a small group of MEPs drawn primarily from the AFET Committee—used to enable the parliament to address matters which involve classified information in the CFSP field (hereafter, the 'Common Foreign and Security Policy - CFSP Special Committee'). There are a number of options for extending this committee's remit or using a similar model for the oversight of the AFSJ bodies. The remit of this Special Committee could potentially be extended, through an amended inter-institutional agreement, to the AFSJ field in order to allow the EP to address matters involving classified information relating to, inter alia, the AFSJ agencies. Alternatively, the EP and the Council could agree to create a special committee in the AFSJ along the lines of the CFSP special committee model. Both special committee options have a number of significant drawbacks.

A first problem is that a special committee of this nature is ultimately only a vehicle for its parent committee to have some access to classified information. Neither the existing special committee nor the proposed special committee for the AFSJ (as conceived of here) would have a specific oversight mandate. If it were to be given a specific mandate, it would

make sense to pursue the option of a security cleared permanent sub-committee instead (see below). Moreover, given that a special committee would be a small group of MEP's without its own secretariat and meeting on an occasional basis, it is difficult to see how it could undertake the various oversight functions outlined in chapter five, and summarised here.

Secondly, there are doubts about whether a special committee could make effective use of the classified information to which it had access in the context of discussions with Council and/or agency officials. Given that the special committee would not have a specific mandate or the capacity to produce reports, it is unclear what purpose would be served by it having access to classified information. Furthermore, members would obviously be prohibited from transmitting or referring to classified information in discussions with their colleagues in the LIBE Committee. This would make it difficult for the LIBE Committee to make use of the special committee's privileged access to classified information in its own work. For this reason, the use of a special committee in the AFSJ would be inconsistent with Recommendation 16 which stresses the need for the body responsible for oversight of the AFSJ agencies to be same body that has access to classified information relating to these agencies.

Thirdly, if members of a special committee for the AFSJ were not experts on the subjects and agencies being discussed, they may not have the relevant knowledge to ask the most relevant questions and/or seek access to relevant information. The risk of a special committee possessing insufficient specialised knowledge would be significantly increased if the EP and Council selected the option of extending the mandate of the existing CFSP special committee. This is because its members and staffers are primarily drawn from the AFET Committee and may not have specific knowledge or expertise relevant to the AFSJ.

Finally, a special committee arrangement for the AFSJ (and similar arrangements in other policy areas) would not obviate the need for a comprehensive legal framework on the EP's access to information in the AFSJ field and beyond. There is a risk that by granting access to classified AFSJ information to a special committee of MEPs, the Council may attempt to bypass the need for a fundamental reconsideration of the framework for parliamentary access to information.

Recommendation 19: The European Parliament should not seek to extend the existing Special Committee's mandate to include the Area of Freedom, Security and Justice (AFSJ), or to create a new special committee for the AFSJ.

The EP's existing CFSP Special Committee may address CFSP matters that include the discussion of classified information with the High Representative. Given that Sitcen falls under the purview of the High Representative, the CFSP Special Committee could use its meetings with her to address issues relating to Sitcen. Members of the CFSP Special Committee could, for example, seek to learn more about the composition of Sitcen, its current priorities, or the role it plays in providing assessments on threats to the EU's internal security.

Once again, the use of a special committee has a number of significant drawbacks. First, giving a very select group of MEPs access to information on the work of Sitcen may do little to raise broader awareness of the role of Sitcen amongst MEPs and staffers. The potential for such discussions to contribute to broader awareness of Sitcen's role would also depend on how much of the information discussed in a special committee meeting on Sitcen is deemed to be classified. Second, the success of this option would depend on the willingness

of the chair of the AFET Committee to take up the issue of Sitcen's internal security functions with the High Representative; this may be unlikely given that the AFET does not deal with internal security matters and has numerous other priorities to be addressed with the High Representative. Finally, there is, of course, no guarantee that the High Representative would be willing to discuss these issues given that Sitcen's work remains highly sensitive due to the presence of seconded officers from national intelligence agencies.

Yet, in spite of these drawbacks, the CFSP special committee is currently the only mechanism available to the EP for discussions about the work of Sitcen. As we have consistently stated, the EP is in a weaker position vis-à-vis Sitcen than it is with regards to the AFSJ agencies for a variety of reasons: e.g., Sitcen is not an autonomous agency funded from the EU budget, the EP doesn't have powers of co-legislation in the CFSP, and it doesn't have a clear treaty-based mandate to directly oversee Sitcen. The CFSP Special Committee is therefore, the only mechanism through which the EP may be able to conduct some limited oversight of the Sitcen.

Recommendation 20: The European Parliament should use its existing Special Committee to examine the work of the European Union's Situation Centre. The Special Committee could use its privileged access to classified information to address the role played by the Situation Centre in the Area of Freedom, Security and Justice.

Creation of a LIBE Sub-Committee for the oversight of the AFSJ agencies

The EP could consider establishing a sub-committee of the LIBE Committee to oversee the AFSJ agencies. This would be a permanent body, established in accordance with the EP's Rules of Procedure. We shall first put forward some suggestions regarding the modalities of such a sub-committee before outlining the reasons for which we believe this may be an effective mechanism for developing the EP's oversight of the AFSJ agencies.

Mandate

The mandate of any sub-committee would need to remain within the broad parameters of the LIBE Committee's mandate, which states that 'the Committee on Civil Liberties, Justice and Home Affairs Committee is responsible for […] Europol, Eurojust, Cepol and other bodies and agencies in the same area'. Within this context, the sub-committee would assume primary responsibility for the oversight of AFSJ agencies by the European Parliament. We envisage that the sub-committee's jurisdiction would extend to all of the AFSJ agencies which currently fall under the remit of the LIBE Committee. Under the current division of responsibilities in the EP, the sub-committee of the LIBE could not directly oversee the Sitcen because it is part of the EEAS, which falls under the jurisdiction of the AFET Committee. It could nevertheless cooperate closely with the AFET Committee, its Sub-Committee on Defence and the CFSP Special Committee on matters relating to the activities of the Sitcen which are relevant to the AFSJ.

The sub-committee could, for example, be given the task of performing the oversight functions outlined in chapter five and any other functions which the EP deems to be relevant. If the functions and powers of the AFSJ agencies were to evolve, the sub-committee's mandate would be amended accordingly. On the basis of the oversight

mandate and functions outlined earlier in this study, the sub-committee's mandate may include, but should not be limited to:

i. Serving as the forum for periodic and ad hoc meetings with, inter alia, the directors/president of the AFSJ agencies; representatives of the management boards/college; relevant officials from the Commission and Council;
ii. Receiving and reviewing the annual work plans and reports of the AFSJ agencies;
iii. Receiving threats assessments from the AFSJ agencies;
iv. Relations with the Joint Supervisory Bodies and any other specialised non-parliamentary oversight bodies which are created to oversee the AFSJ agencies. This role would include reviewing the annual and thematic reports of the JSBs and maintaining regular dialogue with them;
v. Drafting the LIBE Committee's own initiative and legislative reports on matters relating to the AFSJ agencies;
vi. Performing the advisory functions of the LIBE Committee with regards to the appropriation and discharge of the budgets for the AFSJ agencies, thereby providing expert opinions to support the work of the Budgets and Budgetary Control Committees;
vii. Cooperation with other committees of the European Parliament which have jurisdiction over matters related to the AFSJ agencies. Notably, the sub-committee could maintain dialogue with the AFET and the CFSP Special Committee regarding the Sitcen. If the EP decides to take up the option of drafting opinions on the human rights record of the AFSJ agencies' partners in third states, the sub-committee should consult with the AFET's Sub-Committee on Human Rights on this matter;
viii. Reviewing certain aspects of the AFSJ agencies' cooperation with third states and international organisations, including scrutinising the information sharing agreements concluded in this context;
ix. Reviewing relationships between AFSJ agencies, including their memoranda of understanding; and
x. Coordinating relations with national parliaments and representing the European Parliament in inter-parliamentary meetings which are relevant to the AFSJ.

In line with our earlier comments regarding the role of the EP in overseeing the AFSJ agencies, we do not believe that the sub-committee should duplicate the work of the JSBs in examining the legality of the use of personal data by certain AFSJ agencies. Moreover, it would not play a role in examining other operational activities of the agencies, e.g., their work files or the joint operations which they coordinate. Equally, the sub-committee should not encroach upon the jurisdiction of national parliaments and other oversight bodies responsible for scrutinising the work of national authorities that is connected to the AFSJ agencies.

Membership

The membership of the sub-committee would need to be determined in accordance with the guidelines established under Rules 186 and 190 of the European Parliament's Rules of Procedure. The existing sub-committees (of the Foreign Affairs Committee) on Security and Defence, and Human Rights have 28 members and 28 substitutes, and 30 members and 21 substitutes, respectively. These MEPs generally (but not necessarily) hold concurrent membership in the Foreign Affairs Committee.

It is our view that these numbers are too large considering the fact that two of the principal reasons for proposing a sub-committee are: (1) the need for a small, confidential forum for

discussions with the heads of the agencies and management boards; and (2) the need for MEPs to have access to some classified information relating to the agencies. A committee with as many as 50 members and substitutes would not fulfil these needs. Indeed, many of the aforementioned concerns which the agencies (and the Council and Commission) have about the confidentiality of discussions and protection of classified information would not be addressed if the sub-committee contained so many MEPs. Aside from concerns about the protection of classified information, a sub-committee arrangement would need to create conditions in which, inter alia, agency directors would feel confident that they could raise concerns or sensitive issues with a group of MEPs, without the content of such deliberations being further disseminated. Ultimately, agency directors and officials from the Council, Commission and JSBs are likely to abstain from discussing sensitive issues with the EP if they are not confident that discussions will remain confidential.

On the national level, the overwhelming majority of specialised parliamentary oversight committees include five to fifteen MPs (see Table 1 in chapter four). As is discussed in chapter four, such committees are normally smaller than other parliamentary committees for reasons of maintaining confidentiality. Accordingly, it is our view that a sub-committee should contain no more than 15 MEPs (including substitutes). This may, however, be difficult to accomplish in view of the requirement that the composition of EP committees and sub-committees reflects the overall composition of the parliament.

It would be beneficial if members of the sub-committee were either full or substitute members of the LIBE Committee. This would increase the likelihood that sub-committee members would have sufficient knowledge of the AFSJ agencies to enable them to contribute effectively to the sub-committee's functions. Finally, the EP could consider including some MEPs that are members of other (sub)-committees that deal with matters related to the AFSJ agencies and/or have other expertise which is relevant to the oversight of AFSJ agencies. These MEPs could include members of the Budgetary Control Committee, the Foreign Affairs Committee and its Sub-Committee on Human Rights. Chapter four illustrated that there is precedence for the inclusion of ex officio members (of other parliamentary committees) in national parliamentary oversight committees. This can help to ensure that there is proper coordination between committees that deal with related matters.

Access to information

All members of the sub-committee and its staffers would have the right to access classified information within the parameters of the sub-committee's mandate. In addition, certain categories of information could be subject to proactive disclosure to the sub-committee by the agencies, their management boards/college and, where appropriate, the Council and Commission (see above). The sub-committee would not, however, need to have access to information held in the agencies' databases or any personal data. The sub-committee would be required to implement the measures to protect information, which are discussed in chapter five.

Resources

The sub-committee would need to be supported by full-time security cleared staff. This is particularly essential in view of the fact that MEPs are frequently members of several committees and have to divide their time between work in their own states, Brussels and Strasbourg. Staffers are also essential to developing the parliament's institutional

knowledge and expertise on the AFSJ agencies; they ensure that such knowledge is retained even when MEPs move to other committees or leave the EP.

Assessment

Whether or not the European Parliament needs to establish a LIBE sub-committee to oversee the work of the AFSJ agencies depends to a large extent on how its mandate to oversee these agencies is defined in the forthcoming legislation on Europol, Eurojust and Frontex. If the EP's oversight mandate and functions remain broadly similar to the way they are now, i.e., relatively limited, it is not clear that a sub-committee would be necessary. If, however, the EP assumes additional oversight functions along the lines of the options presented in chapter five, there is a strong case for the establishment of a sub-committee. There are four main reasons for which we believe a sub-committee could be created.

First, we have argued there is a need for the EP to have access to classified information from and pertaining to the AFSJ agencies, as well as the possibility of holding confidential, off-the-record discussions with agency directors and other relevant stakeholders. Yet, the EP's existing institutional arrangements for oversight are not well suited to such functions because too many MEPs are involved and there is no precedent for smaller, confidential discussions with the agencies. We have cautioned against solving this problem by using a mechanism or body which simply has access to classified information regarding the AFSJ agencies without an accompanying mandate to use this information as part of oversight processes. It is worth reiterating that access to information by a body of parliament is not an end in itself: it must be a means to enable parliament to oversee particular agencies. For this reason, we were critical of the possible use of a special committee model for the AFSJ. The need to link access to classified information with a clear mandate for oversight is one of the main arguments in favour of creating a sub-committee.

A second argument in favour of the creation of a sub-committee is that the LIBE Committee might not have the time to engage in many of the proposed oversight functions outlined in chapter five. If the EP wishes to play an increased role in the oversight of the AFSJ agencies, the creation of a sub-committee could be a persuasive choice.

Third, a sub-committee would correspond with our earlier recommendation that the EP should have one body which has primary responsibility for all areas of parliamentary oversight of the AFSJ agencies. The sub-committee would be able to draw together its findings from various oversight functions and ongoing dialogue with the agencies, Council, Commission, JSBs and national parliaments. This would enable the EP to produce recommendations which can improve the work of the agencies, while also providing inputs to feed into other aspects of its own work. Notably, the insights of the sub-committee could help to ensure that the various roles which the EP plays vis-à-vis the AFSJ agencies are fully connected. For example, the EP's co-legislation functions would be closely informed by the findings and recommendations of its oversight work, and the sub-committee's oversight would also inform the use of the EP's budgetary powers.

Finally, the creation of a sub-committee would enable the EP to gradually develop more detailed knowledge and expertise on the AFSJ agencies. In our view, this is something which is currently lacking within the EP, and yet is crucial if the EP is to play a more active role in scrutinising the work of the AFSJ agencies.

Recommendation 21: The European Parliament should create a LIBE Sub-Committee for the oversight of the AFSJ agencies. The precise scope and content of the sub-committee's

mandate would be defined in accordance with the Parliament's rules of procedure but would be closely tied to the oversight functions given to the EP by new legislation on Europol, Eurojust and Frontex.

Strengthening cooperation between the European Parliament and national parliaments in the oversight of AFSJ agencies

The Lisbon Treaty specifically requires that national parliaments should be involved in the oversight of Europol and Eurojust. While the precise nature and scope of national parliaments' role differs between states, this study highlighted three main ways in which national parliaments already exercise some oversight of these agencies (see chapter three). Firstly, some national parliaments oversee the work of their own government's representatives at the Council and on agency management boards, i.e., they scrutinise national inputs to AFSJ agencies. Secondly, national parliaments can engage with AFSJ agencies directly by, for example, holding hearings with directors and other senior officials, and producing reports on the agencies. This engagement has typically been aimed at generating awareness of the agencies' work rather than any direct review or scrutiny of the agencies' activities. Moreover, parliaments are part of national systems of oversight which scrutinise actions taken by national authorities such as the police. The modalities of such oversight are the prerogative of national bodies, and it is beyond the scope of this study to issue recommendations in this regard. A third dimension of national parliamentary involvement in the oversight of the AFSJ agencies is cooperation with other parliaments and the EP (see chapter three); this will be our focus here.

In our view, the aims of inter-parliamentary cooperation should primarily focus on strategic matters rather than any specific operations of the AFSJ agencies. There are three areas in which inter-parliamentary cooperation could be particularly useful. Firstly, national parliaments and the EP could benefit from further discussions, as well as exchanges of information, experiences and good practices, on their oversight of national authorities' activities that are connected with the AFSJ agencies. For example, there is a clear need for further information on how, if at all, national parliaments and other relevant national oversight bodies (such as judicial bodies) oversee: (a) national contributions or inputs to the AFSJ agencies, such as information sent to AFSJ agencies; and (b) the actions of national authorities taken on the basis of information provided and/or operations coordinated by these bodies, such as arrests and questioning of persons suspected of involvement in serious criminal activity. National overseers could use such information to inform their own approaches to scrutinising activities of, for example, the police or border agencies, which have a nexus with the AFSJ agencies. Secondly, national parliaments and the EP could, insofar as national law would allow, exchange information about particular problems (within their jurisdictions) related to aforementioned activities of national authorities' activities that are linked to the work of AFSJ agencies. Finally, national parliaments and the EP could work together to evaluate whether new and existing regulations relating to the AFSJ agencies comply with the principles of subsidiarity and proportionality.

There are different views as to whether this cooperation should be institutionalised through some form of permanent inter-parliamentary body or whether it should proceed more informally through existing inter-parliamentary fora. For example, in its communication of December 2010, the Commission made proposals for involving national parliaments in the oversight of Europol. The Commission proposed setting up a joint or permanent inter-parliamentary forum in which both national and European members of parliament would be

represented, along the lines of Articles 9 and 10 of the Protocol on the Role of National Parliaments in the European Union. It furthermore suggested that such a forum could establish a sub-group to liaise directly with Europol. The forum would be able to invite the Europol director and it could meet regularly and establish a sub-group responsible for liaising with Europol directly. The Commission's proposals have received some support from national parliaments. However, the added value of the creation of such an inter-parliamentary forum has been questioned by a number of EU member states and national parliaments. All of the forms of cooperation discussed above could potentially take place within the context of existing forums for inter-parliamentary dialogue.

Perhaps more significantly, it is highly doubtful that a permanent body including representatives from all national parliaments could be workable. National parliaments' positions on, levels of interest in, and knowledge of AFSJ related matters vary greatly across the EU. It would therefore, be very challenging to reach consensus on issues such as an agenda for oversight, let alone on more substantive questions. A forum which included so many actors with different agendas could be unworkable and yet, it would be difficult to devise a formula for a smaller forum because it would inappropriate to exclude any national parliaments. In addition national parliaments have both different levels of access to information – from national authorities – and access to different types of information on the AFSJ agencies. They may therefore, be starting from very different positions in terms of their awareness of particular matters.

In view of these challenges, we do not recommend the establishment of a permanent forum for inter-parliamentary cooperation on oversight of the AFSJ agencies. It would be preferable for national parliaments and the EP to address the AFSJ agencies in the context of existing inter-parliamentary forums. These include joint meetings/hearings between the LIBE Committee and relevant committees of national parliaments, as well as the COSAC. In fact, the AFSJ, the political monitoring of Europol and the evaluation of Eurojust's activities have become regular items on the COSAC agenda. A majority of COSAC's members have supported the idea of COSAC debates on Europol and Eurojust to be preceded by a hearing of the directors of the respective agencies and experts. A potential role for COSAC in the political monitoring of JHA agencies is founded on Article 10 of TFEU Protocol No 1 on the role of national parliaments. This article stipulates that COSAC should promote the exchange of information and best practices between national parliaments and the European Parliament, including their special committees, and may organise inter-parliamentary conferences on specific topics. COSAC could continue to provide a useful venue for the types of cooperation discussed above.

Recommendation 22: Inter-parliamentary cooperation on the oversight of the AFSJ agencies should take place within the context of existing forums for cooperation between the European Parliament and national parliaments. The European Parliament does not need to establish a new permanent inter-parliamentary body.

CHAPTER 1. INTRODUCTION*

This study provides a comparative assessment of the oversight of intelligence agencies in European Union member states and other democracies. Its aim is to identify good practices that can inform the debate surrounding the development of parliamentary oversight of the EU Area of Freedom, Security and Justice (AFSJ) agencies and the Situation Centre (Sitcen). For the purposes of this study, we will use the term 'AFSJ bodies' to refer to the AFSJ agencies (Europol, Eurojust and Frontex) and Sitcen.[3]

In this introductory chapter we will outline the objectives, structure and rationale of the study. In the first section, we will explain our interpretation of the mandate for this study. On this basis, the second section will outline the aim and structure of the study. In section three we outline the methodology used for this study. This will be followed, in section four, by a brief discussion of the main rationale for parliamentary oversight of security sector agencies. The fifth section will define 'oversight', which is a key term that will be used throughout the study. The final section in this chapter will highlight the differences and similarities between national intelligence agencies and the EU's AFSJ bodies.

1.1. Mandate

The European Parliament's Directorate-General for Internal Policies mandated the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the European Union Institute (EUI) to carry out a study on '*parliamentary oversight of intelligence agencies in relevant EU Member States and other major democracies'.* This study was expected to '*identify democratic standards and best practice as well as a proper balance between the demands of secrecy and the need for scrutiny which can be used by the European Parliament (EP) when it sets up its own oversight body'.*[4] The tender did not specify which oversight body it was referring to or indeed, precisely what such a body would oversee. However, after consultation with the EP's Directorate General for Internal Policies, it was decided to interpret this mandate against the backdrop of four important trends and developments which have prompted a discussion on how the EP can strengthen oversight of the EU's AFSJ agencies, as well as Sitcen, which plays a role in the AFSJ.

(1) The Treaty of Lisbon gives the EP and national parliaments a mandate to strengthen their oversight of two AFSJ bodies: Europol and Eurojust.[5] It explicitly provides for the new regulations on Europol and Eurojust to include provisions on parliamentary 'scrutiny' (in the case of Europol) and 'evaluation' (in the case of Eurojust). Within the next two years, the Commission will put forward proposals for these regulations; the EP will have the opportunity to ensure that this legislation includes appropriate provisions on parliamentary

* The members of the project team would like to express their sincere gratitude to the national parliamentary liaison officers, members and staffers of national parliaments and non-parliamentary oversight bodies for providing detailed responses to the DCAF-EUI questionnaire. We are would also like to record our thanks to members and staffers of the European Parliament, as well as officials from the Council, Commission, Europol, Eurojust and the Joint Supervisory Bodies who provided valuable insights for this study. Furthermore, we would like to thank the members of the project advisory board and Suzana Anghel for their invaluable comments on earlier drafts of this study. Finally, we are very grateful for the support of DCAF colleagues, Ben Buckland, Gabriel Geisler and William McDermott, who provided excellent editorial assistance.

[3] This study will not address bodies within the Council or Commission that were not explicitly mentioned in the mandate. Accordingly, the Standing Committee on Operational Cooperation in Internal Security (COSI) will not be discussed. In addition, this study will not address the European Police College (CEPOL).

[4] European Parliament Directorate General Internal Policies (2010), p. 3.

[5] See Articles 85 and 88 of the TFEU.

oversight. In addition, the fact that the area of freedom, security and justice is now subject to the standard legislative procedure means that the EP is now better placed to ensure that new or revised legal frameworks for the AFSJ agencies include provisions on parliamentary oversight. Indeed, it has already done so in draft regulation on Frontex, which is currently under discussion.[6]

(2) The EP may have some opportunities to address the work of Sitcen, which performs a number of functions pertaining to internal security, because it is now part of the European External Action Service (EEAS). While the EEAS (and thus Sitcen) falls under the Common Foreign and Security Policy (CFSP), which is an intergovernmental policy area, the Treaty of Lisbon gives the EP some new powers in this area.

(3) There have been important developments in the area of access to information, which are intrinsically linked to strengthening oversight of the AFSJ bodies. In 2010, the EP and Commission concluded a new inter-institutional agreement, which significantly improves the EP's access to information from the Commission. In addition, the EP is currently considering the revision of the EU's legislation on access to information, as well as the possibility of a new inter-institutional agreement with the Council which would include provisions on parliamentary access to classified information. The trajectory of these ongoing discussions will have profound implications for the EP's oversight of AFSJ bodies.

(4) More generally, over the past decade, the EP has developed a growing interest in both national security agencies and AFSJ bodies. This has been evidenced by its strong interest in the development of the Frontex Regulation, and the Europol and Eurojust decisions, as well as two temporary committees that examined the activities of national security agencies and made important recommendations in regard to oversight.[7]

1.2. Aim and structure of the study

On the basis of this interpretation of the mandate, the primary aim of this study is to provide a comparative assessment of the oversight of intelligence agencies in European Union member states and other democracies, with the aim of identifying good practices that can inform the debate on strengthening oversight of the AFSJ bodies by the European Parliament. In order to identify practices which are relevant for the EP, we will first provide a clear picture regarding the current mandates and powers of the AFSJ bodies, as well as existing arrangements for the oversight of these bodies by the EP and other relevant actors. Accordingly, chapter two will provide an overview of the legal basis, mandate and current powers of Europol, Eurojust, Frontex and Sitcen, and will identify several areas of their work that might raise concerns from the point of view of oversight. Chapter three will critically analyse the EP's existing role and powers for overseeing the AFSJ bodies, as well as the scope of its access to information from these bodies. This chapter will also analyse the role of national parliaments in overseeing the AFSJ bodies, and the role of the Joint Supervisory Bodies of Europol and Eurojust in overseeing these agencies' processing and transferring of personal data. This assessment is necessary in order to identify any weaknesses in the EP's current oversight functions which could be addressed through the adoption of practices from national approaches to oversight of intelligence agencies. Chapter four will provide a detailed comparative assessment of how parliamentary and specialised non-parliamentary oversight is organised and carried out on a national level. This chapter will pay particular attention to access to information by parliamentary and

[6] See chapter two.
[7] These four developments will be further elaborated on in chapter three.

non-parliamentary oversight bodies. Finally, chapter five will draw together the analysis from the foregoing chapters in order to outline a series of options for consolidating and strengthening oversight of Europol, Eurojust, Frontex and Sitcen. This will include suggestions on improving the use of current oversight arrangements and proposals on developing new legal and institutional frameworks for parliamentary or specialised oversight of the AFSJ bodies.

1.3. Methodology

The methodology for this study has four main components. The first two were used to gather information on parliamentary and specialised oversight of intelligence agencies on a national level. We distributed a detailed questionnaire (see Annex C) to all national parliaments in EU member states and, where applicable, non-parliamentary oversight committees. The results are used extensively in chapter four and are presented in the tables that are included in this chapter. We also commissioned experts to draft case studies on the oversight of intelligence agencies in nine EU member states (Belgium, France, Germany, Hungary, Italy, the Netherlands, Spain, Sweden, and the United Kingdom), as well as Australia, Canada and the United States. The case studies of oversight on a national level (see Annex A) provide in-depth insights into national oversight institutions and practices. We selected these case studies to provide geographical and systemic diversity. They were drafted in accordance with standardised terms of reference in order to facilitate comparison. The questionnaires and expert case studies were supplemented by extensive desk research on national laws, the reports of oversight institutions, national jurisprudence, the jurisprudence of the European Court of Human Rights, reports of the Council of Europe's Venice Commission and relevant UN standards on the oversight of intelligence agencies.[8]

The third and fourth components of our methodology focused on generating information about the current role of the EP in the oversight of the EU's AFSJ bodies and, to a lesser extent, the role played by the joint supervisory bodies of Europol and Eurojust. We conducted interviews with almost 35 individuals from the EP (including both staffers and MEPs), the AFSJ bodies, the Joint Supervisory Bodies, the Commission and the Council. These interviews served to provide invaluable information on both the political context of the development of oversight arrangements for the AFSJ bodies and the current work of these bodies.[9] In addition, we commissioned a number of expert studies on role of the EP in the AFSJ, Europol and Eurojust, and a general overview of the EU's AFSJ architecture (see Annex B). Finally, we reviewed pertinent EU legislation, EP reports, agency documents and academic articles. The authors also benefited greatly from the inputs of the Project Advisory Board, which has reviewed and provided comments on this study, including the annexes.

[8] The authors provided substantial background research to assist with the drafting of United Nations Human Rights Council (17 May 2010), 'Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight', A/HRC/14/46, [hereafter, the 'UN compilation of good practice on the legal and institutional framework for intelligence agencies and their oversight'].

[9] Interviews were held in Brussels and The Hague from December 2010 to February 2011. Our interviewees were promised confidentiality in order to enable them to speak freely and to express views that may not necessarily be the official positions of their organisations. Accordingly, we will refer to interviewees by numbers.

1.4. Relevance of parliamentary oversight of security sector agencies

In seeking to strengthen its oversight of the EU's AFSJ bodies, the EP is building upon the internationally accepted norm that security sector agencies (i.e., the police, intelligence services, border agencies and the armed forces) should be subject to democratic oversight.[10] The rationale for democratic oversight can be distilled into two key points. Firstly, parliaments legislate on behalf of a population to give security sector agencies a mandate and powers to provide a public service. Parliaments should therefore hold these institutions to account for their fulfilment of their mandates and use of their powers. This should include ensuring security sector agencies' policies and practices are lawful, effective and respect the fundamental values of the societies they serve, including democracy and human rights.[11] Secondly, parliaments approve the allocation of public money to fund security providers and should therefore hold these organisations to account for the use of this money.[12] Parliaments do not necessarily assume these responsibilities alone; indeed, they frequently legislate to establish specialised non-parliamentary bodies to oversee particular security sector agencies.

1.5. Defining oversight

The term *oversight* is central to this study. For the purposes of this work, oversight refers to an actor scrutinising an organisation's (or individual's) activities with the aim of evaluating its compliance with particular criteria and on this basis, issuing recommendations or orders to the organisation concerned. Oversight may cover all aspects of an organisation's work or may be confined to specific areas, such as an organisation's finances, policies or use of personal data. Equally, overseers may scrutinise these activities in accordance with very general criteria or may focus on, inter alia, their compliance with the law or effectiveness. Oversight is closely tied to the notion of 'accountability' as oversight processes may contribute to holding an organisation or individual to account; however, being overseen is not necessarily tantamount to being held accountable. Indeed, the aims of oversight are often broader than holding actors to account; for example, oversight contributes to improving the performance of a given organisation, informing the public about an organisation's activities, and building public confidence. For the purposes of this study, oversight is not 'time sensitive', meaning that a body may oversee a given activity at any point from its planning, to ongoing implementation or once it is completed. Accordingly, oversight is a catchall term which can encompass processes such as *monitoring, evaluation*, *scrutiny* and *review*—at various points in this study oversight will be used interchangeably with these terms. Oversight should, however, be seen as distinct from concepts such as 'management' and 'control', which imply direct involvement in decision making regarding an organisation's policies or practices. Many of the bodies which are involved in oversight of intelligence agencies also manage or control these bodies in various ways.

[10] See, for example, OECD DAC Guidelines and Reference Series 2005.
[11] See, for example, Parliamentary Assembly of the Council of Europe 2005; European Commission for Democracy Through Law (2007), *Report on the Democratic Oversight of the Security Services*, adopted by the Venice Commission at its 71st plenary meeting, Venice, 1–2 June 2007 [hereafter the Venice Commission Report], p. 18.
[12] See, for example, the Venice Commission Report, p. 9, and the UN compilation of good practice on the legal and institutional framework for intelligence agencies and their oversight.

It should be stressed that access to information, and particularly classified information held by and pertaining to organisations being overseen, is another key concept in this study. Access to information is an integral dimension of oversight because without such information, it is extremely difficult to scrutinise the work of any organisation.

In a democratic polity, a range of actors are involved in the oversight of intelligence agencies, including: parliament, autonomous bodies, political executives, judicial bodies, the media and civil society, and internal mechanisms within intelligence agencies. While each of these actors fulfil important and often mutually complimentary oversight functions, this study will, in line with the mandate outlined in the tender, focus on the oversight of intelligence agencies by parliaments and autonomous oversight bodies. The term '*specialised oversight body/committee*' will be used (interchangeably with oversight body) to refer to: (a) parliamentary (sub-) committees responsible for the oversight of intelligence agencies, and (b) autonomous non-parliamentary bodies that are responsible for the oversight of these agencies, and not part of the executive, parliament or the agencies they oversee.

1.6. National intelligence agencies v. the EU's AFSJ bodies

Broadly speaking, the role of the AFSJ bodies is to facilitate, coordinate and strengthen cooperation between national authorities with the aim of promoting security and justice within the EU. This study will focus on three key agencies: Europol (which performs this role with respect to law enforcement), Frontex (which focuses on improving the management of the EU's external borders) and Eurojust (which focuses on judicial cooperation), as well as the Situation Centre (which, in the realm of internal security, provides threat assessments to relevant decision makers—see chapter two).

In view of the fact the EP is interested in strengthening oversight of these bodies, a mandate to study and draw lessons from the oversight of national 'intelligence agencies' may appear to be an unusual choice. The term 'intelligence agency' generally refers to a state body that collects, analyses and disseminates information—on threats to national security or other national interests—to policy-makers and other executive bodies.[13] Intelligence agencies may perform these 'intelligence functions' exclusively outside of their state's territorial jurisdiction (e.g., the UK's Secret Intelligence Service), exclusively within their state's territory[14] (e.g., Germany's Federal Office for the Protection of the Constitution), or both inside and outside their territory (e.g., the Dutch General Intelligence Service or AIVD). In a few states (e.g., in Sweden and Denmark), these bodies may also possess police powers and are therefore sometimes called 'police security services'. However, arguably the defining feature of the national intelligence agencies is their power to use what are known as 'special powers' to collect information, such as the powers to intercept communications, conduct covert surveillance, use secret informants, and even enter dwellings surreptitiously. Please note that for reasons of consistency, we will use the term *'intelligence agency'* to refer to all of the aforementioned bodies, e.g., organisations which are variously labelled as 'security services', 'domestic intelligence agencies' or 'intelligence services'. This study will not, however, address military intelligence agencies or agencies whose mandates focus exclusively on foreign intelligence, i.e., matters outside of their state's territory. The reason for this is that this study focuses on the EU's AFSJ, which relates to 'civilian' internal security—it is beyond the scope of this study to scrutinize the

[13] See, for example, Gill and Phythian (2006), pp. 1–19.

oversight of national agencies that are not civilian bodies or do not play a role in internal security.

The AFSJ bodies do not possess the powers discussed in the previous paragraph and, when juxtaposed alongside this description, it is evident that the EU's AFSJ bodies are not intelligence agencies in the way that they are conceptualised at the national level. Indeed, the AFSJ bodies might be seen as more closely analogous to their counterparts of national level police services (Europol), border agencies/border police (Frontex), judges and prosecutors (Eurojust) and joint analysis or fusion centres (Sitcen). Nevertheless, the AFSJ bodies perform the aforementioned 'intelligence functions' of national intelligence agencies, albeit not necessarily in the same way or for the same purpose. Notably, they collect (though without recourse to the abovementioned special powers), analyse and disseminate information to a range of decision makers. Another important similarity between the AFSJ bodies and national intelligence agencies is that they too receive, produce and disseminate classified information. This has important implications for oversight because overseers need access to classified information in order to scrutinise the work of agencies whose activities are 'classified' and/or entail the use of classified information—this is an area in which the EP can learn much from national systems of oversight.

We should nevertheless remain cautious about the 'portability' of oversight models and practices from the national to the EU level given that national overseers and the EP scrutinise agencies with very different mandates and powers. Oversight has to be understood in the context of the organisations which are being overseen. And, as we have noted, there are major differences between national agencies that primarily exist to inform the executive about threats to national security and AFSJ bodies that exist to coordinate, support and inform relevant actors in 27 states, across fields ranging from law enforcement to border management. The AFSJ do not only have multiple 'customers' for their outputs and their work is founded upon the inputs of multiple contributors. These contributors are national authorities in 27 different jurisdictions, all of which have their own legal framework, mandate and oversight arrangements.

In addition to differences between national agencies and AFSJ bodies, the EU has manifestly different constitutional arrangements than states. We shall highlight just a few of these differences that have important implications for the transferability of practices from the national to the EU level. First, while states have a single executive branch that is responsible for intelligence agencies, and accountable to parliament in this regard, the EU has a split executive with the Council and Commission both having responsibility in the ASFJ. Second, national executives generally exercise much more direct control of national intelligence agencies than the Commission and Council in regard to AFSJ bodies. This has important implications for parliamentary oversight because at a national level, national executives are more clearly accountable for the actions of intelligence agencies. Finally, national intelligence agencies may be overseen by one parliament but the AFSJ bodies are subject to oversight by the EP and multiple national parliaments that have different powers and approaches to oversight. We should remain mindful of these differences when considering transplanting national practices to the EU level.

[14] Please note that the label 'security service' normally refers to public bodies which perform the aforementioned functions exclusively within their state's territory (e.g., the UK's Security Service). This term is often used interchangeably with the label 'domestic intelligence service/agency'.

CHAPTER 2. THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE BODIES

This chapter outlines the legal basis, mandate and current powers of the AFSJ bodies as of April 2011 in order to provide an overview of the tasks and powers of these bodies which are or could be subject to oversight. The AFSJ bodies' 'operational powers' primarily consist of two elements: 1) coordinating and supporting the work of national agencies; and 2) processing, storing and transferring personal data. As we will see in chapter four, oversight bodies on the national level are predominantly concerned with overseeing the correct use of special powers by national agencies. Therefore, we will assess whether the AFSJ bodies have any special powers that need to be overseen. Another dimension of the work of intelligence agencies on the national level is the sharing of information with each other, and with third countries. This sharing of information, particularly the sharing of personal data, can give rise to human rights concerns because recipients may undertake actions on the basis of this information that might result in the limitation of human rights. Consequently, we also describe in this chapter how, and with whom, the AFSJ bodies are sharing information.

2.1. Europol

2.1.1. Legal basis and main tasks

The Europol Convention of 26 July 1995[15] established Europol as an international organisation in 1995 and entered into force on 1 October 1998. In order to provide Europol with a more flexible legal basis[16], its legal basis was changed into a Council Decision that was formally adopted by the JHA Council of 6 April 2009.[17] With the new Decision, Europol was changed into an EU Agency. Europol is likely to be given again a new legal basis within the next three years because Article 88 of the Treaty of Lisbon provides that the European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Europol's structure, operation, field of action and tasks. In response, the European Commission has stated, in its Action Plan Implementing the Stockholm Programme, that a Proposal for a Regulation on Europol will be put forward in 2013.[18]

Europol's formal objective as the EU's law enforcement agency is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.

Its six principal tasks are: (a) to collect, store, process, analyse and exchange information and intelligence; (b) to notify the Member States without delay of information concerning them and of any connections identified between criminal offences; (c) to aid investigations in the Member States, in particular by forwarding all relevant information to the national units; (d) to ask the competent authorities of the Member States concerned to initiate, conduct or coordinate investigations, and to suggest the setting up of joint investigation teams in specific cases; (e) to provide intelligence and analytical support to Member States in connection with major international events; and (f) to prepare threat assessments,

[15] OJ C 316 of 27.11.1995.
[16] European Commission 20 December 2006, p. 2.
[17] Council Decision of 6 April 2009 establishing the European Police Office (Europol) [hereafter 'Europol Decision'].
[18] COM (2010) 171 of 20.4.2010.

strategic analyses and general situation reports relating to its objective, including organised crime threat assessments.[19]

Europol's two main 'strategic intelligence' products are the EU Terrorism Situation and Trend Reports (TESAT) and the European Organised Crime Threat Assessment (OCTA)[20]. The OCTA is especially important since it is the document on which the Council of the EU bases its priorities and recommendations for the fight against organised crime in Europe.[21] This analytical report is produced by the strategic analysts in Europol's Analysis and Knowledge Unit, which draws on contributions from the Analytical Work Files,[22] Europol's SCAN Team[23] and external partners, including Eurojust and third countries. The full version of OCTA is classified as 'restricted'[24] and therefore not generally available to MEP's, but there is a public version of the document available.

Additional tasks include: (a) developing specialist knowledge of the investigative procedures of the competent authorities of the Member States and to provide advice on investigations; and (b) providing strategic intelligence to assist and promote the efficient and effective use of the resources available at the national and Union levels for operational activities and the support of such activities. In 2010, Europol sent a mobile office with analysts to the Member States in order to provide them with on-the-spot assistance to analyse information on 31 occasions.[25]

Since March 2007, Europol has had a mandate to participate in a 'support capacity' in the activities of 'joint investigation teams' (JITs).[26] Joint investigation teams consist of judicial and police authorities of at least two Member states, which are responsible for carrying out criminal investigations into specific matters for a limited period of time. In 2010, Europol participated in 7 JIT's and it supported other JIT's as well.[27] Within the limits provided for by the law of the Member States where the JIT operates, Europol officials are allowed to assist in 'all' activities and exchange information with all the members. In practice, this means that Europol's assistance is limited to giving expert advice in setting up the JIT, and providing analytical support during the investigations. Investigators are able to share information on the spot without formal requests. Even as part of a JIT, Europol cannot take part in any coercive measures.[28] Europol's staff also do not have immunity when they participate in joint investigation teams.[29]

In 2009, Europol received another task after the EU-US agreement on the processing and transfer of financial messaging data for purposes of the US Terrorist Finance Tracking Programme (TFTP Agreement) was adopted.[30] This agreement regulates the transfer of bulk data from the 'Designated Provider' of international financial payment messaging services in Europe to US authorities (US Department of the Treasury) in order to support the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. Europol was given the task of verifying whether requests from the US to obtain financial

[19] Article 5 Europol Decision.
[20] Europol also produces two specific organised crime threat assessments on Russia (ROCTA) and on West Africa (OCTA-WA).
[21] In 2013, OCTA will be superseded by the Serious and Organised Crime Threat Assessment (SOCTA).
[22] Analytical Work Files are files in which Europol stores data on criminal offences for the purpose of analysis (see below).
[23] The Europol Scanning, Analysis & Notification (SCAN) System provides national competent authorities with strategic early warning notices regarding new Organised Crime (OC) threats.
[24] Article 1.2.2 of Annex II of the 2010 Framework Agreement between the Commission and the European Parliament defines EU Classified information (EUCI) as any information and material classified as 'TRÈS SECRET UE/EU TOP SECRET', 'SECRET UE', 'CONFIDENTIEL UE' or 'RESTREINT UE'. OJ L304/47, 20 November 2010. The 'restreint ue' classification is applied to information and material the unauthorised disclosure of which could harm the essential interests of the Union or of one or more of its Member States.
[25] Europol 20 May 2011, p. 28.
[26] See in detail: The Management Board of Europol 29 March 2007.
[27] Europol 20 May 2011, p. 41.
[28] Article 6 of the Europol Decision.
[29] Council of the European Union 15 May 2009.
[30] European Union and the United States of America 27 July 2010.

messaging data stored in the EU by the Designated Provider comply with a number of data protection related criteria that were outlined in Article 4.2 of the TFTP agreement. After this verification procedure, Europol is required to notify the designated provider that it has verified these requests; the requests then have binding legal effect in the US and the EU. MEPs, national parliamentarians and national data protection authorities initially voiced concern over the secrecy surrounding the implementation of this agreement.[31] When the TFTP Agreement entered into force on 1 August 2010, Europol classified the handling of US requests at the level of 'RESTREINT UE/EU RESTRICTED', partly in view of technical limitations in the secure information exchange system between Europol and the US. After a leak of a document describing the 'technical modalities' of how Europol would exercise its verification role, the US demanded that Europol classify these requests as 'SECRET UE/EU Secret', which it has done since November 2010.[32] Later, the Europol Joint Supervisory Body (see chapter three) and several members of the European Parliament criticised Europol for agreeing to the requests from the US on the basis of too little information.[33] It is interesting to note that Europol has received so much criticism about a task it never asked for and which is not part of its core mandate.

2.1.2. Powers

Europol currently has 698 personnel, including 100 analysts and 129 seconded liaison officers from the competent national agencies at Europol.[34] Europol also hosts liaison officers from 10 third countries and organisations who work together with Europol on the basis of cooperation agreements.[35] These liaison officers are subject to the national law of the seconding Member States and they are sent to Europol to represent the interests of the state within Europol.[36] In 2010, Europol's total budget was 92.8 million euro.

From the description of its tasks, it is clear that Europol performs almost exclusively coordination and support functions. It shall 'support and strengthen' operational actions of the Member States, which predominantly means that it can make suggestions, provide analytical support or forward information to the Member States. It should be stressed that Europol officials do not have coercive powers, which are usually given to national intelligence agencies. Notably, Europol personnel cannot conduct searches of property, intercept communications, or conduct surveillance; nor can they question, arrest or detain suspects.[37] Equally, Europol cannot ask member states' authorities to use such powers against a person. Finally, Europol doesn't have its own informants; information from private persons may only be processed by Europol if it is received via a national unit or via the contact point of a third state with which Europol has concluded a cooperation agreement.[38]

Since its inception, questions have been raised as to whether Europol will eventually be an 'FBI style' international police force which has coercive powers in dealing with serious crime with a cross-border element in Europe.[39] This concern returned with every amendment to the original Europol Convention[40] and it is likely to come up again in the run-up to the adoption of a Europol Regulation. In this context, it is important to note that Article 88 (3) of the TFEU clearly states that 'any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State or States whose territory is concerned. The application of coercive measures shall be the exclusive responsibility of the competent national authorities'. Equally, several interviewees pointed out that it is very

[31] *EU Observer* 28 February 2011.
[32] Europol 8 April 2011, p. 6.
[33] European Parliament LIBE Committee 16 March 2011.
[34] Europol 20 May 2011, p. 9.
[35] Ibid., p. 12.
[36] Article 9 Europol Decision.
[37] De Moor and Vermeulen, in Annex B of this volume; De Witte and Rijpma, in Annex B of this volume.
[38] Article 25.4 Europol Decision.
[39] See, for instance: Ellerman 2002.
[40] See, for instance: Hayes 2002; JUSTICE September 2002.

unlikely that Member States will ever allow a European Agency to use coercive powers on their territory, against their citizens.[41]

Europol relies predominantly[42] on Member States when it comes to 'collecting' intelligence on serious crimes.[43] Europol may of course directly retrieve and process data, including personal data, from publicly available 'open sources' such as media and public data and commercial intelligence providers.[44] The only other two sources from which it receives intelligence seem to be third states and international organisations.

Europol National Units in the Member States and liaison officers have the right to put personal data into the Europol Information System; the primary purpose of this system is to collate data contributed by different Member States and third parties with the aim of identifying patterns. This data relates to two categories of persons. The first category consists of those persons that are suspected of having committed a criminal offence in respect of which Europol is competent or who have been convicted of such an offence. Member States can lower this initial threshold of inserting information by also adding information on a second category of persons regarding whom there are 'factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent'.[45] Article 13.6 of the Europol Decision states that 'competent authorities designated to that effect by the Member States' can also provide intelligence to Europol, which could include state security and/or civilian and military intelligence agencies. In practice, however, this rarely happens. The bulk of data consists of criminal intelligence coming from national police authorities.[46] In December 2010, the EIS contained information about more than 35,000 persons.[47] It is important to note that liaison officers assist in the exchange of information with liaison officers of other Member States under their responsibility in accordance with national law. Such bilateral exchanges may also cover crimes which fall outside the competence of Europol, as far as allowed by national law.[48] According to one observer, it is 'tragic' that 'four fifths of the information exchanged by national liaison officers stationed at Europol is exchanged without actually going through Europol, and hence without being stored in Europol's information systems and without being accessible to Member States other than those directly involved'.[49]

The Analysis Work Files (AWFs) also contain sensitive data on potential witnesses, victims, informants, and contacts and associates of a suspected criminal. This data can reveal racial or ethnic origin, and information relating to political opinions, religious or philosophical beliefs, trade union membership, health or the sex life of a person. Only Member States with a need to know have access to a case-related AWF. If an analysis is of a general nature and of a strategic type, all Member States, through liaison officers and/or experts, shall be fully cognizant of the findings thereof.[50]

Europol's dependence on criminal intelligence from national law enforcement agencies is often regarded as its biggest weakness.[51] In many EU states, national police agencies still remain to be convinced of the added value of Europol and have concerns about the further dissemination of information they share with Europol. In addition, national police forces may decline to provide information, if doing so would, for instance, harm national security

[41] Interviews 18, 19.
[42] Interviews 15, 18, 19.
[43] Article 5.1 Europol Decision. Article 14.6 spells out how the state can determine the conditions for the handling of the data it sends to Europol.
[44] Article 25.4 Europol Decision.
[45] Article 12.1 Europol Decision.
[46] Interview 32.
[47] Europol 20 May 2011, p. 14.
[48] Article 9.3.D Europol Decision.
[49] De Moor and Vermeulen in Annex B of this volume.
[50] Article 14 Europol Decision.
[51] See: Fägersten 2010.

interests or jeopardise the success of ongoing investigations and/or the safety of individuals.[52] Consequently, they do not necessarily share information through Europol and cannot be compelled to do so. Indeed, bilateral and informal exchanges of information and data is still the preferred *modus operandi* for many agencies, as much less stringent data protection regulations apply when information is exchanged through bilateral channels rather than through Europol. [53]

2.1.3. Relationships with third parties

2.1.3.1. Other EU agencies

Europol and Eurojust concluded a first operational agreement in 2004, which was revised in 2009. The main purpose of this agreement is 'to make the investigation and prosecution of crimes within the [agencies'] respective mandates as efficient as possible and to avoid duplication of effort wherever possible'. This agreement provides for the exchange of operational, strategic or technical information, and even personal data. In 2008, a secure communication link was established to facilitate the exchange of information between Europol and Eurojust. Europol and Eurojust have also agreed on a table of equivalence to exchange classified information above the level of 'restricted'. In addition to information sharing, a staff exchange programme between Europol and Eurojust started in 2011. Europol and Eurojust write joint press releases[54] and joint documents, for instance, on judicial-police cooperation in operational cases for the EU's Standing Committee on operation cooperation on internal security (COSI).[55] Point III.2.3 of the Hague Programme ('Police cooperation'), Annex I of the Presidency Conclusions of the Brussels European Council (4/5 November 2004),[56] provides that Eurojust and Europol *'…should report annually to the Council on their common experiences and about specific results…'*. These reports are not sent to the EP.

Europol has had a cooperation agreement with Frontex since 2008.[57] This agreement is of a strategic nature and allows only for the exchange of strategic and technical information,[58] explicitly excluding the exchange of personal data. This includes, for instance, information on new methods used in committing offences, routes and changes in routes used by smugglers, threat assessments, risk analysis and crime situation reports. Technical information includes police working methods as well as investigative procedures and results, training methods, criminal intelligence analytical methods and identification of law enforcement expertise. Experts of Eurojust and Frontex may be invited to the analysis of work files, provided that the conditions of Article 14.8 of the Europol Decision are fulfilled. Europol and Frontex have also produced joint reports to the Council.[59]

Europol has had a strategic agreement in the form of a memorandum of understanding with Sitcen since 2005 (see below). It is not available to the European Parliament.

2.1.3.2. Agreements with third states and organisations

Europol can conclude cooperation agreements with third states and international organisations. Such agreements may concern the exchange of operational, strategic or

[52] Article 8.5 Europol Decision.
[53] Interviews 13, 18, 19, 26, 28 and 32.
[54] See, for example: Eurojust-Europol Joint Press Release 8 February 2011.
[55] Council Doc. 9387/11 (*not public)*.
[56] Council of the European Union 13 December 2004.
[57] See: Europol 28 March 2008.
[58] Ibid., Article 2.
[59] Ibid.; Council of the European Union 15 February 2008.

technical information, including personal data and classified information.[60] Agreements with third states and organisations may be concluded only after receiving the approval of the Council, which has to consult the Europol Management Board and, as far as it concerns the exchange of personal data, obtain the opinion of the Joint Supervisory Body via the Management Board (see below).

Europol currently has operational agreements with Interpol, Australia, Canada, Croatia, Iceland, Norway, Switzerland and the United States, including a 'supplemental agreement' on exchange of personal data with the US. It has strategic agreements with Albania, Bosnia & Herzegovina, Colombia, the Former Yugoslav Republic of Macedonia, Moldova, Russia, Turkey, Serbia, Montenegro, Ukraine and the United Nations Office on Drugs and Crime (UNODC) and the World Customs Organisation.

Before the adoption of the Lisbon Treaty, the European Parliament rejected the draft Council decision determining the list of third States and organisations with which Europol could conclude agreements.[61] MEP's also criticised the agreement that was concluded in 2001 between Europol and the US. This agreement was supplemented by another agreement on 20 December 2002 to allow the exchange of personal data. Members of the European Parliament expressed concern at the time about these agreements since the US did not afford an equal level of data protection to its citizens and was, furthermore, unable to provide a list of all the agencies that could request or have access to data provided by Europol. One observer noticed that this measure was being 'rushed through' and provided 'no realistic opportunity for national and European parliaments or civil society to subject the proposal to proper scrutiny.[62] The new Europol Regulation to be adopted is likely to address this issue.

2.2. Eurojust

2.2.1. Legal basis and main tasks

The decision to create Eurojust was taken in October 1999 at the Council in Tampere in order to improve, simplify and speed up the coordination and cooperation between the judicial authorities of the Member States in investigations and prosecutions of serious organised crime cases.[63] The Nice Treaty of 26 February 2001[64] provided an explicit treaty basis for a new EU agency. This was given effect by the Eurojust Council Decision of February 2002, which finally established Eurojust as a 'body of the Union' with legal personality.[65] Eurojust's Council Decision was subsequently amended in 2003[66] and 2008.[67] The new Eurojust Decision strengthened Eurojust's operational capabilities and enhanced its relationship with third parties; it entered into force on 4 of June 2009.[68] The Treaty of Lisbon (Article 85) provides for the development of a new legal basis for Eurojust, in accordance with the ordinary legislative procedure. The European Parliament and the Council, by means of legislation adopted in accordance with the ordinary legislative procedure, shall determine Eurojust's structure, operation, field of action and tasks in the future, which might include, according to Article 85 of the TFEU: (a) the initiation of criminal investigations, as well as proposing the initiation of prosecutions conducted by competent national authorities, particularly those relating to offences against the financial

[60] See in detail Articles 23–24 Europol Decision.
[61] See, for instance: European Parliament 16 November 2009.
[62] Statewatch 20 December 2002. See also: Peers 2002.
[63] European Parliament 1999.
[64] Treaty of Nice, OJ C 80 of 10.3.2001; Article 31 (2) of the TFEU.
[65] Article 1 EJ Council Decision.
[66] Council Decision 18 June 2003.
[67] Council Decision 16 December 2008.
[68] See De Moor and Vermeulen in Annex B of this volume.

interests of the Union; (b) the coordination of investigations and prosecutions referred to in point (a); and (c) the strengthening of judicial cooperation, including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network. The European Commission has stated in its Action Plan Implementing the Stockholm Programme that a Proposal for a Regulation on Eurojust will be brought forward in 2012.[69]

The objectives of Eurojust are to 'stimulate and improve' the coordination of investigations and prosecutions in the Member States by facilitating the execution of international mutual legal assistance and the implementation of extradition requests, or by any other form of support to the competent authorities of the Member States in order to render their investigations and prosecutions more effective.[70] In 2009, Eurojust held 141 coordination meetings, which dealt with 1,222 'standard' cases and 150 'complex cases'. Forty-five per cent of the cases dealt with fraud, 17% with drug trafficking, 14% with terrorism, 6% with murder and 5% with trafficking in human beings. At these coordination meetings, representatives of judicial and police authorities of the involved countries can meet each other and discuss the state of proceedings, verify the requirements for mutual legal assistance or decide upon the strategy on how to solve a case (who prosecutes what where). Eurojust financially supports these meetings by paying the travel, accommodation and translation costs of these meetings.

Each member state sends a prosecutor, judge or 'police officer of equivalent competence' who has his/her regular place of work at the seat of Eurojust.[71] Eurojust can act through these national members[72] or as a 'college'. The College consists of all the national members and each national member has one vote.[73] Eurojust will act as a college in three main situations: when a Member State requests that a case is dealt with by Eurojust, when the case involves investigations or prosecutions which have repercussions at the Union level or which might affect Member States other than those directly concerned, or when a general question relating to the achievement of its objectives is involved. Under the current legal framework, Eurojust's mandate and powers are clearly focussed on coordination, the provision of advice and support. Eurojust does not prosecute cases and does not have any enforcement powers of its own.

2.2.2. Powers

Eurojust consists of the College composed of 27 National Members. They are judges, prosecutors or police officers with equivalent powers (in line with the legal system of the Member State). Besides the College, there are approximately 140 staff members, including administrative staff and the Case Management Team that are paid by the EU, as well as the deputies, secretaries and seconded national experts that assist the National Members of the College. EU officials may also be seconded to Eurojust as temporary staff. In 2010, Eurojust had a budget of 30.2 million euro. The budget does not cover the salaries of national members.

Initially, the powers of the national members were defined on the basis of national law, which contributed to both a lack of clarity and substantial discrepancies regarding the extent of the powers of Eurojust in Member States.[74] The 2008 amendment to Eurojust's Decision made it clear, however, that all Member States in their capacity as competent national authorities are entitled to receive, transmit, facilitate, follow up and provide supplementary information in relation to the execution of requests for, and decisions on,

[69] European Commission 2010, p. 18.
[70] Council of the European Union 28 February 2002, Consolidated Eurojust Decision [hereafter Consolidated EJ Decision], Article 3.
[71] Article 2 Consolidated EJ Decision.
[72] Ibid., Article 6.
[73] Ibid., Article 10.
[74] Mitsilegas 2009, p. 197.

judicial cooperation, including regarding instruments giving effect to the principle of mutual recognition.[75] All the Member States had to implement this amendment by June 2011.

Eurojust, both acting as a College and through its national members, may ask (but not compel) the competent authorities in Member States to: (i) undertake an investigation or prosecution of specific acts; (ii) accept that a specific member state may be in a better position to undertake an investigation or to prosecute specific acts; (iii) coordinate between the competent authorities of the Member States concerned; (iv) set up a joint investigation team; (v) provide it with any information that is necessary to carry out its tasks; (vi) take special investigative measures; and (vii) take any other measure justified for the investigation or prosecution.

Eurojust created an EU-wide judicial database called the Case Management System (CMS), which contains sensitive information on all investigations and prosecutions reported to Eurojust. The rapporteur of the European Parliament on the revision of the Eurojust Decision stated that it is important for Eurojust 'to maintain closed lists of data (on persons who are the subjects of a criminal investigation) and data which should be allowed being processed by Eurojust'.[76] National judicial authorities also have access to the CMS of Eurojust through the Eurojust national coordination system.

2.2.3. Relations with third parties

2.2.3.1. Other EU agencies

Eurojust shall establish and maintain 'cooperative relations' with Europol, Frontex and the Council, in particular its Situation Centre, according to Article 26.1 of the Eurojust Decision. As was noted above, Eurojust has concluded a cooperation agreement with Europol (see above). Eurojust will commence negotiations for cooperation with Frontex in 2011.[77]

It is not known whether a working agreement or arrangement exists between Eurojust and Sitcen. Article 26.3 of the Council Decision just stipulates that Eurojust may directly receive and use information from an entity included in Section 26.1, 'in so far as this is necessary for the legitimate performance of its tasks', and it may directly transmit information, including personal data, to these entitites 'in so far as this is necessary for the legitimate performance of the recipient's tasks and in accordance with the rules on data protection provided in this Decision'. This wording suggests at least that any arrangement between Sitcen and Eurojust would not involve the sending of personal data from Eurojust to Sitcen, since Sitcen does not have a mandate to process personal data. Such agreements or working arrangements may only be concluded after consultation by Eurojust with the Joint Supervisory Body (see chapter three).

2.2.3.2. Third states and organisations

Like Europol, Eurojust may conclude agreements with third states and international organisations.[78] Such agreements facilitate the coordination of investigations and prosecutions in other countries. Eurojust has concluded agreements with Norway, Iceland, Romania, the United States of America, Croatia, the Former Yugoslav Republic of Macedonia and Switzerland. It has concluded further memoranda of understanding with UNODC, CEPOL, the European Judicial Training Network and the Iberoamerican Network of

[75] De Moor and Vermeulen in Annex B of this volume.
[76] LIBE Committee 7 July 2008.
[77] Eurojust 2011, p. 16.
[78] Article 26 Consolidated EJ Decision.

International Legal Cooperation.[79] In 2010, it continued the negotiation of an agreement with the Russian Federation, as well as with Moldova, Liechtenstein, Albania, Cape Verde, Montenegro, Serbia, Bosnia and Herzegovina and Israel.[80] Eurojust may only conclude the agreements after approval by the Council, acting by qualified majority. Such agreements may include sharing of personal data. Eurojust has to inform the Council of any plans it has for entering into any such negotiations and the Council may draw any conclusions it deems appropriate.[81]

2.3. Frontex

2.3.1. Legal basis and mandate

In contrast to Europol and Eurojust, Frontex was created by a Council Regulation[82] in order to improve the 'integrated management' of the external borders of the European Union by coordinating the operational cooperation of EU Member States, Schengen Associated Countries and other partners. The Agency became operational in October 2005. Currently, a new Regulation is in the final stages of being developed; this section addresses Frontex's legal framework as it stands in April 2011 when the new regulation was not yet adopted.[83]

Frontex's responsibilities fall into two principal categories. The first one is providing technical and informational assistance to Member States by training of national border guards, following up on the development of research relevant for the control and surveillance of external borders and delivering risk analyses to Member States. The agency's tasks as regards risk analysis are to 'develop and apply a common integrated risk analysis model' to 'prepare both general and tailored risk analyses to be submitted to the Council and the Commission' and to 'incorporate the results of' its risk analysis model in its development of a training curriculum for border guards.[84]

The second responsibility is the coordination of operational activities between Member States in the field of management of external borders. This includes assisting Member States when they need increased technical and operational assistance at external borders; providing Member States with the necessary support in organising joint return operations; and deploying Rapid Border Intervention Teams to Member States in accordance with Regulation (EC) No 863/2007.[85]

2.3.2. Powers

Currently, 286 people are working for Frontex, of which 73 persons are seconded national experts (SNE). Frontex seconded officers come from a national, regional or local public administration or an intergovernmental organisation and must possess a security clearance. These SNE's assist the Frontex staff, including by participating in Frontex missions. SNEs 'acting alone' will not exercise any of the responsibilities that belong to Frontex by virtue of

[79] See Eurojust's website, 'Agreements with third parties/countries', available at (http://www.eurojust.europa.eu/official_documents/eju_agreements.htm).
[80] Eurojust 2010, pp. 12–13; adopted by the College on 8 December 2009.
[81] Consolidated EJ Decision, para. 26a.
[82] Council Regulation No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operations Cooperation at the External Borders of the Member States of the European Union [hereafter 'Frontex Regulation'].
[83] For an overview on the positions of the Council, Commission and LIBE Committee on the proposed amendments to the new Regulation in March 2011, see Council of the European Union 25 March 2011.
[84] Article 4, Reg. 2007/2004.
[85] Article 2.1 Frontex Regulation; Regulation (EC) No 863/2007 of the European Parliament and of the Council of 11 July 2007 establishing a mechanism for the creation of Rapid Border Intervention Teams and amending Council Regulation (EC) No 2007/2004 ('Rabit Regulation').

the powers conferred upon it, unless the Executive Directors have explicitly empowered the SNE in writing.[86] The agency's budget in 2010 was 92.8 million euro.[87]

Frontex is first and foremost a coordination agency whose task is to enable and facilitate the exchange of operational information between the border guards of Member States and the pooling of technical and human assets.[88] Frontex has a situation centre which gathers and collates information from partner countries, within and beyond the EU's borders, as well as from open sources such as academic publications and the press, in order to monitor the day-to-day situation at the EU's external borders. Member States provide Frontex with information on illegal border crossings, illegal stays, refusals of entry, asylum applications, facilitation, false documents and returns of illegal stayers. Until now, Frontex has not had the opportunity to process personal data.

It is important to note that Frontex does not have its own border guards. All officials that participate in a border operation or a 'returns operation' remain national border guards who exercise their tasks in accordance with their national laws.[89] Members of Rapid Border Intervention Teams (RABIT) are paid by the Member States but receive a daily subsistence allowance from Frontex. These border guards may only perform tasks and exercise powers for border checks or border surveillance in accordance with the Schengen Borders Code.[90] While performing their tasks and exercising their powers, members of the teams may carry service weapons, ammunition and equipment as authorised according to the home Member State's national law. However, the host Member State may prohibit the carrying of certain service weapons, ammunition and equipment, provided that its own legislation applies the same prohibition to its own border guards. All actions of a Frontex-coordinated operation happen, as a general rule, in the presence of border guards of the host Member State. The host state's command officer has the operational responsibility for the team and has the power to give instructions to his assigned team. Frontex also appoints one or more Coordinating Officers who may express the views of the Agency on the instructions of the host state, which is obliged to take these views into consideration.[91]

2.3.3. Relations with third parties

2.3.3.1. Other EU agencies

Frontex has a cooperation agreement with Europol (see above), which authorises the exchange of classified information at a 'restricted' level. Frontex is currently implementing a Secure Area Network that will allow it to handle classified information up to the level of EU 'restricted'. Frontex's to be adopted new regulation (see below) will allow the agency to exchange personal data with Europol.[92] As stated before, Frontex and Eurojust are currently preparing a cooperation agreement. It is not clear if and how Frontex is cooperating with Sitcen.

[86] Frontex Management Board Decision no. 22/2009 of 25 June 2009 laying down rules on the secondment of national experts (SNE) to Frontex.
[87] Frontex 2011.
[88] See, for instance, the Rapid Pool from which the members of a RABIT operation are drawn (Article 4.2 RABIT regulation).
[89] In a 'joint returns operation', Frontex provides assistance to Member States when they want to return migrants to their home country. Frontex does not organise or coordinate the return of these migrants. See: Kvistholm 21 April 2009.
[90] Regulation (EC) No 562/2006 (Schengen Borders Code).
[91] See Article 5.2 Rabit Regulation.
[92] Council of the European Union, Doc 7961/11, p. 72.

2.3.3.2. Third countries and international organisations

According to Frontex, the establishment of operational cooperation with third countries is valued as 'an indispensable tool' for effective management of the global fight against illegal migration and cross-border crime.[93] The agreements are concluded with law enforcement authorities with operational responsibility for border control, as well as regional border control cooperation structures. Frontex has signed other 'working agreements' on the establishment of operational cooperation with the competent authorities of 13 third countries.[94] These working agreements typically include that Frontex and the third state will develop 'activities in the field of information exchange and risk analyses', and the coordination of 'certain joint operational measures and pilot projects for maintaining and improving border control' between EU member states and the third country. The Council, Commission and the Parliament have little to say in the formulation and signing of these agreements. The Regulation merely states that Frontex may cooperate with the authorities of third countries and international organisations through working arrangements concluded with these authorities 'in accordance with the relevant provisions of the Treaty'. De Witte and Rijpma find it problematic that these arrangements take the form of bilateral international agreements or non-binding memoranda of understanding, since often the non-binding legal nature of these bilateral agreements means that they are not published and are kept secret from the public.[95] Along the same lines, Peers further notes[96] that the texts of these agreements are not online and little is known about their application in practice.

2.4. The EU's Situation Centre (Sitcen)

2.4.1. Legal basis and main tasks

The EU's Joint Situation Centre (Sitcen) was created in 2000 by an administrative decision of the first High Representative of the Union for the Common Foreign and Security Policy, Javier Solana, as a distinct entity that would support the EU's response to crisis situations outside the Union. Sitcen was attached to the Office of the High Representative and, as an integral part of the General Secretariat of the Council, its legal basis was the same as the General Secretariat of the Council, i.e., Article 207(2) of the Treaty of the European Communities. As the European Security and Defence Policy (ESDP) became operational in 2001, and after the 9/11 attacks of that same year, the Member States asked Solana to draw up proposals of how a broader intelligence analysis structure could be put in place. Solana decided to use Sitcen as the institutional framework in which to embed a broader range of analysis and assessment functions.[97]

After the 2004 Madrid bombings, the Council gave Sitcen the additional task of providing the Council with strategic terrorist threat assessments, based on intelligence from national services, and the improved exchange of information with Europol.[98] For this purpose, in January 2005 Sitcen's Analysis Unit established links with the Counter-Terrorism Group, which is an informal gathering of the heads of EU Member States' security services, plus

[93] See Frontex's website, 'External Relations', available at (http://www.frontex.europa.eu/external_relations/).
[94] The Russian Federation, Ukraine, Croatia, Moldova, Georgia, the Former Yugoslav Republic of Macedonia (FYROM), Serbia, Albania, Bosnia and Herzegovina, the United States, Montenegro, Belarus, Canada and Cape Verde, as well as with the CIS Border Troop Commanders Council and the MARRI Regional Centre in the Western Balkans.
[95] De Witte and Rijpma in Annex B of this volume.
[96] Peers in Annex B of this volume.
[97] Belgian Standing Committee I (ed.) 2010, p. 76.
[98] Parliamentary Question E-3940/06EN. Answer given by Mr Frattini on behalf of the Commission (10.11.2006).

those of Switzerland and Norway.[99] Whenever there is a significant event with a possible terrorism aspect, the EU counter-terrorism coordinator is also instantly alerted and kept informed throughout the crisis about the situation by Sitcen.[100] Accordingly, it began to play a role as an actor that influences the EU's internal security policies. After it was given this task, Sitcen started to host seconded intelligence officials from the Member States to assist it with this task.

With the establishment of the European External Action Service in 2010, the Situation Centre has been transferred to the EEAS.[101] In the new structure of the European External Action Service, Sitcen reports to three main actors: the Chair of the Political and Security Committee, the Managing Director for Crisis Response and Operational Coordination, and the EEAS 'Crisis Management Structures'. These structures consist of other former staff of the General Secretariat of the Council, including EU Military Staff and its 'Watchkeeping Capability' and the Crisis Management and Planning Directorate (including the 'Crisis Room') of the Commission. The Commission had a 'crisis room' of six people which maintained a platform for exchange of information between the Commission and EU Delegations during acute crises.[102] The integration of Sitcen's operations unit, the Watchkeeping Capability and the Crisis Room will allow a larger unit of people to work 24/7 to support the EU Delegations' network worldwide, and Common Security and Defence Policy (CSDP) Operations.[103] These structures are placed under the direct authority and responsibility of the High Representative.

This set-up suggests that Sitcen's main role will continue to be that of serving as the EU's information provider in crisis management situations, especially with regard to conflicts and the political dimension of natural disasters. In talks with Member States, Catherine Ashton has labelled Sitcen as the 'single crisis response centre'.[104] Sitcen provides situation-assessments during five phases of activity where such info is needed, which are: early warning, policy development, decision support, conduct of operations and mission evaluation.[105] Sitcen aims to identify and analyse threats (as defined in the European Security Strategy) with the aim of providing early warning to policymakers responsible for the EU's prevention of and response to conflicts. Sitcen can even provide this assistance on the spot, since it has a small team of officials ready to deploy to a crisis location 'in order to assist the Presidency with coordination and communication functions'.[106] Accordingly, the High Representative sent two Sitcen officials to Haiti in the aftermath of the earthquake in order to gather information, assist with consular issues, evacuate EU citizens, set up communications between Haiti and Brussels and set up a temporary EU office in the logistical base of the UN Stabilization Mission in Haiti.[107] Recently, it was reported that a Sitcen official accompanied a European External Action Service (EEAS) fact-finding mission to Libya.[108] While it is clear that Sitcen will primarily support decision making in the CFSP field and thus focus on events outside the Union's borders, it will continue to provide the aforementioned assessments regarding terrorist threats within the Union. This means that it plays a role in the internal security of the EU. It is for this reason that it is of interest for this study, which as we noted in chapter one will not focus on the oversight of external intelligence gathering activities.

It is important to note that Sitcen is the least well known and least understood of the AFSJ bodies discussed in this study. This is largely because it remains non-transparant in a

[99] In April 2004, the Club de Bern decided that the CTG should play the major role in implementing intelligence-related aspects of the Council's Declaration on Combating Terrorism.
[100] House of Lords (2009), Q95.
[101] Council Decision of 26 July 2010, Article 4.3a.
[102] European Parliament 17 November 2010.
[103] European Parliament 24 March 2011.
[104] Ibid.
[105] Shapcott 2007.
[106] Belgian Standing Committee I (ed.) 2010, p. 77.
[107] EU Institute for Security Studies 2010.
[108] Rettman 2011.

number of respects: its founding document and mandate has not been made public. It does not issue public reports on its activities, or on the agreements it has concluded with EU bodies or other external actors. This lack of transparency has been counterproductive and has led to considerable misunderstanding regarding its functions and powers, including the misconception in some quarters of the European Parliament that Sitcen is the EU's equivalent of the CIA. The High Representative has stated to the European Parliament that neither Sitcen nor any other components of the EEAS is an 'intelligence service', and stressed that she has no intention of establishing one as part of the EEAS.[109]

2.4.2. Powers

The Council Decision on the EEAS states that the 'specificities' of the new Crisis Management structures shall be respected, as well as 'the particularities of their functions, recruitment and the status of the staff'.[110] This is of particular relevance to Sitcen, which consists of around 120 officials, including a substantial number of seconded officials coming from national intelligence agencies. These officials were attached to Sitcen in the aftermath of the Madrid Bombings in 2004, when it was tasked with delivering strategic terrorist threat assessments to the European Union. A result of the presence of these seconded officials, the composition of the SitCen is considered classified information.[111] The seconded officers are funded by the Member States and Sitcen's budget is not known.

Sitcen does not have recourse to information collection powers that are generally possessed by national intelligence agencies. Its staff cannot, inter alia, engage in covert surveillance, intercept communications, or use human agents to gather information. Indeed, as the former Director of the Sitcen William Shapcott has stated, Sitcen has had 'no operational role'[112] and it is not likely to get such a role in the future. Its powers are 'limited essentially to sharing assessed intelligence' with a view to producing evaluations to support policymakers in Brussels.[113] Sitcen can therefore best be described as a fusion centre, in the sense that it fuses open source information, diplomatic reporting, military and civilian intelligence to produce all-source situation assessments.

Sitcen conducts its work largely on the basis of open source information and 'assessed' intelligence from a variety of sources, including its seconded intelligence analysts and shared diplomatic reports. Sitcen does not have access to personal data or raw information from national agencies. Information from national intelligence agencies is provided at their discretion and on a strictly 'need to know' basis. Besides information coming from Member States and open sources, Sitcen also receives information 'which [is] not in the open source field but that [is] not in the intelligence field either', such as the EU monitoring mission in the Balkans, or the Aceh Monitoring Mission.[114] Sitcen also has access to images from EU government-owned satellites, namely France's Helios and Pleiades systems, Germany's SAR-Lupe and Italy's Cosmo-SkyMed, on top of existing data from US-owned commercial satellites.[115] Sitcen receives some diplomatic information from all 135 EU delegations in the world,[116] which consists of approximately 5000 officials and a continuous stream of political reports on the situations unfolding on the ground,[117] which help—inter alia—to inform it about the terrorist threats the EU is facing.

[109] European Parliament 3 May 2010.
[110] Council Decision July 2010, Article 4.3a.
[111] House of Lords 21 January 2009b, Q120.
[112] House of Lords 6 December 2010, p. 5.
[113] Ibid., p. 14.
[114] Shapcott 2007.
[115] Rettman 14 September 2010.
[116] House of Lords 21 January 2009, Q97.
[117] Interview with Eneko Landaburu - A European Perspective on Crisis Response, p.70 in A. Ricci (ed.) From Early Warning to Early Action?: The Debate on the Enhancement of the EU's Crisis Response Capability Continues. Office for Official Publications of the European Communities, 2008.

2.4.3. Relationship with third parties

In September 2009, the Council stated that the following actors received Sitcen products: the Presidency, the Member States, the Council's civilian and military authorities, CFSP, ESDP and third-pillar structures, Commission DGs and partner agencies (RELEX, DEV, JLS, EUROPOL), and national civilian and military contributors.[118] It has also provided briefings to MEPs in advance of visits by EP delegations to certain states outside the EP.[119] Nevertheless, former Sitcen director William Shapcott has stated that Sitcen 'not often' provided info to actors outside the Council.

Sitcen has a memorandum of understanding for exchanging information with Europol. There are no details known about this arrangement, except that Europol and Sitcen only exchange 'finished products'.[120] The main analytical reports from Frontex are regularly shared with Sitcen.[121] Sitcen also cooperates with NATO and the UN (including the World Food Programme, UNHCR, UNICEF, OCHA) and the African Union.[122]

2.5. Conclusion

This chapter has provided an overview of the legal bases, mandates and powers of the four AFSJ bodies addressed in this study. We have shown that the AFSJ bodies' mandates and powers primarily consist of two elements: coordinating and supporting the work of national agencies, and in the case of Europol and Eurojust, processing, storing and transferring personal data. However, these bodies do not have recourse to any coercive or special powers as they exist on a national level.

Europol and Eurojust are the agencies that are currently authorised to process, store and transfer personal data within the parameters of their respective mandates. These are activities which interfere with the right to privacy and may serve as the basis for use of coercive or special powers —which have particularly significant human rights implications— by member or third states' authorities. These concerns are amplified when information is shared between AFSJ bodies and third countries that may not respect international standards of human rights and data protection. In view of this, these activities clearly need to be subject to oversight by an independent body. It is a point of concern that often, the agreements upon which such sharing takes place, are not available to the EP, for example, the working agreements between Frontex and third countries, and the agreement between Sitcen and Europol.

This chapter also made it clear that the EP does not seem to have access to all threat assessments which the AFSJ bodies produce. Without this information, it is hard for the EP to fully assess whether, in order to counter these threats, the AFSJ bodies may, for example, need new powers (i.e. requiring legislative amendments), additional resources or new cooperation agreements with particular third states.

An additional matter of concern relates to the lack of transparency of the Sitcen. As mentioned above, its founding document and mandate have not been made public. It does not issue public reports on its activities, or on the agreements it has concluded with EU bodies or other external actors. This lack of transparency has led to the creation of

[118] E-4121/09, Reply to written question on 28 September 2009.
[119] Interview 11.
[120] House of Lords 21 January 2009c, Q108.
[121] Council of the European Union 25 January 2011, p. 19.
[122] House of Lords 21 January 2009c, Q104.

counterproductive myths on the nature of Sitcen's activities. It is in the interests for both Sitcen and the EP that Sitcen becomes more transparent.

This chapter has also shown that Member States' police, prosecutorial, border and (to a much lesser extent) intelligence agencies are both the principal suppliers and the main customers of the AFSJ bodies. Indeed, the AFSJ bodies function primarily on the basis of information provided by national authorities, such as police and prosecutorial services, and their principal output is the information and analysis which is sent to these agencies. National authorities may take action unilaterally or as part of joint operations coordinated by an AFSJ agency, on the basis of such information. These actions may range from inserting information into a database to arresting and detaining individuals. They are undertaken by employees of national authorities, in accordance with national law and are therefore, more appropriately overseen by national oversight mechanisms, including the judicial bodies and parliamentary committees. In the following chapter, we will discuss how national parliaments can oversee the decisions and actions of their state's representatives in the AFSJ.

CHAPTER 3. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF THE EU's AFSJ BODIES

This chapter consists of three sections. The first section will examine the specialised non-parliamentary oversight bodies—the Joint Supervisory Bodies—the EU has created to oversee how Europol and Eurojust process and transfer personal data. Since the oversight of the AFSJ bodies, especially of Europol and Eurojust, is a shared responsibility of the EP and the national parliaments, the second section of this chapter will outline how national parliaments oversee the AFSJ bodies. Since the Treaty on the Functioning of European Union (TFEU) gives the EP and national parliaments an explicit mandate to oversee Europol and Eurojust, we will focus on these two bodies. In the last section of this chapter we will assess which powers and tools the EP has at its disposal to oversee the AFSJ bodies. This assessment is necessary in order to identify any weaknesses in the EP's current oversight of the AFSJ bodies, which could be addressed through the adoption of practices from national systems of oversight of intelligence agencies, which will be discussed in chapter four. Given that access to relevant information is an important foundation of oversight, we will pay particular attention to the legal framework for access to AFSJ-related information by the EP. Since the focus of this study is on oversight by parliament and specialised oversight bodies, a detailed discussion on how the AFSJ bodies are subject to executive oversight (by the Council or the Commission), judicial oversight (by the European Court of Justice), internal oversight (by the Management Boards) or of the European Ombudsman and the European Anti-Fraud Office is outside the scope of this study.

3.1. The Joint Supervisory Bodies for Europol and Eurojust

Chapter two made clear that some of the few operational powers Europol and Eurojust have are the processing, storing and transfer personal data. The EU created two independent 'joint supervisory bodies' (JSBs) for Europol and Eurojust,[123] which review the activities of these agencies in order to ensure that the processing of personal data is carried out in accordance with the applicable legal framework.[124] Since Regulation (EC) 45/2001 would apply to the future processing of personal data by Frontex, the European Data Protection Supervisor monitors the application of the provisions of this Regulation to all processing operations carried out by Frontex. Sitcen is not used for the exchange or analysis of personal data.[125]

The JSB's mandate includes reviewing the permissibility of the transmission of data to third parties. Europol and Eurojust have to guarantee a level of data protection which corresponds at minimum with the principles of the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[126] The JSBs must give their opinion at two stages when agreements on information sharing with third countries are concluded. First, they give an opinion on a draft agreement. Secondly, they have to ensure that the third party maintains an adequate level of data protection in the implementation of the agreement. This is an extremely important role since the

[123] Article 34 of the Europol Decision; Article 23.1 of the Eurojust Decision.
[124] The Europol Decision states that this Decision 'respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union' (preamble 24, Europol Decision).
[125] Reply by the Council to Parliamentary Question E-4103/09, 5 October 2009.
[126] Article 27 of the Europol Decision; Article 14.2 of the Eurojust Decision.

European Parliament is not informed and does not play any formal role in the drafting of such agreements or, indeed, their review once they have been signed.

Both bodies also serve as an appellate body for persons who request access, correction or deletion of data held by Europol and Eurojust.[127] To lodge an appeal, a person should write to the JSB within three months of receiving an unsatisfactory reply from Europol or Eurojust. Persons may also refer to the Europol JSB if they have submitted a request to Europol for access to their own personal data or for this information to be checked, corrected or deleted and have not received a reply after more three months. It is hard to assess the effectiveness of these complaint mechanisms as both JSB's have addressed a very limited amount of cases. Eurojust's JSB has, since its inception, only dealt with two appeals, while Europol's JSB has handled nine cases since it was established.

Both JSBs have additional tasks beyond these core functions. Since 2010, the Europol JSB has been responsible for monitoring whether Europol respects the personal data protection principles in the Terrorist Financing Tracking Programme (TFTP) Agreement when deciding on the admissibility of the US' requests to the Society for Worldwide Interbank Financial Telecommunication (SWIFT). (see below) The Eurojust JSB is also a body to which the Eurojust Data Protection Officer (DPO) may appeal in the event that in her/his view Eurojust has failed to comply with applicable data processing rules. The DPO can refer the matter to the JSB if the Eurojust College has not resolved a finding of non-compliance with these rules within a reasonable time.[128] The Eurojust JSB also supervises the activities of Eurojust liaison magistrates abroad.[129]

3.1.1. Composition

Europol's JSB is composed of a maximum of two members or representatives of each of the independent national supervisory bodies. These national bodies have the task to monitor independently, in accordance with their national law, the permissibility of the input, the retrieval and any communication to Europol of personal data by the Member State concerned, and to examine whether such input, retrieval or communication violates the rights of the data subject.[130] In comparison, Eurojust's JSB is quite small; it is composed of one representative from each Member State, three of whom are permanent members. The three permanent members meet four times per year in The Hague and they are joined by one or more ad hoc judges for the examination of an appeal concerning personal data from the Member State that appointed them. Europol's JSB also meets four times per year.[131] The JSBs are supported by a small secretariat in Brussels that advises the JSB, prepares their meetings and assists with inspections.[132]

The meetings of the JSBs are not public and the members are bound by a confidentiality agreement.[133] This confidentiality is necessary given that individual cases, and thus personal data, may be under discussion. While Europol's JSB issues 'public minutes' that

[127] Articles 30.7 and 32 of the Europol Decision; Article 19.8 of the Eurojust Decision.
[128] Article 17.4 of the Eurojust Decision.
[129] Article 27.5 of the Eurojust Decision.
[130] Article 33 of the Europol Decision.
[131] Article 23.4 of the Eurojust Decision.
[132] Council Decision of 17 October 2000.
[133] Article 23(11) of the Eurojust Decision; Council act of the Joint Supervisory Body of Eurojust of 23 June 2009 laying down its rules of procedure [hereafter 'Eurojust JSB RoP'], Article 29; Council Act n° 29/2009 of the Joint supervisory Body of Europol of 22 June 2009 laying down its rules of procedure [hereafter 'Europol JSB RoP'], Article 31.

summarise the items that were discussed at a meeting, Eurojust's JSB does not follow this practice.

Documents of the JSBs are, in principle, accessible to the public but access can be refused where it is necessary to protect any one of a broad range of public interests. For example, Europol's JSB shall refuse access to a document where such refusal is necessary: (a) to protect security and public order in the Member States or to prevent crime; (b) to protect the rights and freedoms of third parties; (c) to enable Europol to fulfil its tasks properly; and/or (d) to enable the Joint Supervisory Body to fulfil its tasks properly. These considerations 'cannot be overridden by the interests of the applicant'.[134] The Eurojust JSB can refuse public access to a document where disclosure would undermine the protection of: (1) the public interest as regards: (a) public security and criminal investigations; (b) defence and military matters; (c) international relations; (d) the financial, monetary or economic policy of the Community or a Member State; (e) the fulfilment of Eurojust's tasks in reinforcing the fight against serious crime; (f) national investigations in which Eurojust is assisting; and (2) privacy and the integrity of the individual, in particular in accordance with the rules regarding the protection of personal data.[135] In addition, the Eurojust Joint Supervisory Body shall refuse access to a document where, among other things, disclosure would undermine court proceedings, the purpose of inspections, investigations and audits, 'unless there is an overriding public interest in disclosure'.[136] Where the Joint Supervisory Body holds a document received from a third party or which contains information on a third party, it shall consult with that third party with a view to assessing whether an exception is applicable, unless it is clear that the document shall or shall not be disclosed.

3.1.2. Powers

In order to fulfil their tasks, both JSBs have access to all files and premises where personal data is being processed. Europol and Eurojust have to supply all documents, paper files or data stored in Europol's or Eurojust's data files. Both JSBs have free access to all Europol and Eurojust premises at any time, and they carry out inspections *in situ*. In practice, the JSBs notify the agencies in advance of their visit.

Europol's JSB visits Europol once a year for a full inspection, while Eurojust's JSB inspects Eurojust 'fully' every two years with a follow-up visit the next year. Where necessary, additional inspections dedicated to specific issues are carried out. This has not happened at Eurojust yet but the Europol JSB carried out an inspection in November 2010 to evaluate Europol's implementation of the TFTP Agreement. The Europol JSB has issued a three page summary on the eight inspections it did at Europol between 2005 and 2008 but there is no information available on any of the annual inspections it carried out after 2008. The JSB provided a helpful public version of its additional TFTP inspection in November 2010.

Europol's JSB issues non-binding opinions on Europol's activities that have a data protection dimension; indeed, Europol's Management Board is obliged to consult with the JSB in this regard. Europol's Joint Supervisory Body has, for instance, issued opinions on implementing rules, such as 'the draft Management Board rules on receipt of information from private parties', and it also gives its opinion on draft agreements with third countries.[137] The JSB has binding powers only in appellate cases (discussed above) covered

[134] Europol JSB RoP, Article 7.4.
[135] Eurojust JSB RoP, Article 32.4.
[136] Eurojust JSB RoP, Article 32.5.
[137] See (http://europoljsb.consilium.europa.eu/opinions/rules.aspx?lang=en) for a complete list of public opinions.

by Article 32.4 of the Europol decision. Acting on the basis of a two-thirds majority, the JSB can overrule Europol's decision not to give access to data input by Europol in the Europol Information System, data stored in the analysis work files or in any other system established by Europol. Failure to comply with a final decision of the Appeals Committee is best regarded as a violation of the Europol Decision.

If the JSBs discover violations of the provisions of the Eurojust or Europol Decision with regard to the storage, processing or utilisation of personal data, it shall inform Eurojust or the Director of Europol accordingly and shall request a reply within a given period. Failure to comply with a decision of the Eurojust Joint Supervisory Body taken in accordance with its Rules of Procedure shall be regarded as a violation of the Eurojust Decision. Decisions of the Joint Supervisory Body shall then be final and binding on Eurojust.[138] If the Europol Joint Supervisory Body considers that a reply is insufficient, not submitted in a timely manner, or if any other difficulty arises, it can refer the matter in writing to the Management Board. Equally, if the JSB is not satisfied with the director of Europol's response to a complaint regarding a violation of data protection standards by Europol, it can refer the matter to the Management Board. The fact that the JSBs have never resorted to this 'conciliation procedure' may indicate that the JSBs have sufficient power to ensure that Europol and Eurojust comply with data protection rules. According to several persons interviewed for this research, the JSBs' work has been well received by the agencies and other relevant actors, and their recommendations are nearly always implemented.[139] Moreover, the European Data Protection Supervisor has applauded the JSB for its input in the Europol-US agreement, where 'pressure of the JSB' led to a 'number of crucial safeguards with respect to the transfer of personal data to the US'.[140]

It is noteworthy that the work of the JSBs has attracted surprisingly little interest from the EP. Since 2003, Europol's JSB has sent its biennial activity reports to the EP. Eurojust's JSB has done the same with its annual activity report. However, to the best of our knowledge, neither chair has been formally invited to the EP in order to discuss issues raised in their reports. One interviewee suggested that the EP rapporteurs on Europol have never consulted the JSB when drafting their reports, in spite of the JSBs' unique insight into Europol's activities.[141] It should, nevertheless, be noted that there are signs this may be changing. At the time of writing, the Europol JSB's report on the Terrorist Financing Tracking Programme was generating significant interest from MEPs. In this context, the chair of the Europol JSB presented to Parliament the conclusions of its first inspection of Europol's role in the implementation of the TFTP agreement.[142] Further dialogue of this nature should be strongly encouraged. When the director of Europol and the President of Eurojust present their annual reports, Parliament might use this opportunity to ask questions about if/how the agencies have followed up the recommendations of their respective JSBs.[143] This is especially important in the context of the conclusion of draft agreements which are scrutinised by the JSB's.

[138] Eurojust JSB RoP, Article 8.
[139] Interview 26, 30, 32.
[140] Hustinx 2005, p. 3.
[141] Interview 26.
[142] LIBE (2011)0316_1, LIBE Committee Meeting Agenda, 16 March 2011.
[143] Peers, in Annex B of this volume.

3.2. National parliaments' role in overseeing the AFSJ bodies

Articles 85 and 88 of the Treaty on the Functioning of the European Union (TFEU) state specifically that the new regulations on Eurojust and Europol respectively have to 'determine arrangements for involving the European Parliament and national Parliaments in the evaluation of Eurojust's activities' and should 'lay down the procedures for scrutiny of Europol's activities by the European Parliament, together with national Parliaments'. Since the TFEU gave the EP, and national parliaments, an explicit mandate in the oversight of these two agencies, we will focus our attention on how national parliaments have overseen these two particular bodies. The Lisbon treaty does not specify a similar task for Frontex simply because the Treaty does not explicitly refer to Frontex. According to Peers, this omission may be because when the Constitutional Treaty (the precursor to the Treaty of Lisbon) was originally drafted and signed in 2002 to 2004, Frontex was not yet established.[144]

The different references to the role of the EP and national parliaments in Articles 85(1) and 88(2) of the TFEU (i.e., 'the *evaluation* of Eurojust's activities' as distinct from the '*scrutiny* of Europol's activities') are not explained in the *travaux* of the Convention which drew up the text of the Constitutional Treaty. Steve Peers points out that the difference might possibly be explained by the fact that judicial bodies are seen to need more independence from political control.[145] This difference is also partly reflected in the fact that in those cases where national parliaments have been involved in scrutinising AFSJ Bodies, they have primarily been interested in scrutinising the work of Europol.

As we have seen in chapter two, the AFSJ bodies consist of a mix of seconded personnel from the Member States and EU staff members. This unique intergovernmental feature of the AFSJ bodies requires that the EP works closely together with national parliaments. National staff members are paid by the Member States and cooperate with the agencies in accordance with national laws. As such, their cooperation with and contributions to an AFSJ body are more appropriately overseen by national parliaments and, where appropriate, non-parliamentary mechanisms on a national level. Eurojust is, however, different in this context because its national members benefit from a large degree of independence, which reflects the independent character of the judicial nature of the work they carry out.

National parliaments play two other important roles in regard to the oversight of AFSJ bodies. First, they are responsible for ensuring that institutions respect the principles of subsidiarity and proportionality, and thus they play a role in assessing whether the AFSJ bodies are set up and acting in accordance with those principles. Second, in accordance with the constitutional rules of each member state, parliaments may hold their national governments and agencies to account for their policy on the EU and the AFSJ bodies in particular.

3.2.1. Legal framework at the EU level

The relevant legal framework that regulates the involvement of national parliaments in the oversight of AFSJ bodies can be found in the (1) Treaty on the European Union (TEU), (2)

[144] Reg. 2007/2004 was adopted on 26 Oct. 2004, while the Treaty was signed on 29 Oct. 2004.
[145] Peers, in Annex B of this volume.

the Protocol on the role of national parliaments in the European Union, (3) the TFEU and (4) the Rules of Procedures of the European Parliament. Article 12.c of the TEU sets out the different ways in which national parliaments may 'contribute actively to the good functioning of the Union', including through involvement in 'the political monitoring of Europol and the evaluation of Eurojust's activities'. Further detailed arrangements can be found in the 'Protocol on the role of national parliaments in the European Union'.[146] Most importantly, Article 9 of the Protocol prescribes that 'the European Parliament and national Parliaments shall together determine the organisation and promotion of effective and regular inter-parliamentary cooperation within the Union'. The protocol sets out the various means through which this can be done. These include a requirement for the Commission to forward consultation documents (green and white papers and communications) to the national parliaments upon publication (Article 1). Secondly, draft legislative acts are sent to national parliaments (Article 2) and national parliaments may give a reasoned opinion to the EP, Council and Commission on whether such acts comply with the principles of subsidiarity and proportionality (Article 3). Thirdly, the Court of Auditors is required to forward its annual reports to national parliaments (Article 7). Lastly, in the context of inter-parliamentary cooperation, a conference of parliamentary committees for Union affairs (COSAC) may submit any contribution to the EP, Council and Commission, and it may organise inter-parliamentary conferences on specific topics, including AFSJ bodies (Article 10).

A last set of rules concerning the role of national parliaments can be found in the Rules of Procedures (RoP) of the EP.[147] The RoP of the EP sets out various ways of exchange of information, contacts between the EP and national parliaments (Rule 130), the functioning of the Conference of European Affairs Committees (COSAC, Rule 131) and the Conference of Parliaments (Rule 132).

3.2.2. Legal framework at the national level

It needs to be underlined that national parliaments are sovereign in determining how—and indeed, if—they wish to oversee the EU in general, and the AFSJ bodies in particular. National parliamentary oversight of the AFSJ bodies is determined by the constitutional rules and statutory law of each Member State. Three levels of national parliamentary oversight of the AFSJ bodies can be distinguished: (1) holding national governments accountable for their actions concerning AFSJ bodies; (2) direct engagement with AFSJ bodies; and (3) participating in inter-parliamentary cooperation concerning AFSJ bodies.

First, in accordance with the constitutional rules of each member state, national parliaments may participate in national decision making on EU affairs by monitoring and directing their own government's EU policy in the Area of Freedom, Justice and Security. In this context, national parliaments can scrutinise draft EU legislation and could hold their ministers in the Justice and Home Affairs Council to account when it approves changes to the mandates of the AFSJ bodies, gives (new) priorities to these bodies, or comments on the reports of these bodies.[148] Some national parliaments have actively scrutinised the work of their national government in this regard. The UK's House of Lords for instance has

[146] 'Protocols to be annexed to the Treaty on the European Union, to the Treaty on the Functioning of the European Union and, where applicable, to the Treaty establishing the European Atomic Energy Community - Protocol on the role of national parliaments in the European Union', *Official Journal of the European Union,* 17 December 2007, pp. 148–150.
[147] European Parliament, *Rules of Procedure,* 7th Parliamentary Term, March 2011.

given recommendations to the UK Government on its policy towards these bodies. It encouraged the Home Office to encourage the Serious Organised Crime Agency (SOCA) to insert more info into Europol's database.[149]

Another example is the Dutch Second Chamber's request that the Dutch government make necessary resources available for specific operations of Frontex in guarding the Southern borders of the EU.[150] National parliaments are in a position to express such opinions when they approve the national financial contributions to the AFSJ bodies but little or no comparative research has been done on whether national parliaments have actually used this power frequently. However, this power is now less relevant since the EU agencies are primarily funded by the EU budget.

De Witte and Rijpma note that national parliaments have experienced difficulty in scrutinising Europol's work through the national representatives on the Management Board, in finding information and in coordinating their efforts—internally amongst national parliaments and with the European Parliament.[151] Some national parliaments (e.g., Latvia, Lithuania and the Czech Republic) invite their national liaison officer to Europol to attend meetings of the relevant parliamentary committee(s) but this practice does not seem to be widespread. From the COSAC questionnaire, it also is not clear to which extent national parliamentary committees examine the role of personnel seconded to the AFSJ bodies. [152]

Second, national parliaments have shown interest in scrutinising the AFSJ bodies. Roughly two out of three national parliaments have exercised some form of monitoring of Eurojust and Europol through their respective Committee on EU Affairs.[153] Importantly, the UK House of Lords has published reports on all three AFSJ agencies under discussion.[154] While national states have conducted this type of scrutiny on an ad hoc basis, we are not aware of any national parliament having adopted specific procedures to scrutinise these agencies on a more systematic basis, or indeed, any specific benchmarks to monitor the performance of Europol and Eurojust.[155] Parliaments may engage with AFSJ bodies directly by inviting their directors to attend parliamentary hearings or by visiting the premises of the AFSJ bodies. For example, the UK's House of Lords EU Select Committee visited the headquarters of Europol in The Hague and received evidence from the Director of Europol as well as representatives of the Commission, a Member of the European Parliament and the EU Counterterrorism Coordinator report on Europol. This took place in the context of an inquiry into the role of Europol in coordinating the fight against serious and organised crime.[156] The President of Eurojust also has visited and delivered speeches to national parliaments.[157]

Third, while the previous two forms of national parliamentary oversight of AFSJ bodies are conducted without coordination with the parliaments of other Member States, national parliaments may also participate in various forms of inter-parliamentary cooperation dealing with AFSJ bodies. Firstly, the Conference of Community and European Affairs

[148] In the case of Eurojust, the Council, for example, adopts conclusions on Eurojust's annual reports which include an assessment of Eurojust performance in the previous year and recommendations to Eurojust and the Member States on future actions that need to be done.
[149] Lords Hansard 2009.
[150] Kamer 2011.
[151] De Witte and Rijpma, in Annex B of this volume.
[152] COSAC 2010, pp. 24–27.
[153] Ibid., pp. 24 and 26.
[154] House of Lords Select Committee on the EU 2004, March 2008 and November 2008.
[155] COSAC 2010, pp. 24–27.
[156] House of Lords, EU Select Committee 2008, Point 5.
[157] Interview 32.

Committees of Parliaments of the European Union (COSAC) may deal with AFSJ bodies. For example, the XLIII COSAC conference specifically dealt with the role of national parliaments in the political monitoring of Europol and the evaluation of activities of Eurojust after the entry into force of the Lisbon Treaty in December 2010.[158] Secondly, the Conference of Speakers of the Parliaments may also address issues directly relevant to AFSJ bodies, as happened at its conference in Brussels in April 2011. At this conference, it discussed the role of parliaments in monitoring the European Area of Freedom, Security and Justice and the participants agreed that that closer and deeper parliamentary oversight of Europol is necessary.[159] Thirdly, the LIBE committee may convene inter-parliamentary meetings on the issue of AFSJ bodies. For example, in 2010, the LIBE Committee hosted an inter-parliamentary committee meeting on the evaluation of Europol, Eurojust, Frontex and Schengen with participation of national parliaments.[160] National parliaments and the European Parliament exchange information through the Interparliamentary EU Exchange Information Network (IPEX), a website for the electronic exchange of information.[161] There are also informal contacts between national and European parliamentarians and within trans-European political groups also on AFSJ issues.

As early as 2001, recommendations for the creation of a 'Parlopol' Committee were made; this would have consisted of a joint committee of members of the European Parliament and national Parliaments to oversee Europol but it was not established as a formal parliamentary committee.[162]

3.3. The role of the European Parliament in overseeing the AFSJ bodies

In this section, we assess which tools and powers the European Parliament has at its disposal to scrutinise and evaluate the AFSJ bodies. The Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) is the logical venue to undertake such activities as it is responsible for the protection within the territory of the Union of citizens' rights, human rights and fundamental rights; legislation in the areas of transparency and the protection of natural persons with regard to the processing of personal data; and the development of an area of freedom, security and justice, in particular measures relating to police and judicial cooperation in criminal matters.[163] The only body discussed in this study whose activities would not directly fall within the mandate of the LIBE Committee is the Sitcen. Technically, the Sitcen falls under the purview of the Committee on Foreign Affairs (AFET) and its Sub-Committee of Defence (SEDE). This is because these committees are responsible for the Common Foreign and Security Policy (CFSP) and the European Security and Defence Policy (ESDP), including the EEAS within which Sitcen is located. In practice, however, neither of these committees has taken a clear interest in overseeing the work of Sitcen. While AFET and SEDE have primary responsibility for matters concerning Sitcen, aspects of its work may also fall under the jurisdiction of the LIBE committee. As we have already noted in chapter two, Sitcen provides strategic assessments on terrorist threats within the EU and thus plays a role in internal security.

[158] COSAC 2010, pp. 24–27.
[159] Conference of the Speakers of the Parliaments of the EU 2011, Point. 5
[160] European Parliament LIBE Committee 2010.
[161] See (www.ipex.eu).
[162] European Parliament 2006, p. 5.
[163] European Parliament Rules of Procedure, Annex VII, XVII.

The general responsibility of these committees is to examine questions referred to them by Parliament. Any committee may, with the agreement of Parliament's Bureau, instruct one or more of its members to undertake a study or fact-finding mission. Additionally, the committee may, subject to approval by the Bureau, organise a hearing of experts if it considers such a hearing essential to the effective conduct of its work on a particular subject.

A Committee of the European Parliament can also draw up 'own initiative reports' on issues that fall within the scope of its competence. The Conference of Presidents, the body responsible for the organisation of Parliament's work, authorises the forwarding of 'own initiative reports' to the plenary.[164] The LIBE Committee has frequently prepared such own initiative reports on JHA related issues, including on the role of the various JHA agencies. The EP issued such a report on the evaluation and future development of Frontex and EUROSUR in 2008,[165] and on the future development of Europol in 2003.[166] Currently, own initiative reports are being prepared on organised crime in Europe[167] and on the European Internal Security Strategy,[168] which also take into account the role of Europol and Eurojust. These reports provide a useful outlook on the future directions of JHA policies and they serve as an evaluation of the given agency.

3.3.1. The European Parliament's access to classified information

A mandate to oversee particular dimensions of an AFSJ body's work is of limited use unless it is accompanied by access to the necessary information. Similarly, oversight powers—such as the right to summon the Director of an agency to appear before a committee—are likely to be ineffective unless the body with recourse to such powers has the right to access particular information in the context of these hearings. Since there is no single clear legal framework in place for the EP to access AFSJ-related information, including threat analyses from the AFSJ bodies,[169] it is useful to elaborate upon the different rules that regulate the EP's access to (classified) information in the hands of these agencies. Members of the EP are able to ask questions and request information to assess Parliament's access to information in the hands of the Commission and the Council as well. A cursory look into the register of the European Parliament revealed that the in the 6th and 7th Parliamentary Term, MEP's asked seven written questions about Sitcen, 27 about Eurojust, 105 on Europol and 158 on Frontex. Most responses to these questions came from the Commission. Questions for oral answers with debate may be put to the Council or the Commission by a committee, a political group or at least 40 Members with a request that they be placed on the agenda of Parliament,[170] but it seems that this specific type of debate has not really touched upon the subjects discussed in this study.

3.3.1.1. Regulation 1049/2001

Regulation 1049/2001 defines the principles, conditions and limits governing the right of public access to documents of the EP, the Council and the Commission. Article 15.3 of the TFEU extended the public right of access to documents of all Union institutions, bodies, offices and agencies. The Commission foresaw this development and in 2008 it

[164] Rule 45 of the Rules of Procedure of the European Parliament.
[165] Sánchez 2008.
[166] von Boetticher and Turco 2003.
[167] European Parliament LIBE Committee 29 March 2011.
[168] European Parliament Libe Committee 14 February 2011.
[169] Interviews 4, 9 and 13.
[170] Rule 115 of the Rules of Procedure of the European Parliament.

promulgated proposals to revise Regulation 1049; these proposals were further updated in early 2011.[171] The Commission's proposals have been the subject of heated discussion in the EP and several committees have issued reports or opinions on this matter. At present, there is a significant gulf between the Commission's proposals and the counter-proposals put forward by the EP, led by the LIBE Committee's Michael Cashman.

As a general rule, Regulation 1049 stipulates that 'all documents of the institutions should be accessible to the public'. However, this default rule is limited by Articles 4 and 9 of the Regulation, which contain extensive exceptions to this rule. Article 4 states that European institutions can refuse access to documents where disclosure would undermine, inter alia, public interests such as public security, defence and military matters, international relations and the privacy of individuals. It also codifies the so-called 'third party rule', which stipulates that an institution receiving a request to access information must seek the permission of the party from which the document originated before granting access. Article 9 of Regulation 1049 regulates access to 'sensitive documents' that are classified as top secret, secret or confidential. While Article 9.1 states that these documents 'protect essential interests' of the Union and the Member States, in particular in the areas of public security, defence and military matters, the regulation does not specify the general principles regarding the classification of 'sensitive' documents.[172] It is important to note that Regulation 1049 stipulates that the legal basis for the European Parliament's access to 'sensitive documents' from the Commission and Council should be arranged through inter-institutional arrangements.[173] Both the Commission and the Council currently have such an inter-institutional agreement with the Parliament (see below) which covers some aspects of parliamentary access to sensitive information.

The application of Regulation 1049, including its exceptions, has been extended to the AFSJ agencies by virtue of a specific provision in their respective founding acts. Article 28 of the Frontex Regulation states that Frontex shall be subject to Regulation 1049 'when handling applications for access to documents held by it'. Article 45 of the Europol Decision and Article 39 of the Eurojust Decision state that the Management Board or the College shall adopt rules concerning access to Europol/Eurojust documents on the basis of a proposal of the Director (for Europol) and the Administrative Director (for Eurojust), taking into account 'the principles and limits set out' in Regulation 1049. As the EU's AFSJ bodies are not formally 'institutions', there are no specific inter-institutional agreements between Parliament and these agencies to regulate access to information.

One of the most fundamental questions under discussion is whether or not the revised version of Regulation 1049 should address access to classified information by parliament, as well as for access by the general public. Indeed, many people inside and outside the European Parliament argue that differences of opinion on this issue are one of the main stumbling blocks stalling the adoption of a revised regulation.[174] The Commission's proposal largely follows the approach taken in the existing Regulation 1049; namely, that the regulation addresses access to documents by the general public and that access to information by the EP should be regulated by inter-institutional agreements.[175] By contrast, the EP Rapporteur on the revision of 1049 has drafted a detailed set of amendments to the Commission's proposal which would see the new regulation address access to information

[171] European Commission 21 March 2011. Earlier, the Commission had proposed a substantive revision of Regulation 1049 in 2008, which was subject to debates in the European Parliament. See also: European Commission 30 April 2008.
[172] See also: Labayle 2009.
[173] Article 8.7 and recital 9 of REG 1049/2001.
[174] Interviews 9, 11, 18, 28 and 29.
[175] European Commission 30 April 2008, Recital 15.

for both Parliament and the general public.[176] The Commission, Council and some in the European Parliament (largely from the EPP group) remain opposed to this approach and would like to confine the discussion on Parliament's access to classified information through a reference to inter-institutional arrangements.[177] (See chapter five).

3.3.1.2. Inter-institutional agreements between the Parliament and the Commission/Council on access to classified information

As we have already noted, Regulation 1049 stipulates that the legal basis for the European Parliament's access to 'sensitive documents' of the Commission and the Council should be arranged through inter-institutional arrangements.[178] Proponents of having an overarching regulation that deals with access to information for both the Parliament and the general public have pointed out that these inter-institutional agreements are hierarchically inferior to treaty principles, such as the principle of 'mutual sincere' cooperation[179] or regulations, and that it is inappropriate to use such inter-institutional agreements to regulate general principles, such as access to classified information.[180] The Parliament concluded most recently such arrangements with the Council in 2002[181] and with the Commission in 2005 and 2010.[182] While the 2010 agreement between the Parliament and the Commission provides a comprehensive legal framework for parliamentary access to information from the Commission, the inter-institutional agreement with the Council focuses on access to information in the ESDP field only. Several similar agreements are currently being discussed, including a draft 'Inter-institutional Agreement between the European Parliament and the Council concerning access by the European Parliament to classified parts of international agreements subject to its consent'.

3.3.1.2.1. The 2002 inter-institutional agreement and the special committee

An inter-institutional agreement between the EP and the Council regulates the access of the EP to 'sensitive' information held by the Council in the ESDP area.[183] In the event of a crisis or at the request of the President of the European Parliament or the chairman of the AFET committee, the Presidency of the Council or the High Representative shall inform the President of the EP and a 'special committee' of the content of the sensitive information 'where it is required for the exercise of the powers conferred on the European Parliament by the Treaty on the European Union'.[184] In practice, it has always been the head of AFET who requested access to information. This 'special committee' is chaired by the Chairperson of the AFET committee and includes four additional members who are designated by the

[176] See, for instance, Article 3.a.9 of the Cashman report which states that 'in accordance with the democratic principle outlined in Articles 9 to 12 TEU, the European Parliament as the citizens' representative shall have access to EU classified information'. Committee on Civil Liberties, Justice and Home Affairs 12 May 2010.
[177] Interview 20.
[178] Article 8.7 and recital 9 of REG 1049/2001.
[179] Article 13.2 of the Treaty of the European Union.
[180] Interview 6.
[181] Interinstitutional Agreement of 20 November 2002.
[182] Annex 1 of the 2005 Agreement regulates the forwarding of 'confidential information' to the Parliament (the Framework agreement on EP-Commission relations and the European Parliament decision on the revision of the framework agreement on relations between the European Parliament and the Commission (2005/2076(ACI)) are available at (http://www.europarl.europa.eu/sides/getDoc.do?objRefId=96173&language=EN#BKMD-9). It was replaced by Annex 2 on the forwarding of confidential information to Parliament in 2010 (see European Parliament decision of 20 October 2010 on the revision of the framework agreement on relations between the European Parliament and the European Commission (2010/2118(ACI)), available at (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0366+0+DOC+XML+V0//EN&language=EN#BKMD-1).
[183] Interinstitutional Agreement of 20 November 2002.
[184] Interinstitutional Agreement of 20 November 2002, Article 3.3. This special committee is not to be confused with the special committees described.

Conference of Presidents, as well as four substitutes—these MEPs do not have to be members of the AFET committee but often have been.[185] Consultation of sensitive documents by the members of the Special Committee of the European Parliament has to take place in a secured room on the Council premises. Its members and substitute-members are meant to have appropriate security clearance from their national governments. However, in practice, not all members of the committee had such a clearance and, yet they had access to classified information. This was the result of delays and, more importantly, the fact that in some EU states it is not seen as appropriate to subject parliamentarians to a vetting process.[186] Security-cleared staffers can be present but sometimes had to be excluded from the briefings, which took place approximately four times per year. Often no documents were provided during these meetings and many meetings only consisted of an oral briefing or, as one interviewee put it, 'a coffee with Solana'.[187] Members of this Special Committee could have used these meetings to ask questions about Sitcen but have not done this in the past mainly because its members didn't see it as a priority issue.[188]

The High Representative has suggested that the modalities of the 2002 Agreement will apply to the EEAS as well but there is a lot of confusion among and within the institutions about whether this is the case. However, at the time of writing, no meetings of the Special Committee have taken place since the creation of the EEAS. The possible revision of this agreement is being discussed within the institutions, especially since the creation of the European External Action Service, which will play a pre-eminent role in the policy area covered by the 2002 agreement.

3.3.1.2.2. Draft inter-institutional agreement between the Parliament and the Council on access to information relating to international agreements

According to Article 218.10 of the TFEU, the European Parliament needs to be 'immediately and fully informed at all stages' of the formulation of agreements between the Union and third countries that involve the EP's consent procedure, which now includes agreements in the Area of Freedom, Security and Justice. This obligation affects the Council and the Commission when the latter is presenting draft negotiating guidelines to the Council or negotiating on the Council's behalf with third countries. Some in the EP argue that the Council regularly fails to comply with this article by not providing enough information to the EP,[189] or by not providing information in due time for the EP to exercise its tasks. In the SWIFT case, for example, the President of the EP complained that the Council gave the EP only one week to approve the SWIFT agreement before it was due to enter into effect. The President suggested that, ideally, the EP needs at least three months in order to reflect whether to give its consent to any agreement. In response to this controversy, the Council proposed that an 'Inter-institutional Agreement between the European Parliament and the Council concerning access by the European Parliament to classified parts of international agreements subject to its consent' would be drawn up and that this proposal would be submitted to the Parliament for discussion between the two institutions.[190] The text of this document is not yet publicly available.

[185] Interview 17.
[186] Interviews 17 and 21.
[187] Ibid.
[188] Interviews 11, 17 and 21.
[189] Interviews 5 and 9.
[190] Buzek 2010.

3.3.1.2.3. The 2010 Framework agreement between Parliament and the Commission

Annex 2 of the 2010 Framework agreement between Parliament and the Commission regulates the 'forwarding to Parliament and the handling of confidential information' from the Commission 'in connection with the exercise of Parliament's prerogatives and competences'. This annex contains the most comprehensive provisions on parliamentary access to classified information that have ever been formulated between the EP and another EU entity. The annex covers all policy areas and provides the President, the chairs of the parliamentary committees, the Bureau and the Conference of Presidents of the European Parliament with a fairly broad right to request and receive 'EU Classified Information' (EUCI) that is 'required for the exercise of Parliament's prerogatives and competences'.[191]

Such requests can include all levels of EUCI. The agreement also provides a basis for the Commission to forward EUCI to the EP on its own initiative. While the agreement gives the EP the possibility of accessing a broad range of EUCI, its access to information may be limited by the third party rule, which is clearly enshrined in the agreement: 'confidential information from a State, an institution or an international organisation shall be forwarded only with its consent'.[192]

The agreement also stipulates the information security standards that the Parliament needs to take into account when it receives EUCI from the Commission. MEPs and parliamentary staffers can only have access to information classified as 'secret' or above if they have an 'appropriate' security clearance.[193] MEPs without the requisite national security clearance can still access information up to and including information classified as 'confidential' (the second of the four levels of EUCI) in accordance with 'practical arrangements defined by common accord, including signature of a solemn declaration that they will not disclose the contents of those documents to any third person'.[194] Staffers can be given access to all levels of EUCI if they are 'designated in advance by the parliamentary body/office-holder' as having a need to know the information concerned and have security clearance.

The arrangement specifies further measures for access to and the handling of confidential information.[195] Interestingly, the arrangement provides for an option to hold a meeting of a relevant committee *in camera*, with cleared staffers, where numbered documents can be 'distributed at the beginning of the meeting and collected again at the end'. No notes of those documents and no photocopies thereof may be taken.[196] Before transmission, all personal data may be expunged from the documents.

It is important to note that Annex 2 of the agreement has not yet been fully implemented because it requires parliament to establish security rules and procedures that are equivalent to those of the Commission. At the time of writing, an EP working group is continuing to work on the formulation of these rules and procedures, which will enable the EP to receive classified information on its own premises.

Although this agreement represents a significant advancement in terms of the EP's access to information from the Commission, its application is limited to Commission documents.

[191] European Parliament 20 October 2010, Annex 2.
[192] Ibid., Article 2.1.
[193] Ibid., Article 2.5.1.
[194] Ibid., Article 2.5.2 of Annex 2.
[195] Ibid., Article 3 of Annex 2.
[196] Ibid., Article 3.2.2 of Annex 2.

This is a significant limitation in the AFSJ field because much of the information, which might be relevant to the EP, resides with the AFSJ agencies and/or is contained within Council documents.

3.3.1.3. Access to information from the EEAS

The High Representative has suggested that the modalities of the Framework agreement with the Commission could be applied to the EEAS as well but we have observed that there is no agreement among and within the institutions about whether this will indeed be the case. This is important in order for the EP to get access to information related to Sitcen since Sitcen is now a part of the EEAS (see above, chapter two). What seems clear is that the High Representative's Declaration on Political Accountability should not be automatically read as committing the EEAS to apply Annex 2 of the framework agreement between the EP and the Commission.[197] Rather, it is far more likely that the EEAS will try to apply the 2002 agreement between the EP and the Council to EEAS documents.[198] This would be highly problematic, however, since the 2002 Agreement with the Council only relates to 'sensitive' information related to ESDP issues, while the EEAS deals with a range of issues that go beyond security and defence policy. Since the EEAS has a hybrid status, it was also suggested that different rules might apply to different parts of the EEAS.[199] It was also submitted that if a document is under discussion by the Council, it automatically becomes a 'Council' document and not an EEAS document.[200] It seems to be clear that there needs to be a new separate inter-institutional agreement between the EEAS and the Parliament, which regulates access to classified information by the EP.

3.3.1.4. Pro-active disclosure of non-classified information to the European Parliament

Oversight is facilitated through a number of reporting and evaluation obligations that are laid down in the founding instruments of Europol, Eurojust and Frontex. Each year, the agencies are obliged to adopt a work programme and to prepare a general report on their activities in the previous year. Europol's Management Board sends its work programme and annual report to the Council, who forwards it to the Parliament. Frontex's Management Board on the other hand sends its annual report and the work programme directly to the EP, while Article 32.1 of the Eurojust Decision states that the President, on behalf of the Eurojust College, has to issue in writing an annual report to the Council on the activities and management, including budgetary management, of Eurojust. Article 20 of Eurojust's Rules of Procedure further states that Eurojust shall 'maintain the necessary channels of communication with the EP in accordance with this decision'. Needless to say, this proactive disclosure of information to the EP does not extend to classified information.
Neither Sitcen nor the EEAS more generally have similar obligations to report to the EP. Pursuant to Article 13.2 of the EEAS Decision, the High Representative only has to submit a report to the EP on the functioning of the EEAS by the end of 2011. This report might cover some activities of Sitcen but this remains to be seen.

The agencies discussed in this study are all subject to independent evaluations, which are available to the Parliament as well. Every four years, Europol's Management Board has to commission an independent external evaluation of the implementation of the Europol

[197] Interview 11.
[198] Interviews 18 and 19.
[199] Interviews 4 and 11.
[200] Interview 21.

Decision and of the activities carried out by Europol.[201] The objective of such an evaluation is to assess, in an independent and objective manner, the impact of the Europol Council Decision on Europol's performance, and to determine the areas where new legal provisions and/or practical operational arrangements would render Europol 'more effective'.[202] Eurojust's College and Frontex's Management Board have to commission such an evaluation every five years.[203] The independent external evaluations of Eurojust and Europol are sent to the European Parliament. The Frontex Regulation stipulates that the Management Board shall receive these findings and issue recommendations regarding changes to this Regulation, the Agency and its working practices to the Commission, which shall forward them together with its own opinion as well as appropriate proposals to the Council. 'An action plan with a timetable shall be included, if appropriate. Both the findings and the recommendations of the evaluation shall be made public'.[204] They can be consulted on the Frontex website.[205]

3.3.2. Oversight mechanisms of the European Parliament

3.3.2.1. Summon agency directors

Currently, the Parliament does not have uniform powers to summon AFSJ agency directors to the Parliament to engage in a debate with them. Article 48 of the Europol Council Decision provides that the Europol Director, the Chairperson of the Management Board and the Presidency of the Council are obliged—instead of permitted—to appear before the European Parliament at its request.[206] By contrast, the President of Eurojust, on behalf of the College, is only expected to 'report to the Council every year on the activities and management, including budgetary management, of Eurojust'. Still, the President has presented the annual report every year to the LIBE Committee. The Frontex Regulation states in Article 25(2) that both the Parliament and the Council may invite the Executive Director of the Agency to report on the carrying out of his/her tasks. However, Frontex's refusal to attend a public hearing on the 'Tragedies of Migrants at Sea' organised by the LIBE Committee in July 2007, caused considerable consternation amongst some Members of the European Parliament,[207] and clearly showed that the Director of Frontex did not consider this an obligation.[208] Yet, in its amendments to the new Frontex Regulation, the Parliament has not recommended making it a requirement for the Director of Frontex to appear before it. The EP simply suggested that the new Frontex Regulation would clarify this reporting duty to focus 'on the general report of the Agency for the previous year, the work programme for the coming year and the Agency's multi-annual plan'.

The EP has no formal power to summon the director of Sitcen to appear before Parliament but recently, the new head appeared before the parliament together with the Executive Secretary General of the EEAS.[209] Additionally, the former director of Sitcen occasionally appeared before the Sub Committee on Defence to give MEPs briefings on its work on an ad

[201] Article 37.11 of the Europol Decision.
[202] See, for instance: Europol Contract notice, NL-The Hague: evaluation of the implementation of the Europol Council Decision and of Europol's activities 2011/S 62-099550, 30.3.2011, available at (http://www.europol.europa.eu/procurement/docs/D-MB-1101.pdf).
[203] Article 41a.1 of the consolidated EJ Decision; Article 33.1 of the Frontex Regulation.
[204] Article 33.3 of the Frontex Regulation.
[205] See: External evaluation of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union 2009.
[206] Article 48 of the Europol Decision.
[207] House of Lords 5 March 2008.
[208] De Witte and Rijpma, in Annex B of this volume.
[209] European Parliament LIBE Committee 11 April 2011.

hoc basis.[210] Since Sitcen is placed under the direct authority and responsibility of the High Representative, it should be noted that, in accordance with Article 36 of the TEU, the High Representative will 'regularly consult' the European Parliament on the main aspects and the basic choices of the CFSP and will ensure that the views of the European Parliament are 'duly taken into consideration'. In the preamble of the 'Declaration on Accountability', High Representative Ashton has said that she will 'build on' the 'consultation, information and reporting engagements' of the former three main foreign policy actors in the Union: the former Commissioner for external relations, the former High Representative for the Common Foreign and Security Policy, and the rotating Council Presidency. She adds, however, that 'where necessary' 'these engagements will be adjusted in light of Parliament's role of political control and the redefinition of the role of the High Representative as set out by the Treaties and in accordance with Article 36 [of the] TEU'.

It is important that the Parliament can engage with the directors of the agencies in a public debate as this allows for the initiation of a dialogue between MPs and directors on general policies of their agencies or specific cases, in which MPs can ask questions and directors can defend or explain the actions of the agencies. However, a number of interviewees questioned the public nature of these meetings on the basis that directors cannot (or are unlikely to) say anything profound or critical of their agency in a public forum.[211] A second point of criticism voiced in connection with the hearings with agency directors was the disappointingly low number of members that were actually present to question the directors.[212] Interest and participation on the part of MEPs in these hearings is essential to make such hearings work but the reality seems to be that many MEPs do not have the time to engage properly in scrutinising the documents they receive from the agencies and are, therefore, ill-prepared to ask pertinent questions of the agencies.[213]

3.3.2.2. Informal meetings

It should be stressed that several interviewees pointed out that there existed a substantial amount of informal contact between members or staffers of the LIBE committee and the agencies, which allowed for an ongoing informal dialogue between the EP and the agencies.[214] Also, the AFET committee has developed a custom of organising informal meetings with staffers of the AFSJ bodies in order to be briefed on certain issues, but this didn't necessarily involve meetings on the work of Sitcen.[215] Another type of informal contact between the EP and the agencies is through sending delegations to the relevant agencies. The LIBE committee has sent delegations to visit the premises of Eurojust, Europol and Frontex. Such missions have greatly contributed to make MEPs and their staffers aware of the mandates, powers and working methods of these organisations.[216] Indeed, Europol has stated that the LIBE committee's visit to Europol in June 2010 could already 'serve as a practical example of the strengthening of Europol's democratic accountability and transparency'.[217] Finally, it is noteworthy that the directors and senior member staff of Europol, Frontex and Eurojust regularly attend conferences and hearings organised by the LIBE Committee and political groups. These are informal meetings and do not constitute oversight but nonetheless help to strengthen contacts between the EP and the agencies, as well as MEP's knowledge of the agencies' work.

[210] Interview 11.
[211] Interviews 16 and 32.
[212] Interviews 2, 10 and 18.
[213] Interviews 2, 13 and 16.
[214] Interviews 30 and 32.
[215] Interview 11.
[216] Interviews 2, 30 and 32.

3.3.2.3. Budgetary powers of the European Parliament

The European Parliament is the budgetary authority for the AFSJ agencies (i.e., Europol, Eurojust and Frontex), as well as its discharge authority.[218] The EP's powers to oversee the EU budget are based on Articles 310–324 of the TFEU, which empowers the EP to adopt the annual budget administered by the Commission (TFEU, Article 310), the multi-annual financial framework (Article 312), as well as to give a discharge to the Commission in respect of the implementation of the budget (TFEU, Article 317–319). As a budgetary authority, the EP can, together with the Council, decide on the amount of money that the agencies can spend from the budget of the European Union. However, it has no say over contributions of the EU Member States to the AFSJ agencies and Sitcen. As the sole discharge authority, the EP evaluates how the agencies have spent the budget that was allocated to them. This discharge procedure may give rise to three situations: the granting, postponement or refusal of discharge by a Resolution of the European Parliament. The refusal of discharge may lead to the freezing of an agency's funding.

3.3.2.3.1. The EP as a budgetary authority

Each year, the Management Board of the AFSJ agencies (or the College, in Eurojust's case) adopts a draft estimated budget together with a draft work programme. This is forwarded to the Commission by 31 March, which in turn forwards it to the Council and Parliament. On the basis of this estimate of the agency, the Commission enters the amounts necessary into the draft EU budget.[219]

Within the EP, the Committee on Budgets (BUDG) is responsible for drafting the EP's position on the annual EU budget. It produces a report on all sections of the budget, including the part related to the Area of Freedom, Justice and Security and the Union's decentralised bodies.[220] The LIBE Committee provides input to the BUDG committee by means of an opinion. In addition, MEPs, political groups or Committees as a whole can table amendments that will be voted upon in the BUDG committee. During this process, the Management Boards of the agencies adopt their budgets, but this only becomes final after adoption of the general EU budget and, where necessary, it will be adjusted.

In order to properly exercise financial scrutiny over the agency's budgets, the BUDG committee needs to have proper access to information about the activities of the agencies that are funded by the EU budget. As a general rule, the BUDG committee has easier access to information than the Committee on Budgetary Control (CONT) and specialised committees such as LIBE because it has more powers than these committees. The BUDG committee has 'the power of the purse', meaning that money can only be apportioned to an agency once the BUDG committee has passed the EU budget. It can also threaten to use the 'reserve procedure' if the Commission is not prepared to hand over requested information about the activities of the agencies.[221] The reserve procedure involves the BUDG committee 'blocking' a given amount of an agency's funding and making its release contingent upon the fulfilment of particular criteria established by the committee. In 2008,

[217] Europol 20 May 2011, p. 68.
[218] For an overview of the activities of the BUDG committee, see (http://www.europarl.europa.eu/activities/committees/publicationsCom.do;jsessionid=6E57D97166F6CE607D921B99042C7237.node1?language=EN&body=CONT).
[219] De Witte and Rijpma, in Annex B of this volume.
[220] See, e.g., Committee on budgets 9 March 2010.
[221] Interviews 3, 8 and 10.

for example, the EP put 30% of the administrative budget of Frontex 'in reserve', only to be released when the EP was satisfied that the agency had improved its effectiveness and accountability.[222] It is important to note that the BUDG Committee can use this procedure upon the recommendation of the LIBE committee for instance, which has happened in the past.[223] Using the reserve procedure as a means to get information from the agencies is not an ideal way of accessing information but the fact that the EP has tried to use (or abuse) this procedure is symptomatic of the fact that there is not a proper framework for the European Parliament's access to information.[224]

Cooperation between the LIBE and BUDG committees suggests that the LIBE can influence, inter alia, policy priorities by proposing budgetary amendments, which the BUDG committee may or may not take account of. Or, in other words, the LIBE Committee can take advantage of the powers of BUDG in support of the fulfilment of its mandate to oversee AFSJ bodies. However, there are two notable obstacles in this regard. Firstly, the expenditures of the EU budget for the AFSJ bodies are grouped according to functional categories of expenditures. For example, the 2011 budget for Europol represents the expenditures on the basis of the following categories: staff, other administrative expenditures (e.g., rental of buildings, IT, postal and telecommunications) and operational activities.[225] These expenditures are not linked to policy objectives or outputs of the agency concerned—the budget is input rather than output focussed. This makes it very difficult for the EP to approve budget proposals according to policy priorities. Instead, the current budget format only allows for incremental budgeting, i.e., to increase or decrease the planned budget vis-à-vis the previous year(s). Secondly, according to some interviewees, MEPs are often not aware of the potential of the budgetary oversight powers at their disposal and sometimes lack the assertiveness to use these powers in a more 'technocratic' procedure of the BUDG committee.[226]

3.3.2.3.2. The EP as a discharge authority

While the ultimate discharge authority lies with the plenary of the EP,[227] the EP Committee on Budgetary Control (CONT) scrutinises how the EU budget is spent; how well goals are met, in terms of efficiency; and whether or not an organisation's performance represents value for money. The Committee investigates problems raised by the Court of Auditors or the Anti-Fraud Office (OLAF) and suggests improvements to the system in order to ensure legality and to fight against fraud and possible corruption in the use of EU funds.[228] While the adoption of the EU budget is a power that the EP shares with the Council, the discharge authority lies exclusively with the EP. LIBE provides the Committee on Budgetary Control (CONT) with an opinion on the discharge in respect of the implementation of the agencies that fall under its purview. In these opinions, the LIBE makes suggestions to CONT regarding what should be incorporated in its motions for a resolution on discharge of the AFSJ agencies' budgets. The CONT also publishes a yearly overall report on the performance, financial management and control of EU agencies.[229]

[222] House of Lords 5 March 2008, page 28, point 77; De Witte and Rijpma, in Annex B of this volume. The legal basis of the reserve procedure is the Consolidated Financial Regulation (24/02/2009), Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities, Articles 23, 24 and 43.
[223] Interview 10.
[224] Interviews 9 and 10.
[225] Europol 2011.
[226] Interview 10.
[227] Interview 3.
[228] Presentation and competences of the European Parliament's Committee on Budgetary Control (http://www.europarl.europa.eu/activities/committees/presCom.do?language=EN&body=CONT).
[229] De Witte and Rijpma, in Annex B of this volume.

The threat to refuse or delay the discharge of a budget can be used as a tool for requesting changes to the policy, procedures or activities of the agency concerned through its discharge recommendations. By contrast, the CONT may use its discharge reports and resolutions to commend an agency's work. For example, in its report for the discharge of 2009, the CONT complimented Eurojust on its initiative to include 'Key Performance Indicators' in its 2010 plans and recommended this as best practice for the other agencies, allowing relevant stakeholders to better evaluate agencies' performance. It furthermore encouraged agencies to establish multi-annual work programmes.[230]

The refusal to discharge a budget can have major implications, including forcing the relevant director/executive responsible from office.[231] In 2010, parliament refused discharge for the implementation of the European Police College (CEPOL) 2008 budget. This decision was taken on the basis of a negative opinion from the CONT, which was influenced by the LIBE Committee.[232] As a result, the agency's funding was frozen and new management put in place. Discharge for the implementation of CEPOL's 2009 budget was also delayed on the advice of CONT, which deemed the reporting 'insufficient to allow a clear understanding of implementation of concrete actions'.[233]

3.3.2.4. Ad Hoc powers of the European Parliament

On a proposal from the Conference of Presidents, Parliament may at any time set up special committees (formerly known as 'temporary committees'), whose powers, composition and term of office shall be defined at the same time as the decision to set them up is taken; their term of office may not exceed twelve months, except where Parliament extends that term on its expiry.[234] These committees have less powers and less impact when compared to (temporary) committees of inquiry (discussed below).

3.3.2.4.1. Special Committees

Since 1979, thirteen temporary committees have been set up to look into a wide variety of issues ranging from budgetary resources to the impact of the German Unification or the problems and opportunities offered in the area of human genetics. Two temporary committees have, however, dealt with security and intelligence matters. The Temporary committee on the ECHELON interception system was created in 2000 and the Temporary Committee on the alleged use of European countries by the CIA for the transport and illegal detention of prisoners (TDIP) was set up by the EP in 2006.[235] Both inquiries undertook a process of fact-finding to verify whether given activities had taken place and evaluated, among other things, the legality of these activities. It is important to note that these temporary committees primarily dealt with the activities of national intelligence agencies and, to a lesser extent, the Council's knowledge of such activities.[236] They did not, however, address the work of any of the AFSJ bodies as there was no suggestion that they had any involvement in the matters examined by these temporary committees. Indeed, to date, no temporary/special committee has addressed the work of any AFSJ body.

[230] European Parliament Committee on Budgetary Control 7 February 2011.
[231] Interview 3.
[232] De Witte and Rijpma, in Annex B of this volume.
[233] EP Press Release, 11 April 2011.
[234] European Parliament RoP, Rule 184 (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+RULES-EP+20110307+RULE-184+DOC+XML+V0//EN&navigationBar=YES).
[235] European Parliament 2001; European Parliament 2007.
[236] See: Born and Wills 2011, pp. 202–203.

The temporary committees on Echelon and the TDIP were created by resolutions of the EP in response to allegations that illegal activities had taken place which implicated a number of European states. Both committees were seriously hampered by the fact that they were unable to access all necessary information due to a lack of cooperation from many national governments and the Council, and the fact that temporary committees do not have investigatory powers, e.g., subpoena powers and the ability to hear witnesses under affirmation. Consequently, they had to rely on a combination of whistleblowers, work that had already been done by investigative journalists and NGOs, and the goodwill of some national governments and officials.[237] Ultimately, both the TDIP and the temporary committee on Echelon were unable to fully address the issues within their mandates and could not reach definitive conclusions due to a lack of access to information. Moreover, the committees were not able to hold officials in Member States to account because they lacked the powers to compel their appearance before them, as well as to issue binding orders.[238] In spite of these limitations, the temporary committees helped to generate awareness of important concerns on a pan-European level by virtue of their location within international parliamentary assemblies, their multinational composition, and reporting in numerous European languages.[239]

3.3.2.4.2. Committees of inquiry

The European Parliament can also set up committees of inquiry (sometimes known as 'temporary committees of inquiry', which are distinct from temporary committees) to investigate 'alleged contraventions of Union law or alleged maladministration in the application of Union law'.[240] Since the Maastricht Treaty, only three committees of inquiry have been established. These were the inquiry into the Community Transit Regime (TRANSIT),[241] the inquiry into the BSE crisis (ESB1)[242] and an inquiry into the crisis of the equitable life assurance society (EQUI).[243] The requirement that committees of inquiry can only be created to investigate alleged contraventions of Union law has been seen as limiting the potential range of issues which a committee of inquiry could examine, particularly when compared to temporary/special committees which can examine almost anything. Nevertheless, the activities of an AFSJ agency could fall under this category, particularly since the Lisbon Treaty moved the AFSJ from the intergovernmental third pillar into the general framework for EU integration. While the EP has never used a committee of inquiry to examine AFSJ matters, the parliament's power of inquiry is an important tool that could be used to investigate serious problems pertaining to an AFSJ agency.

The Treaty of Maastricht provided the legal basis for the right of the EP to establish such committees of inquiry.[244] Their *modus operandi* are subject to a detailed inter-institutional agreement that governs the exercise of the EP's right to inquiry.[245] Hearings and testimony ordinarily take place in public but proceedings can take place *in camera* if requested by one quarter of the members of the committee of inquiry, by the Community or national authorities, or where the committee of inquiry is considering secret information.[246]

[237] Ibid., pp. 208–211.
[238] For an in-depth analysis of the work of these temporary committees, see: Aidan Wills 2010b.
[239] Ibid.
[240] European Parliament RoP, Rule 185.1.
[241] See (http://www.europarl.europa.eu/comparl/tempcom/transit/default.htm).
[242] See (http://www.europarl.europa.eu/comparl/tempcom/bse/default.htm).
[243] See (http://www.europarl.europa.eu/comparl/tempcom/equi/default_en.htm).
[244] Corbett, Jacobs and Shackleton 2005, p. 296.
[245] Corrigendum to the Decision of the European Parliament, the Council and the Commission of 6 March 1995, p. 1.
[246] European Parliament March 2011, Article 2.

In comparison to temporary/special committees, committees of inquiry have more powers at their disposal. While committees of inquiry do not have a general power of summons, they may invite an institution or a body of the European Communities or the Government of a Member State to designate one of its members to take part in its proceedings.[247] Furthermore, EU authorities and Member States shall provide a committee with the 'documents necessary for the performance of its duties, save where prevented from doing so by reasons of secrecy or public or national security arising out of national or Community legislation or rules'.[248] Further limitations may apply to a committee's access to documents, since EU bodies 'shall not supply the temporary committee of inquiry with documents originating in a Member State without first informing the State concerned'.[249] Needless to say, these provisos could significantly limit their capacity to examine matters relating to the AFSJ bodies because, as was noted in chapter two, much of the information utilised by these bodies comes from Member States.

3.4. Conclusion

This chapter has discussed the role played by the two Joint Supervisory Bodies of Europol and Eurojust in overseeing the processing of personal data by these agencies on an ongoing basis. While it is beyond the scope of this study to conduct a detailed evaluation of the JSBs, indications are that they have the necessary powers in order to fulfil their current mandates. Crucially, the JSBs have access to all files and premises related to the processing of personal data. The JSBs are, moreover, in a strong position to ensure that any practices which violate data protection regulations are corrected. In our view, the JSBs are an appropriate oversight mechanism for scrutinising the use of personal data by the AFSJ agencies. Accordingly, their activities do not need to be duplicated by the EP. Equally, the EP would not need to oversee Frontex's future role in processing personal data because it is envisaged that the European Data Protection Supervisor would perform a similar function to the JSBs. Sitcen cannot process personal data.

In chapter two, we noted that the AFSJ bodies combine intergovernmental and supranational features. On the one hand, these bodies (particularly the AFSJ agencies) are EU entities regulated by EU law and staffed primarily by EU employees. On the other hand, these bodies rely to a large extent on information provided by national authorities, parts of their work are carried out by seconded employees of Member States, and ultimately, it is national authorities that implement measures on the basis of their work —all of these activities are primarily regulated by national law. This has important implications for oversight. Given that national law regulates, inter alia, the sending of information to AFSJ bodies, the use of coercive powers on the basis of information from and/or operations coordinated by AFSJ bodies, it is primarily the prerogative of national judicial bodies and/or other oversight and control mechanisms to ensure that these powers are used lawfully. Currently, it is not clear if and to what extent national bodies, including parliaments, oversee activities of their own state's authorities and employees that have a connection with the AFSJ bodies. In view of the human rights implications of these activities, it would be beneficial for the EP to have more information about this matter from both the perspective of AFSJ bodies and national parliaments. In chapter five we will discuss different options on how the EP can work together with national parliaments in overseeing the AFSJ bodies.

[247] Ibid., Article 3.2.
[248] Ibid., Article 3.4.
[249] Ibid., Article 3.6.

This chapter has shown that the EP already has various oversight mechanisms and powers to oversee the AFSJ bodies. However, we have demonstrated that these mechanisms and powers are not available with regards to all of the AFSJ bodies. For example, the EP does not have uniform powers to summon AFSJ agency directors to engage in a debate with them. The Europol Director is obliged to appear before the EP. By contrast, the President of Eurojust, on behalf of the College, is only expected to 'report to the Council every year on the activities and management, including budgetary management, of Eurojust'. Furthermore, the Frontex Director can only be invited – but not required – to report to the EP. Similarly, the EP has no formal power to summon the director of Sitcen to appear before Parliament.

The EP has formidable budgetary powers vis-à-vis the AFSJ agencies. It can, together with the Council, decide on the amount of money that the agencies can spend from the budget of the European Union. The European Parliament's Committee on Budgets has 'the power of the purse', meaning that money can only be apportioned to an agency once the BUDG committee has passed the EU budget. The EP Committee on Budgetary Control (CONT) scrutinises how the EU budget is spent. The threat to refuse or delay the discharge of a budget can be used as a tool to request changes to the policy, procedures or activities of the agency concerned through its discharge recommendations.

Finally, in case of allegations of serious wrongdoing relating to the AFSJ bodies, Parliament can consider the setting up of a committee of inquiry. Such committees are temporary and may be established on the request of one-quarter of Parliament's Members in the case of alleged infringements of EU law or maladministration in the application of EU law by *inter alia* EU bodies.

This chapter has illustrated that the lack of comprehensive rules on the EP's access to classified information in the AFSJ (and beyond) is perhaps the greatest impediment to effective oversight of the AFSJ bodies. A mandate for the European Parliament to evaluate or scrutinise the performance of AFSJ bodies is of limited use unless it is accompanied by access to the necessary information. Currently, it is clear that there is no single legal framework in place for the EP to access AFSJ-related information (and particularly classified information) from the bodies themselves, the Council, the Commission, and the External Action Service. The AFSJ bodies also lack a uniform system for disclosing classified information. For example, the EP does not have access to threat assessments from Europol or risk analyses from Frontex, which would enable it to understand better the kind of threats faced by the EU and thus the resources and legal powers they may require to counter such threats. Equally, the EP does not have access to evaluation reports of joint operations organised by Europol or Frontex. The situation regarding Sitcen is even more problematic; there is very limited awareness within the EP about the general mandate and powers of Sitcen, let alone more specific information. The EP only has access to classified information related to the policies of the AFSJ bodies from the Council and the Commission on an ad hoc basis. In chapter five we will discuss options on how the EP's access to (classified) information related to the AFSJ bodies could be improved.

While a lack of access to classified information hampers the ability of the EP to oversee the AFSJ bodies. It is important to note, however, that the EP has not yet adopted the necessary information security standards or institutional arrangements in the AFSJ field that would make it easier for relevant committees and MEPs to receive classified information. In the following chapter we will discuss in detail the scope of national parliaments' access to classified information. This will be discussed within the context of a

comparative analysis of the role of specialised oversight bodies in scrutinising national intelligence agencies, with a view to identifying good practices that could be used on the EU level.

CHAPTER 4. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF NATIONAL INTELLIGENCE AGENCIES

4.1. Introduction

This chapter will analyse oversight of national intelligence agencies[250] by parliaments and specialised non-parliamentary bodies.[251] This comparative analysis will examine how oversight is organised and conducted in EU Member States, Australia, Canada and the United States, with a view to identifying common standards and good practices that can inform the EP's approach to the oversight of the AFSJ bodies.

As was mentioned in chapter one, there are profound differences between the role and powers of national intelligence agencies and the EU's AFSJ bodies. Most relevant among these is the fact that while AFSJ bodies cannot use special powers to collect information, this is a crucial—even defining—characteristic of national intelligence agencies. These differences have very important implications for oversight; most significantly, national oversight bodies were primarily established and remain calibrated to ensure that intelligence agencies use special powers in a way that does not violate human rights or compromise legitimate democratic processes. In view of these differences, this chapter will not focus on the oversight of the use of special powers. Equally, it will not focus on the oversight of the use of coercive powers because the majority of intelligence agencies in EU Member States and other democracies do not possess such powers. We will nevertheless, examine the national oversight bodies' scrutiny of certain activities of intelligence agencies that are similar to some of the activities of the EU's AFSJ bodies, namely: information sharing, the collection of open source information, joint analysis and fusion centres, and the use of personal data.

This chapter will, however, primarily focus on the institutional characteristics of national parliamentary and non-parliamentary oversight bodies. The following six aspects of oversight will be addressed: (1) the configuration of these systems; (2) the organisation of specialised parliamentary and non-parliamentary oversight bodies; (3) specialised oversight bodies' mandate and functions; (4) access to classified information by parliaments and specialised oversight bodies; (5) oversight bodies' methods and powers; and (6) protection of classified information handled by these bodies. These issues were identified as being the most pertinent dimensions of national systems of oversight in view of the objective of providing the EP relevant findings to inform its own approach to the oversight of the AFSJ bodies. Before proceeding with an evaluation of these dimensions of oversight, this chapter will first outline a number of reasons for which oversight of national intelligence agencies matters and, indeed, why specialised oversight bodies were created. This discussion is important because it helps to contextualise oversight, which can serve as the basis for a discussion about the rationale for oversight of the AFSJ bodies in chapter five.

[250] The term 'intelligence agencies' is defined, for the purposes of this study, in chapter one.
[251] Note on terminology. The term 'specialised oversight committee/body' is used to refer to parliamentary (sub-) committees which exist to oversee the work of intelligence agencies AND non-parliamentary bodies with the same function. The term specialised refers to the fact that these bodies have a mandate to focus on intelligence agencies. However, we will use the term 'oversight body' to refer to the same actors.

This chapter includes six tables which present various aspects of specialised oversight of intelligence agencies on the national level. These tables were developed on the basis of a questionnaire that was administered to national parliaments in all EU Member States.[252] The information included in the tables is presented as it was provided by national parliaments—it presents their interpretation of, inter alia, the mandate and powers of parliamentary and non-parliamentary oversight bodies. It has not been possible to independently verify the information provided.

4.1.1. The rationale for oversight of intelligence agencies

Many states created parliamentary and other specialised bodies to oversee intelligence agencies in light of revelations about their involvement in illegal and/or improper activities, e.g., Canada, the Czech Republic, Norway, Poland, South Africa, and the US. Notably, during or immediately after the Cold War, it became clear that in many Western states, governments had used intelligence agencies to surveil and disrupt persons involved in legitimate expressions of the rights to freedom of association, assembly and expression.[253] Elsewhere, intelligence agencies were found to have exceeded their legal mandates and powers in tackling domestic terrorism.[254] Perhaps the egregious violations of human rights by intelligence agencies took place in communist/authoritarian regimes, where intelligence agencies were an integral part of the repressive state apparatuses which permeated all areas of society.[255] Against this backdrop, effective oversight (and legal regulation) of intelligence agencies came to be seen as essential for ensuring that they contribute to the security of the populations they serve without undermining democratic processes and human rights. That is, to 'secure democracy against internal and external enemies without destroying democracy in the process'.[256] Needless to say, the development of oversight of the EU's AFSJ bodies is taking place in a vastly different climate from the types of conditions that led to the establishment of oversight bodies on the national level.

Arguments for robust oversight of intelligence agencies can be distilled into five main areas. First, and perhaps most importantly, the law gives most intelligence agencies powers that permit them to restrict human rights and which, if misused, could result in the violation of human rights. Indeed, as Canada's Justice O'Connor stated in the Arar Inquiry: 'national security activities involve the most intrusive powers of the state: electronic surveillance; search, seizure and forfeiture of property; information collection and exchange with domestic and foreign security intelligence and law enforcement agencies; and, potentially, the detention of and prosecution of individuals'.[257] Intelligence agencies are necessarily given a considerable amount of discretion in their use of intelligence collection powers, which increases the scope for such powers to be misused.[258] In view of this, oversight is necessary to help ensure that such powers are used in accordance with national and international law.[259]

[252] This questionnaire can be viewed in Annex C.
[253] See, for example, the findings and recommendations of: United States Senate 1976; Lund Commission 1996.
[254] See, for example, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police 1981 [hereafter, the McDonald Commission].
[255] See, for example, Williams and Deletant 2001; South African Truth and Reconciliation Commission 1998, chapter 8.
[256] McDonald Commission, p. 43. See also: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 2006, p. 425 [hereafter, the Arar Inquiry].
[257] Arar Inquiry, pp. 425–426.
[258] Venice Commission Report 2007, pp. 13, 18.
[259] United Nations Human Rights Council 17 May 2010, p. 9; Arar Inquiry, p. 426; Krieger 2009, p. 211.

Second, on a national level, the political misuse of intelligence agencies has always been a risk, primarily because these agencies can be used to unlawfully gather information about political opponents.[260] Oversight is seen to be an essential safeguard against incumbent governments using intelligence agencies to protect or promote party political interests. This is less of a concern at the EU level because there is not the same direct relationship of control between the executive and the agencies. Perhaps more importantly, the fact that 27 Member States, the Commission and Council are all involved in the political control of these agencies means that there are in-built checks and balances against there (mis)use by any one party or interest group.

Third, the secrecy surrounding national intelligence agencies shields them from the processes of public accountability which apply to public bodies in democracies. For example, these agencies are not usually particularly open with the media and are often exempt from freedom of information legislation.[261] This makes it difficult for the media, civil society organisations and the public more generally to scrutinise the intelligence agencies' work.[262] This further increases the need for oversight by independent bodies that have access to information not available to the general public.

Fourth, in common with all public bodies, intelligence agencies are funded with public money and should therefore be held to account for their use of this money. There is particular need for oversight given that intelligence agencies are normally authorised to make secret payments to covert agents. The potential for the inappropriate use of money is heightened in this area. Robust oversight is necessary to ensure that intelligence agencies use public money lawfully and efficiently.[263]

Finally, while oversight is often seen as necessary to guard against the misuse of, and abuse by, intelligence agencies, it also helps to ensure that these agencies fulfil their mandates effectively.[264] Intelligence agencies are, inter alia, entrusted with collecting, analysing and disseminating information about very serious threats to national security and public safety, such as terrorism. The executive and other agencies, such as the police, rely on the information provided by intelligence agencies to take action to combat these threats. Failures by intelligence agencies to perform such functions effectively, e.g., by missing information indicating a terrorist attack, can have catastrophic consequences.[265] Independent oversight of the work of intelligence agencies helps to ensure that they are as effective as possible.

4.2. Systems for intelligence oversight

On a national level, there are generally six actors involved, in some way, in the oversight of intelligence agencies: the internal management of these agencies, the political executive, the judiciary, parliament, autonomous institutions such as ombudsmen and supreme audit institutions, and the media and civil society.[266] While each of these actors fulfil important and often mutually complementary oversight functions, this study will only address the oversight of intelligence agencies by parliaments (particularly specialised parliamentary

[260] Venice Commission Report 2007, p. 13.
[261] Arar Inquiry, p. 428.
[262] Venice Commission Report 2007; see, in Annex A of this volume, Földvary, Annex A.
[263] Wills 2010; United Nations Human Rights Council 17 May 2010, p. 9.
[264] Krieger 2009, p. 211; United Nations Human Rights Council 17 May 2010, p. 9.
[265] See, for example: National Commission on Terrorist Attacks Upon the United States 2004, Chapter 13.
[266] For an overview of the role played by these different actors see, *inter alia*: Venice Commission Report 2007; Wills 2010; Born and Leigh 2005; South African Ministerial Review Commission on Intelligence 2008.

oversight committees), and specialised bodies created by parliament with a specific mandate to oversee intelligence agencies. The rationale for this focus is the mandate given to us by the EP, which is outlined in chapter one.

Most states have a range of parliamentary and specialised oversight bodies that are responsible for scrutinising various aspects of the work of intelligence agencies. These bodies can be divided into three main categories, which will be discussed in this section: (1) general parliamentary committees; (2) specialised parliamentary oversight committees; and (3) specialised non-parliamentary oversight bodies.

4.2.1. General parliamentary committees

In most states, a number of parliamentary committees are competent to oversee some aspects of intelligence agencies' work. For example, committees responsible for policy areas such as home affairs, security, justice and defence may take an interest in intelligence agencies—in many cases, such committees have overlapping jurisdictions. Similarly, committees on cross-cutting issues, such as human rights, may review aspects of intelligence agencies' work on an ad hoc basis.[267] In addition, committees responsible for budgets and public accounts are competent to oversee the finances of intelligence agencies. However, the committees discussed above provide only perfunctory oversight of intelligence agencies because they typically handle numerous other issues and often lack the time, resources, access to classified information and/or knowledge to focus on these agencies.

4.2.2. Specialised parliamentary committees

In view of the fact that parliamentary committees with broad mandates—in areas such as home affairs, homeland security and justice—are not well suited to overseeing intelligence agencies, many democratic states have opted to establish specialised oversight committees within parliament to oversee intelligence agencies (see Table 1, below). Such committees are normally full committees of parliament rather than sub-committees of committees which have broad mandates that may encompass intelligence matters. The parliaments of Canada and Sweden are examples of exceptions to this trend—they have no specialised committee for the oversight of intelligence agencies.[268]

Specialised parliamentary oversight committees are often mandated to oversee one or more intelligence agencies in general terms (see section 4.4. Mandate and functions of specialised oversight bodies) but may also be given a mandate to oversee a specific aspect of an agency such as its finances. Parliamentary oversight committees are normally established through a statute (e.g., Spain and Italy) but may also be based on parliament's own rules of procedure (e.g., the Netherlands), and in some cases specialised parliamentary oversight committees may even be grounded in the constitution (e.g., Germany).[269]

In many democratic states there is one specialised parliamentary oversight body responsible for scrutinising all intelligence agencies, or specific intelligence functions regardless of which public bodies perform them.[270] Such committees are often joint

[267] See, for example, the British Parliament's Joint Select Committee on Human Rights.
[268] See in this volume: Forcese, Annex A; Cameron, Annex A.
[269] See in this volume: Sanchez, Annex A; Fabbrini and Giupponi, Annex A; Verhoeven, Annex A.
[270] Venice Commission Report 2007, p. 33.

committees, drawing members from both houses of bicameral parliaments, e.g., the Italian parliament's oversight committee (COPASIR) and the Australian parliament's Permanent Joint Committee on Intelligence and Security.[271] In some states, committees that oversee several agencies and activities are only located with one house of a bicameral parliament, e.g., the German *Bundestag's* Parliamentary Control Panel and the Dutch *Tweede Kamer's* Committee on Intelligence and Security Services. A variation of this approach is to have one specialised oversight committee in both houses of a bicameral parliament, each with responsibility for overseeing a broad gamut of agencies and functions. The US Congress is the best example of this with the Senate Select Committee on Intelligence, and the House of Representatives Permanent Select Committee on Intelligence. Finally, some parliaments have opted to create several parliamentary committees, each with an agency-based mandate meaning that they are exclusively responsible for the oversight of a specific agency. The Czech Republic, Romania and Slovakia are examples of states that follow this approach.[272]

Due to the secrecy that surrounds many oversight bodies, it is difficult to evaluate an oversight body's work with any degree of certainty therefore it is hard to compare the performance of two bodies or models. However, it is often regarded as good practice to have one single committee responsible for the oversight of all intelligence agencies and functions as this helps to ensure 'seamless' oversight, avoiding the risk that certain issues fall between the purviews of two or more committees.[273] Oversight may become fragmented if too many committees are involved.[274] On the other hand, one may argue that having several committees which each focus on one intelligence agency allows overseers to focus their time and resources on a smaller range of issues, as well as to specialise in the work of a particular agency.

Specialised parliamentary committees for the oversight of intelligence agencies have a number of advantages in comparison to non-parliamentary oversight bodies (which are discussed in the next sub-section). Most notably, they can be viewed as providing the most 'democratic' approach to oversight because oversight is performed by directly elected representatives of the population.[275] Oversight involving a number of political parties can help to ensure that intelligence agencies serve the interests of society as a whole rather than an incumbent government—the involvement of opposition parties in oversight committees can serve as a valuable counterweight to a governing party's position in the intelligence domain. In addition, parliaments are well placed to ensure that oversight processes have an impact, i.e., the findings and recommendations of a committee acted upon by the executive and intelligence agencies. Indeed, parliaments have numerous tools in this regard including their budgetary appropriation and discharge powers, as well as the possibility of amending the legislation which regulates intelligence agencies.

There are, however, a number of significant drawbacks to vesting intelligence oversight agencies in a specialised parliamentary committee. First, parliaments are, by definition, forums for pursuing partisan political interests; in most parliaments, MPs seek to further the interests of their political party/group to the detriment of the interest of other parties. These aims are often not necessarily compatible with the demands of conducting effective, independent oversight, which requires parliamentary committees to scrutinise the work of

[271] See, in this volume: McGarrity, Annex A; Fabbrini and Giupponi, Annex A.
[272] Responses to the DCAF-EUI Questionnaire from the parliaments of the Czech Republic, Romania and Slovakia.
[273] Venice Commission Report 2007, p. 33; see also, the Arar Inquiry.
[274] See, in this volume: Lepri, Annex A.
[275] See, for example, Venice Commission Report 2007, paras. 227–228; Whitaker and Farson 2009, p. 3.

the executive and its agencies according to objective, legally defined criteria.[276] For example, MPs that are part of the governing party may not be inclined to shed light on issues or events that are likely to be damaging to the government. By contrast, MPs from opposition parties sometimes seek to use their position on an oversight committee for political gain, e.g., by using the powers of their committee position to compel testimony from government ministers on issues wherein they hope to derive a partisan advantage. The (in)stability of parliamentary politics is another drawback to parliamentary oversight of intelligence agencies; notably, where there are newly started 'maverick' populist parties, the risks of leaking of information for political or other gain may be greater.

Second, parliamentarians have numerous demands on their time. They are often members of several committees, have to spend time in plenary debates, and have to combine this with the responsibility of engaging with and representing their constituents. These demands on parliamentarians' time make it difficult for members of intelligence oversight committees to spend significant time conducting detailed oversight of intelligence agencies.[277] This is particularly evident when one compares the amount of time members of parliamentary oversight committees spend scrutinising the work of intelligence agencies with time available to 'professional' overseers, i.e., members of non-parliamentary oversight bodies. Time constraints on oversight are further increased when members of specialised parliamentary oversight bodies are also party/group leaders or spokespersons within a chamber. This is the case, for example, with the Dutch parliament's Intelligence and Security Services Committee, the Spanish parliament's Secret Funds Committee, and some members of the French parliament's *Délegation parlementaire au reseignement*.[278] An inevitable consequence of the numerous demands on MPs' time is that parliamentary oversight committees meet less often than their counterparts in non-parliamentary oversight committees. For example, the German *Bundestag's* Parliamentary Control Panel—one of the strongest examples of a specialised parliamentary oversight committee—meets only once per month.[279] While this frequency of meetings is entirely understandable in view of the competing demands on MPs' time, the lack of continuity can have a detrimental impact upon the quality and consistency of democratic oversight.

A third drawback—which is largely related to the fact that MPs cannot devote much time to oversight—is that MPs often lack the expertise that is necessary to understand intelligence agencies.[280] Intelligence agencies utilise methods for collecting information which are likely to be unfamiliar to most MPs; indeed, this is particularly true given that these agencies now make use of a vast array of advanced technologies.[281] MPs are unlikely to have significant knowledge of such matters when they take up their positions on an oversight committee, and may not have the time to spend learning about them. This problem is further compounded by the relatively short tenures of committee membership, due to frequent elections or the desire of party leaderships to rotate their members between committees in parliament.[282] A lack of knowledge of intelligence matters can make it very difficult for MPs to conduct effective oversight and increases the risk that agencies may exploit overseers' lack of knowledge of the agencies to conceal particular issues. Some states have sought to address this problem by ensuring that members of parliamentary oversight committees have security-related expertise, e.g., by virtue of being a former minister with a security or

[276] See, for example: Whitaker and Farson 2009, p. 3; in this volume, Martin, Annex A; Wills 2010, pp. 42–43.
[277] See, in Annex A of this volume: Cameron; Lepri, p. 7; Sanchez; Verhoeven.
[278] See, in Annex A of this volume: Verhoeven; Lepri; Sanchez.
[279] See, in Annex A of this volume, De With and Kathmann.
[280] See, in Annex A of this volume: Cameron.
[281] European Court of Human Rights June 2006, para. 9.
[282] Wills 2010, p. 43.

intelligence portfolio.[283] Parliaments can also compensate for MPs' lack of knowledge of intelligence agencies by ensuring that committees are supported by an expert staff (see section 4.3.5).

4.2.3. Specialised non-parliamentary oversight bodies

An increasing number of states have established specialised non-parliamentary bodies to oversee intelligence agencies; these are sometimes referred to as 'expert' oversight bodies.[284] These bodies are usually committees (such as the Belgian Standing Intelligence Agencies Review Committee – Committee I) or individual commissioners supported by a staff (e.g., the UK's Intelligence and Interception of Communications Commissioner). Specialised non-parliamentary oversight bodies are permanent bodies, established through legislation, which conduct oversight on an ongoing and even full-time basis. They may be created in addition to some form of parliamentary oversight committee (e.g., in the Netherlands). Other states (e.g., Canada) have opted to almost entirely 'outsource' oversight to a specialised autonomous body and do not have any specific parliamentary committee for the oversight of intelligence agencies.[285] These bodies are generally organisationally and operationally independent from parliament and the political executive. Accordingly, they act autonomously in decision-making processes, including deciding which matters to investigate and report on, and often have their own budgets approved by parliament. It should be noted that there are examples of 'hybrid' bodies which combine features of parliamentary and non-parliamentary oversight committees (see below, section 4.3.3).

Specialised non-parliamentary bodies have a number of advantages in comparison to parliamentary oversight committees, which are the inverse of the drawbacks associated with parliamentary oversight that were discussed above. First, they are normally professional bodies whose members do not have other occupations. This means that they have more time to dedicate to oversight.[286] Second, members of non-parliamentary oversight bodies usually have a much longer tenure of membership which gives them the opportunity to develop expertise over time.[287] They also have fixed tenures of office, which means that their position is not normally dependent upon changes in government or changes in the balance of power in parliament.[288] Oversight by non-parliamentary bodies is continuous: it does not halt when parliament is in recess or dissolve for elections.[289] Third, in many cases, members are selected on the basis of their qualifications rather than their positions within a political party or parliamentary caucus.[290] Frequently, it is a requirement that members possess particular qualifications (see below section 4.3.4 for more details). This helps to ensure that members have the requisite expertise to conduct effective oversight of intelligence agencies.

Fourth, members of specialised non-parliamentary oversight bodies are generally regarded as being more independent than members of parliamentary bodies because they do not

[283] See Ian Leigh's comments in this regard in Annex A of this volume.
[284] Venice Commission Report 2007, paras. 218–240.
[285] See, Forcese in Annex A of this volume.
[286] Venice Commission Report 2007, p. 48.
[287] Wills 2010, p. 43.
[288] See, for example, the Canadian Security Intelligence Service Act (CSIS Act), Section 34(2) and Belgium's Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 30.
[289] See, in Annex A of this volume: Van Laethem. It should be noted, however, that the German Bundestag has adopted measures to ensure that the Parliamentary Control Panel remains functional even when parliament is in recess or during elections (see, in Annex A of this volume, De With and Kathmann).
[290] See, in Annex A of this volume: Van Laethem.

hold political office and/or operate in an environment where oversight can be used for political gain.[291] In fact, there are often strict safeguards to ensure that members do not engage in any other activities which could compromise their position. For example, they may be barred from holding elected office and/or having private business interests for the duration of their membership.[292] Nevertheless, the independence of non-parliamentary specialised bodies still depends, to a large extent, on the individuals appointed by parliament and/or the executive. Indeed, in states where such oversight bodies are appointed exclusively by the executive, it is potentially easier to ensure that overseers are 'government friendly' than with parliamentary oversight committees, which must include representation from a number of parties (see section 4.3.4). An additional drawback to non-parliamentary oversight bodies is that they may be perceived to lack democratic legitimacy. Unlike members of parliamentary oversight committees, members are not directly elected. Consequently, overseers are further removed from the public on whose behalf they conduct oversight.[293]

[291] Venice Commission Report 2007, paras. 218–219; Wills 2010, pp. 40–43.
[292] See, in Annex A of this volume: Verhoeven.
[293] Venice Commission Report 2007, p. 50.

Table 1: Specialised committees responsible for the oversight of intelligence agencies

STATE	Type of Oversight Committee	Number of Members	Number of Staff	Rules on membership	Mandate	Appointed by	Agencies overseen
Austria - *Standing Subcommittee of the Interior Affairs Committee*	Parliamentary Committee	16	2	• Proportional representation • Guaranteed representation of opposition or minority parties	• Oversees policies; completed and ongoing operations; and administration and management of the agency	Parliament	Federal Agency for State Protection and Counter Terrorism
Belgium - *Standing Intelligence Agencies Review Committee*	Non-parliamentary committee	3	10	• Members cannot hold elected office • Requirement that some members are members of the legal profession	• Oversees policies; completed and ongoing operations; administration and management; and budgets and expenditure of the agencies • Investigates complaints from the public • Advises on draft legislation or statutory amendments	Parliament	State Security (the civil intelligence and security service) and the General Intelligence and Security Service of the Armed Forces (the military intelligence and security service) Coordination Unit for Threat Assessment (CUTA) (joint analysis centre/fusion centre)
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	Parliamentary Committee	22	5	• Proportional representation	• Oversees policies; completed and ongoing operations; administration and management; and budgets and expenditure of the agencies	Parliament	National Intelligence Service, the National Service for Protection and the Military Information Service of the Ministry of Defence
Cyprus							
Czech Republic - *Permanent Commission on Oversight over the work of the Security Information Service (BIS)*	Parliamentary Committee	7	1	• Proportional representation, elected by the Chamber of Deputies	• Oversees policies; completed operations; administration and management; and budgets and expenditure of the agency	Parliament	Security Information Service (BIS)
Denmark - *The Folketing's Committee on the Danish Intelligence Services*	Parliamentary Committee	5	2	• Every party has one member	• Subject of the committee's oversight not specified • Receives briefings on the work of the services	Parliament	The Danish Security and Intelligence Service (PET) and the Danish Defence Intelligence Service (FE)
Estonia - *Security Authorities Surveillance Select Committee*	Parliamentary Committee	6	2	• Proportional representation	• Oversees policies; completed and ongoing operations; administration and management; and budgets and expenditure of the agencies • Investigates complaints from the public • Draft legislation or statutory amendments • Issue opinions on draft legislation	Parliament	Security Police Board and the Information Board
Finland - *The Administration Committee*	Parliamentary Committee	17	5	• Proportional representation	• Oversees policies; completed and ongoing operations; administration and management; and budgets and expenditure of the agency • Draft legislation or statutory amendments	Parliament	The Finnish Intelligence Service (= The Finnish Security Police)
France - *Commission des Lois*	Parliamentary Committee	73	18	• Proportional representation	• Oversees policies; administration and management; and budgets and expenditure of the agencies • Draft legislation or statutory amendments	Parliament	*Services du Ministère de l'Intérieur*

STATE	Type of Oversight Committee	Number of Members	Number of Staff	Rules on membership	Mandate	Appointed by	Agencies overseen
Germany - *Parliamentary Control Panel (PKGr),*	Parliamentary Committee	11	9	• Proportional representation • Change of chairman between majority and minority party every year	• Oversees policies; completed and ongoing operations; administration and management • Investigates complaints from the public	Parliament	Federal Office for the Protection of the Constitution, the Military Counter-Intelligence Service and the Federal Intelligence Service
Germany - *G10 Commission*	Non-parliamentary committee	8	9	• Proportional representation • Membership can include parliamentarians	• Oversight and authorisation of surveillance measures restricting the privacy of correspondence, posts and telecommunications • Investigates complaints from the public	Parliamentary Control Panel (PKGr)	Federal Office for the Protection of the Constitution, the Military Counter-Intelligence Service and the Federal Intelligence Service and selected law enforcement agencies
Greece - *Special Standing Committee for Institutions and Transparency*	Parliamentary Committee	13	(Information not provided)	• Proportional representation • Two Vice-Chairpersons and one Secretary of the Committee are elected from the first, second and third, respectively, parliamentary parties of the opposition	• Oversees policies; administration and management; and the legitimacy of the activities of the agency	President of Parliament	The National Intelligence Service
Greece – *Authority for Communication Security and Privacy (ADAE)*	Non-parliamentary committee	14	52	• Requirement that members have "broad social acceptance" and specific legal and technical expertise	• Oversees the lawful interception of communications activities • Investigates complaints from the public	Designated by Parliament and appointed by the Minister of Justice, Transparency and Human Rights	The National Intelligence service (NIS), Ministry of Citizen Protection – Hellenic Police, Ministry of Citizen Protection – State Security Division
Hungary - *Committee on National Security*	Parliamentary Committee	12	2	• Guaranteed representation of opposition or minority parties • Committee is chaired by a member of an opposition party	• Oversees policies; completed operations; administration and management; and budgets and expenditure of the agencies • Investigates complaints from the public	Parliament	Information Office, Constitution Protection Office, Military Intelligence Office, Military Security Office, Specialised National Security Office and National Security Authority
Ireland							
Italy - *COPASIR*	Parliamentary Committee	10	6	• Committee is chaired by a member of an opposition party • Majority and opposition party have same number of members	• Oversees policies; completed operations; administration and management; and budgets and expenditure of the agencies • Investigates complaints from the public • Draft legislation or statutory amendments • Advises on draft legislation	Speaker of the Chamber of Deputies and the Speaker of the Senate	Security Intelligence Department (DIS), External Intelligence and Security Agency (AISE) and Internal Intelligence and Security Agency (AISI)
Latvia - *National Security Committee*	Parliamentary Committee	5	1	• One member from each political group	• Oversees policies; completed and ongoing operations; administration and management; and budgets and expenditure of the agency • Draft legislation or statutory amendments • Investigates complaints from the public	Parliament	National Security Defense Agency

STATE	Type of Oversight Committee	Number of Members	Number of Staff	Rules on membership	Mandate	Appointed by	Agencies overseen
Lithuania - *Committee on National Security and Defence*	Parliamentary Committee	10	6	• Proportional representation	• Oversees policies; administration and management; and budgets and expenditure of the agencies • Draft legislation or statutory amendments	Parliament	The State Security Department (SSD), The Second Investigation Department (SID) under the Ministry of Defense (military intelligence and counter-intelligence)
Luxembourg							
Malta							
The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	Non-parliamentary committee	3	6	• Requirement that some members are members of the legal profession • Members are not parliamentarians	• Oversees policies; completed and ongoing operations of the agencies • Investigates complaints from the public	Combination of Parliament, Head of Government and responsible Minister	AIVD (General Intelligence and Security Service) and MIVD (Defence Intelligence and Security Service) The Counter-Terrorism Infobox (joint analysis centre/fusion centre)
Poland (Sejm) - *Special Services Oversight Committee*	Parliamentary Committee	7	9	• Proportional representation • Guaranteed representation of opposition or minority parties	• Oversees policies; completed operations; administration and management; and budgets and expenditure of the agencies • Investigates complaints from the public • Draft legislation or statutory amendments	Parliament	Intelligence Agency, Defense Intelligence Agency, National Security Agency, the Military Counterintelligence Services, Central Anticorruption Bureau Centrum Antyterrorystyczne (CAT) (joint analysis centre/fusion centre)
Poland (Senate) - *Human Rights, Rule of Law and Petitions Committee*	Parliamentary Committee	7	2	• Guaranteed representation of opposition or minority parties	• Investigates complaints from the public • Draft legislation or statutory amendments	Parliament	Agency of Internal Security, Intelligence Agency, Central Anti-Corruption Bureau
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*	Non-parliamentary committee	3	1	• Members are elected by a qualified majority in Parliament	• Oversees policies; administration and management; and budgets and expenditure of the agencies • Investigates complaints from the public • Issues opinions on draft legislation	Parliament	Security Intelligence Service (SIS), Defence Strategic Intelligence Service (SIED) and Military Intelligence Center (CISMIL)
Romania – *The Committee for Defence, Public Order and National Security*	Parliamentary Committee	24	7	• Proportional representation	• Oversees policies; completed and ongoing operations; administration and management; and budgets and expenditure of the agencies • Investigates complaints from the public • Draft legislation or statutory amendments	Parliament	The Special Communications Service, the Protection and Guard Service, the Defence Intelligence General Directorate within MoD, and the General Directorate for Intelligence and Internal Protection within MoI
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	Parliamentary Committee	9	3	• Proportional representation	• Oversees completed operations; administration and management; and budgets and expenditure of the agency • Investigates complaints from the public • Draft legislation or statutory amendments	Parliament	The Romanian Intelligence Service (SRI)
Slovakia - *Committee for the oversight of the Slovak Information Service*	Parliamentary Committee	13	2	• Proportional representation • Guaranteed representation of opposition or minority parties • Committee is chaired by a member of an opposition party	• Oversees policies; administration and management; and budgets and expenditure of the agency • Investigates complaints from the public • Draft legislation or statutory amendments	Parliament	Slovak Information Service

STATE	Type of Oversight Committee	Number of Members	Number of Staff	Rules on membership	Mandate	Appointed by	Agencies overseen
Slovakia - *Committee for the oversight of the National Security Authority of Slovak Republic*	Parliamentary Committee	13	2	• Proportional representation • Guaranteed representation of opposition or minority parties • Committee is chaired by a member of an opposition party	• Oversees policies; administration and management; and budgets and expenditure of the agency • Investigates complaints from the public • Draft legislation or statutory amendments	Parliament	National Security Authority
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	Parliamentary Committee	7	2	• Guaranteed representation of opposition or minority parties • Committee is chaired by a member of an opposition party • Opposition parties have a majority of members	• Oversees policies; budgets and expenditure of the agencies • Investigates complaints from the public	Parliament	Civil Intelligence and Security Service (SOVA – the Slovene Intelligence and Security Agency), Military Intelligence and Security Service (OVS – the Intelligence and Security Service of the Ministry of Defence) and Criminal Investigation Police (the internal security service, part of the General Police Directorate within the Ministry of the Interior)
Spain							
Sweden - *The Committee on Justice*	Parliamentary Committee	17	7	• Proportional representation	• Oversees policies; budgets and expenditure of the agency • Draft legislation or statutory amendments	Parliament	The Swedish Security Service
Sweden - *The Commission on Security and Integrity Protection*	Non-parliamentary committee	10	7	• Requirement that some members are members of the legal profession • Membership can include parliamentarians	• Oversees completed and ongoing operations of the agencies • Investigates complaints from the public	Government	The Swedish Security Service (the Security Police), The Commission also supervises the use of crime fighting agencies' use of secret surveillance and qualified assumed identities and associated activities.
The UK - *Intelligence and Security Committee (ISC)*	Non-parliamentary committee	9	6	• Proportional representation • Members are parliamentarians • At least one Member from the House of Lords	• Oversees policies; administration and management; and budgets and expenditure of the agencies	Parliament/ Head of Government	Security Service (MI5), Secret Intelligence Service (MI6), Government Communications Headquarters (GHCQ), Defence Intelligence, Joint Intelligence Committee (JIC); Joint Terrorism Analysis Centre (JTAC) (joint analysis centre/fusion centre)

4.3. Organisation of specialised oversight bodies

This section will analyse the organisation of specialised parliamentary and non-parliamentary oversight bodies. We will begin by looking at the characteristics of oversight bodies' membership and will then examine the different processes through which members are selected. This section will also address the resources required by specialised oversight bodies.

4.3.1. Composition of parliamentary oversight committees

Specialised parliamentary oversight committees are, of course, made up of MPs. Looking at Table 1, it is evident that the size of these committees varies from 5 to 24, with most committees having between 10 and 15 members.[294] Oversight committees are generally smaller than other parliamentary committees. This may be explained by the fact that these committees are responsible for a relatively narrow set of issues. However, smaller committees may also be better suited for dealing with highly sensitive issues and classified information. A smaller group of MPs may find it easier to garner the trust and acceptance of the executive and intelligence agencies when it comes to handling sensitive information. That being said, in most parliaments it is seen to be necessary to ensure that all parties are represented on committees.

Most specialised parliamentary oversight committees are full committees rather than sub-committees and can theoretically contain any member of parliament. There are, however, two other notable approaches to the composition of such committees. In the Dutch parliament, the *Tweede Kamer's* Intelligence and Security Services Committee is composed of the leaders of all parties in parliament.[295] The Spanish *Cortes Generales* has a similar model which applies to its Secret Funds Committee. The plenary of parliament elects, by a 3/5 majority, one MP from each group in parliament to have full access to classified information; this group of MPs (and the speaker) constitutes the Secret Funds Committee which oversees various aspects of the intelligence agencies' work.[296] While the MPs selected through this process are not necessarily the party leaders, in practice they have been what Susana Sanchez describes as party 'spokespersons' in parliament.[297] The involvement of party leaders or other senior MPs in oversight committees may help to raise the profile of oversight of intelligence agencies, ensuring it remains on parliament's 'radar'. However, as was already noted, senior MPs may not have the time to dedicate to the work of an oversight committee and, as a result, oversight may be perfunctory.

A third approach is to combine MPs selected for an oversight committee with *ex officio* members who are either drawn from other committees or part of the

[294] Please note that the French National Assembly's '*Commission Des Lois*' is an outlier and should not be considered a specialised oversight committee because it plays a very limited role in the oversight of intelligence agencies and its mandate is much broader than this role. See the website of *la commission des lois* for an overview of the committee's mandate: (http://www.assemblee-nationale.fr/commissions/59051_tab.asp). In France, parliamentary oversight is now performed by the *Délégation parlementaire au renseignement* (see, in Annex A of this volume, Lepri).
[295] The Netherlands, Rules of Procedure of the Dutch Second Chamber 1994, Sections 16 and 22.
[296] See, in Annex A of this volume: Sanchez.
[297] Ibid.

committee by virtue of their position as speaker (e.g., the French parliament's *Délégation parlementaire au renseignement*).[298] For example, in the US Congress, members of the Judiciary, Appropriations, Armed Services and Foreign Relations Committees (from both chambers) are included in the US congressional intelligence committees.[299] This practice of including MPs from several relevant committees may help to ensure better coordination between an oversight committee and committees dealing with related issues, e.g., budgetary oversight or home affairs.

4.3.2. Chairpersonship of parliamentary oversight committees

With regards to the chairpersonship, parliamentary oversight committees typically adopt one of three approaches. Most commonly, the committee is chaired by a member of the largest or governing party in parliament, e.g., the US Congressional Intelligence Committee and the French parliament's *Délégation parlementaire au renseignement*. An alternative approach is for a member of an opposition party to chair parliamentary oversight committees; this is a requirement in a number of EU Member States including Italy, Hungary, Slovakia and Slovenia.[300] This practice can provide a counterweight to government control of intelligence agencies. If the opposition chairs an oversight committee, the governing party(ies) cannot use its (their) majority to impede the oversight of intelligence agencies if, for example, they wish to prevent the examination of potentially embarrassing issues.[301] A final approach, which is used in the German *Bundestag's* Parliamentary Control Panel, is for the chairpersonship to rotate between the governing and an opposition party.[302]

4.3.3. Composition of non-parliamentary oversight bodies

Non-parliamentary oversight bodies normally have fewer members than their parliamentary counterparts, e.g., the Dutch Review Committee on the Intelligence and Security Services (CTIVD) has three members, the Belgian Committee I (three), and the Council for the Oversight of the Intelligence System of the Portuguese Republic (three) (see Table 1). The members of these bodies typically include senior figures who are (semi)-retired from other vocations. Given that these bodies often have a mandate to scrutinise, among other things, the legality of the agencies' work, there is often a requirement that at least one member is a senior lawyer or a member of the judiciary.[303] Elsewhere, there are requirements for the membership to include people from other vocations, for example, members of the Greek Authority for Communication Security and Privacy must be 'distinguished scientists and professionals in the legal and technical sector of communications'.[304] Similarly, Croatian law requires that members of the Council for the Civilian Oversight of the Security Intelligence

[298] See, in Annex A of this volume: Lepri.
[299] See, in Annex A of this volume: Martin.
[300] Responses to the DCAF-EUI questionnaire, question 17, from the parliaments of Hungary, Italy, Slovakia and Slovenia; see also, Hungary, Act No. CXXV of 1995, Section 14(1); Italy, Law 14/2007, 3 August 2007, Article 30(3).
[301] See, in Annex A of this volume: Földvary; Fabbrini and Giupponi.
[302] See, in Annex A of this volume: De With and Kathmann.
[303] For example: The Netherlands, Intelligence and Security Services Act 2002, Article 65(4); Sweden, Act on Supervision of Certain Crime Fighting Activities, p. 980, Section 5.
[304] Response to the DCAF-EUI questionnaire, question 17 from the Hellenic Authority for Communication, Security and Privacy (ADAE).

Agencies have a background in political science, electro-technical sciences, as well as law.[305] These requirements are intended to ensure that oversight bodies include persons with the relevant expertise to both understand and evaluate the activities of intelligence agencies.

The composition of non-parliamentary oversight bodies differs in terms of whether or not they can include parliamentarians. In most cases, sitting parliamentarians are not permitted to serve on specialised non-parliamentary oversight bodies.[306] A second possibility is what Iain Cameron describes as a 'hybrid body', which can include both parliamentarians and non-parliamentarians.[307] The Swedish Commission on Security and Integrity Protection, the German G10 Commission, and the Norwegian EOS-Utvalget Committee are examples of bodies with a hybrid composition. Finally, and somewhat paradoxically, a non-parliamentary oversight body may be made up exclusively of parliamentarians. For example, the UK's Intelligence and Security Committee states that it is a non-parliamentary body but its members must be members of the House of Commons or the House of Lords.[308] Given that non-parliamentary oversight is generally intended to provide impartial, independent oversight, it may seem odd that parliamentarians can be members. Yet, there can be advantages to inclusion of parliamentarians in what are ostensibly non-parliamentary bodies as it balances legitimacy with expertise. The Norwegian and Swedish examples show that this model can work where the separation of powers is not an important concern and constitutional controls mean that the risk of 'political policing' is low. However, the authors are of the view that political oversight involving parliamentarians is generally best located within parliament, and should be supplemented by a committee of apolitical experts outside parliament.

4.3.4. Selection of members of specialised oversight bodies

The process through which members of oversight bodies are selected is important because in order for oversight to be effective it is necessary to select overseers who: a) have the necessary knowledge of and interest in intelligence matters; b) have the will to engage in oversight in an impartial manner; and c) can command the respect and trust of the intelligence agencies.

Members of parliamentary oversight committees are, of course, selected through parliament but there are a number of different methods for doing so—these are often different to those which apply to the selection of members for other parliamentary committees.

One approach is for members to be appointed by a simple majority in parliament; this is, for example, the case for the German *Bundestag's* Parliamentary Control Panel. According to Hans De With and Erhard Kathmann, this is an important check which helps to ensure that only the most professional and trusted members

[305] Croatia, Act on the Security Intelligence System, Article 110(3).
[306] See, for example: Belgium - Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 28(6); Canada, CSIS Act, Article 34(1).
[307] See, in Annex A of this volume: Cameron.
[308] Response to the DCAF-EUI questionnaire, question 14, from the UK Intelligence and Security Committee.

of the *Bundestag* are elected to the Panel.[309] This selection method also helps to ensure that members of oversight committees enjoy broad support from their peers. The Spanish *Cortes Generales* uses a similar approach: the plenary of parliament elects one MP by a 3/5 majority from each party to have access to the highest levels of classified information and thus, by default, to serve as a member of the Secret Funds Committee. This high threshold is considered to be particularly important in Spain due to concerns about giving members of the political group associated with the terrorist group ETA access to classified information regarding the intelligence agencies.[310]

Elsewhere, members of parliamentary oversight committees are selected by the party leadership within parliament, e.g., in the US Congressional intelligence committees and the Hungarian National Security Committee.[311] Another approach is for the speaker of parliament to select members of oversight committees, as in the case for the French parliament's *Commission de verification des fonds speciaux* and the Italian parliament's COPASIR.[312] Finally, in some Westminster systems, e.g., Australia, the prime minister appoints members of parliamentary oversight committees following consultation with opposition parties.[313] The latter three methods of selection are all means to ensure that only parliamentarians that are deemed to be 'appropriate' and sufficiently senior are appointed to oversight committees. However, they can all be manipulated by governing parties to ensure that members of oversight committees are, inter alia, sympathetic to the government on matters of security and unwilling take a very critical approach towards intelligence agencies. In other words, members may not necessarily be selected on the basis of their knowledge of intelligence matters or any particular interest in being involved in oversight.

The processes for selecting members of specialised non-parliamentary oversight bodies vary significantly between states. As Table 1 shows, a significant majority of the non-parliamentary oversight bodies featured in this study are appointed by parliament. Appointments are normally made by the plenary of parliament but may also be the prerogative of a particular committee. For example, in Germany, the *Bundestag's* Parliamentary Control Panel elects members of the G10 Commission, which is a non-parliamentary body that oversees, among other things, information collection and the use of personal data by the German intelligence agencies.

The appointment of overseers by parliament has the advantage that it helps to maintain a link between members of the public and overseers, as directly elected representatives elect overseers. On the other hand, the main drawback of parliamentary involvement is that it politicises the selection process. Prospective members—who are not meant to represent any political interests—may see the need to pander to particular political parties in order to be (re)elected. This clearly undermines the purpose of having a non-parliamentary body to provide apolitical oversight.

[309] See, in Annex A of this volume: De With and Kathmann.
[310] See, in Annex A of this volume: Sanchez.
[311] See, in Annex A of this volume: Martin; Földvary.
[312] Italy, Law 14/2007, Article 29(3)(c).
[313] Australia, Intelligence Services Act 2001, Schedule 1 (part 3).

Alternatively, the executive may appoint non-parliamentary overseers. By way of example, the incumbent government appoints the Canadian Security Intelligence Review Committee (SIRC), the Swedish Committee on Security and Integrity Protection (SAKINT) and the Australian Inspector General for Intelligence and Security (IGIS).[314] While in these cases we are not aware of any evidence to suggest that the executive has used its power of appointment to select people who will not scrutinise particular matters and/or criticise the intelligence agencies, this could undoubtedly occur in some contexts.

An interesting alternative to the appointment of non-parliamentary overseers by either parliament or the executive is to include several branches of government in the appointment process. For example, the judiciary, parliament and executive are all involved in the process for appointing members of the Dutch Review Committee on Intelligence and Security Services. In this case, a panel, which includes the ombudsman and senior judicial figures, recommends possible candidates to parliament, which may or may not take these suggestions into account. Parliament must then present the responsible minister with a list of three candidates from which to choose.[315] This approach has the advantage that it increases the likelihood that members will be selected on the basis of their competences and includes a number of checks against the appointment of persons who not properly qualified or are otherwise inappropriate candidates.

4.3.5. Resources

It is axiomatic that both parliamentary and non-parliamentary oversight bodies need adequate financial and human resources in order to be effective.[316] The precise requirements will, of course, depend on the size of the intelligence agencies they oversee, as well as the type of mandate they have (see section 4.4. for a discussion of oversight bodies' mandates). For example, an oversight body that is mandated to handle complaints and/or conduct in-depth scrutiny of the legality of an agency's activities is likely to require far greater resources than a body whose mandate is to oversee an agency's policies.

Staffers are particularly essential to the functioning of an oversight body because it is generally them who carry out most of the detailed scrutiny of an agency's work (see Table 1 for the number of staffers selected specialised oversight bodies have). Members of oversight bodies are often not full-time; this is particularly true of parliamentary oversight bodies whose members have numerous other commitments. It is therefore essential that an oversight body has its own full-time members of staff.[317] In addition, it is helpful if members can engage their own staff to support them with their oversight work. The German *Bundestag's* Parliamentary Control Panel has a useful mechanism in this regard; members can employ their own staff for committee work, as long as such persons receive

[314] Canada, CSIS Act, Section 34(1); see, in Annex A of this volume: Cameron; Australia, Inspector-General of Security Act 1986, Section 8.
[315] The Netherlands, Intelligence and Security Services Act 2002, Article 65(2); see also, in Annex A of this volume: Verhoeven.
[316] Venice Commission Report 2007, p. 36; United Nations Human Rights Council 17 May 2010, Practice 7.
[317] See, in Annex A of this volume: Verhoeven.

security clearance and the approval of the committee.[318] In addition to permanent staff, it is good practice for oversight bodies to be able to engage the services of an external expert on an ad hoc basis, on for instance, highly technical matters.[319]

4.4. Mandate and functions of specialised oversight bodies

This section will begin by looking at the general mandates of oversight bodies, focussing on the subject of oversight, the criteria used to undertake oversight, and the temporal dimension of oversight. This will be followed by a discussion of two functions of parliamentary oversight bodies, and indeed, parliaments more generally, which may be of particular interest to the EP: the oversight of the appointment of agency directors and the oversight of non-parliamentary oversight bodies. Finally, we will examine the oversight of four aspects of national intelligence agencies' work which are similar to some of the functions of the EU's AFSJ bodies: information sharing, the collection of open source of information, joint analysis or fusion, and the use of personal data by intelligence agencies. Table 2, at the end of this section, provides an overview of some of the activities of intelligence agencies that are overseen by specialised oversight bodies in EU Member States

4.4.1. General mandate

The mandates of both parliamentary and non-parliamentary oversight bodies are generally outlined in legislation. Provisions on oversight are commonly included in the same legislation that regulates the intelligence agency(ies)—but in some states there is specific legislation for oversight bodies, e.g., for the German *Bundestag's* Parliamentary Control Panel, Norway's *EOS Utvalget Committee*, and Sweden's *SAKINT*. Mandates for the oversight of intelligence agencies can be broken down into three components:

1) The subject of oversight, the areas of an intelligence agency's work that are overseen;
2) The criteria for oversight, that is, the terms of reference or assessment used for overseeing particular areas of an agency's work; and
3) The temporal focus of oversight; that is, whether oversight focuses on *ex post* review of an agency's activities or also includes an *ex ante* role and/or ongoing monitoring of an agency's activities.

In many instances these three dimensions of oversight are not explicitly defined in law. Where legal mandates do provide more detail, oversight bodies' mandates are usually defined according to one of the first two components, i.e., overseers are either mandated to focus on particular aspects of an agency's work or scrutinise an agency's fulfilment of particular criteria.

[318] Germany, Parliamentary Control Panel Act (PKGrG), Section 11 (Federal Law Gazette I, p. 2346) [hereafter, Germany, Parliamentary Control Panel Act].
[319] See, for example, Belgium's Committee I, cited in Van Laethem, (in Annex A of this volume); Hungary, Act No. CXXV of 1995, Section 14(5); see, in Annex A of this volume: Földvary.

4.4.1.1. Subject of oversight

Table 1 illustrates that, in practice, specialised oversight bodies in EU Member States oversee a broad spectrum of the activities of intelligence agencies. The majority of the oversight bodies listed in Table 1 oversee the policies, administration and finance of intelligence agencies. A slightly lower number of oversight bodies stated that they oversee completed operations and fewer still monitor ongoing operations. In this context, the term 'operations' primarily refers to intelligence collection measures using, inter alia, the interception of communications, covert surveillance and use of human sources, as well as the sharing of information with domestic and foreign entities. There are two main explanations for the fact that some oversight bodies, primarily of the parliamentary variety, do not oversee intelligence agencies' operations. Firstly, executives and their agencies are highly sensitive about these activities and are very reluctant to open them to the scrutiny of parliamentarians (see sections 4.5.3. and 4.7 for further discussion).[320] Secondly, in many states the oversight of operations is the prerogative of a (quasi-)judicial body and therefore it may be seen as unnecessary for parliaments to delve into these matters.[321]

While this sub-division of the subject of oversight may be analytically useful, the statutory mandates of oversight bodies rarely make reference to these categories. In fact, they are often conspicuous for their lack of specificity. By way of example, the *Bundestag's* Parliamentary Control Panel's mandate is codified in the following way:

> With respect to the activities of the Federal Office for the Protection of the Constitution, the Military Counter-Intelligence Service and the Federal Intelligence Service, the Federal Government shall be subject to the supervision of the Parliamentary Control Panel.[322]

The mandate of the French parliament's *Delegation parlementaire au renseignement* is similarly general:

> *la delegation parlementaire au renseignement a pour mission de suivre l'activité générale et les moyens des services spécialisés à cet effet placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget.*[323]

There are notable exceptions to this approach, such as the UK's Intelligence and Security Committee, which has an explicit mandate 'to examine the expenditure, administration and policy of' the UK's intelligence services, and Australia's Parliamentary Joint Standing Committee on Intelligence and Security, which has a mandate to examine the 'administration and expenditure' of the Australian intelligence agencies.[324] While the mandates of many oversight bodies do not

[320] See, for example, the Venice Commission Report 2007, p. 34.
[321] Venice Commission Report 2007, paras. 195–217.
[322] Germany, Parliamentary Control Panel Act, Section 1.
[323] France, Loi n°2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement, Article 3.
[324] UK, Intelligence Services Act 1994, Section 10(1); Australia, Intelligence Services Act 2001, Section 29.

specify which aspects of agencies' activities should be overseen, they sometimes contain explicit prohibitions on overseeing particular aspects of an agency's work. For example, the French *Délégation parlementaire au renseignement* and the Parliamentary Joint Standing Committee on Intelligence and Security are explicitly barred from examining any operational matters.[325]

It is difficult to advocate a 'best' approach or practice in regards to the subject(s) of an oversight body's mandate. Ultimately, what matters is that all of the abovementioned dimensions of an intelligence agency's work are overseen by a body which is independent from the agencies and the executive.[326] Such bodies could include a combination of the institutions discussed in this chapter, as well as judicial bodies. Nevertheless, a clear delineation of the areas of an intelligence agency's work that should be overseen helps provide overseers with a clear focus for their work and should assist them in allocating time and resources for scrutinising particular matters. On the other hand, a lack of clarity in terms of the 'subject' of oversight may have some advantages. Notably, it may give an oversight body a greater margin of discretion in deciding which aspects of a intelligence agency to examine. A mandate which is too precise might be narrowly interpreted by the executive and/or agencies as grounds for resisting oversight of particular matters. In addition, it may be difficult to disentangle subjects such as operations and policy given that they are intrinsically linked: operations take place on the basis of policy and yet, operations also inform policy.

4.4.1.2. Criteria for oversight

Oversight is normally conducted according to terms of reference that indicate the criteria according to which an intelligence agency's work should be scrutinised. Such criteria should be an integral part of an oversight body's mandate because they indicate how an agency's work is assessed. Criteria for oversight can be divided into three main areas: compliance with the law, effectiveness, and efficiency.[327] The majority of EU national parliaments that responded to the DCAF-EUI questionnaire indicated that a specialised parliamentary and/or non-parliamentary committee oversees intelligence agencies in accordance with all of these criteria. However, in common with the foregoing discussion on the oversight of particular aspects of intelligence agencies' work, national law does not always provide any specific guidance to oversight bodies on which criteria they should assess.[328] We shall briefly describe each of the three criteria.

A mandate to assess *compliance with the law* typically involves scrutinising an agency's activity to assess whether or not they have complied with applicable constitutional, statutory, subsidiary and, sometimes, international law.[329] This focus is sometimes defined more broadly as 'propriety', which goes beyond the law to include the ethicality of particular activities. A number of the oversight bodies examined in this study have mandates which focus exclusively on

[325] For example, in France, see Lepri, (in Annex A of this volume); Australia, Intelligence Services Act 2001, Section 29(3).
[326] United Nations Human Rights Council 17 May 2010, 8–9.
[327] See, for example, Whitaker and Farson 2009, p. 3; Caparini 2007, p. 9; Krieger 2009, 216–217.
[328] E.g., the UK's ISC (in Annex A of this volume, see Leigh); German *Bundestag's* Parliamentary Control Panel, and the French parliament's DPR; on Canada see Whitaker and Farson 2009, 3.
[329] Notably, 17 of the parliaments which responded to this questionnaire indicated that a specialised parliamentary and/or non-parliamentary oversight body assesses security/intelligence agencies in compliance with international law.

evaluating intelligence agencies' compliance with the law, e.g., the Dutch CTIVD, the Swedish Commission on Security and Integrity Protection, and the Council for the Oversight of the Intelligence System of the Portuguese Republic.[330] It is notable that these bodies are exclusively non-parliamentary specialised oversight bodies. Parliamentary bodies are normally required to examine a broader range of criteria (see below).

Overseers whose mandate includes scrutinising an intelligence agency's compliance with the law, such as the Dutch CTIVD and Belgian Committee I, are generally empowered to make this assessment with respect to a broad range of 'subjects of oversight' outlined above (sub-section 4.4.1.1), e.g., operations, policies and administration.[331] In other cases, oversight bodies are mandated to oversee the legality of a very specific aspect of an agency's work. For example, the UK Intelligence and Interception of Communications Commissioners are mandated to examine whether the process for authorising the use of certain special powers to collect intelligence comply with the law.[332] It is the opinion of the authors of this study that a mandate to oversee an agency's compliance with the law should include the examination of operations because it is in this area that agencies leave the largest legal footprint: they perform functions which restrict and may violate human rights.

A mandate to oversee the *effectiveness* or efficacy of agencies' work entails an assessment of if and how agencies' fulfil their statutory tasks, as well as the extent to which they meet the expectations of their customers, i.e., the executive and other government agencies.[333] This assessment is critically important for ensuring that agencies contribute effectively to the security of the state and its population. Several specialised oversight bodies examined in this research have an explicit legal mandate to assess both the lawfulness and the effectiveness of the agencies.[334]

Finally, the oversight of the *efficiency* of the work of intelligence agencies implies an assessment of the relationship between the financial resources expended on particular initiatives and their outcomes. A focus on efficiency is usually linked to a mandate to oversee the finances of these agencies.

4.4.1.3. The temporal dimension of oversight

The mandates of oversight bodies also vary according to the point in time at which they scrutinise given activities of intelligence agencies. In theory, an overseer could scrutinise a particular action or policy at any point in time—from the planning discussions, to the implementation phase, as well as after it has been completed. The mandates of oversight bodies rarely specify the point in

[330] See, in Annex A of this volume: McGarrity, and Cameron; Sweden, Act on Supervision of Certain Crime Fighting Activities, Section 1; Questionnaire Response from the Council for the Oversight of the Intelligence System of the Portuguese Republic, Question 23(a).
[331] E.g.: The Netherlands, Intelligence and Security Services Act 2002, Article 64(2)(a); Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 1.
[332] UK, Regulation of Investigatory Powers Act 2000, Sections 57 and 59.
[333] See, e.g., Caparini 2007, 9.
[334] E.g.: Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 1; Croatia, Act on the Security Intelligence System, Article 107.

time at which oversight should take place. In practice, most oversight bodies take an *ex post* approach to scrutinising intelligence agencies.[335] That is, they look at documents which have been finalised, decisions that have been made and actions which have taken place. An *ex post* approach may be applied to issues ranging from specific intelligence collection operations, to internal regulations and policy, information sharing agreements, and sharing of information with other domestic or foreign entities. It should be noted that the fact that overseers take an *ex post* approach to scrutinising particular activities does not necessarily imply that oversight is reactive, i.e., on the basis of a response to a particular complaint or scandals raised in the media. Overseers can take an *ex post* approach but still scrutinise particular issues or activities proactively, without being prompted by media reports etc.

There are three main areas in which oversight bodies sometimes play a role in examining policies or actions before they are implemented and/or while they are ongoing. First, and perhaps most commonly, parliamentary oversight bodies often have a role in scrutinising and (through the plenary of parliament) approving proposed expenditure by intelligence agencies.[336] Within this context, parliaments may examine (*ex ante*) proposed programmes, priorities for the forthcoming period and, in some cases, specific operations.

Second, some specialised oversight bodies (usually non-parliamentary bodies of a quasi-judicial nature) have a specific mandate to control intelligence agencies' use of special powers to collect information. For example, Germany's G10 Commission plays a role in authorising the interception of communications, monitors the implementation of such measures and may order their termination.[337]

Third, certain oversight bodies play an *ex ante* role by virtue of their being briefed (by the executive) on particular operations before they take place. The US Congress is the main example of this practice. The executive is required to brief *ex ante* select groups of congressmen (the so-called Gang of Four and Gang of Eight) on specific types of operation.[338] The Gang of Four is an informal customary mechanism made up of the chairman and ranking members (most senior member of the opposition party) on the House and Senate intelligence committees. This group often receives briefings on 'sensitive non-covert action intelligence programs', such as highly sensitive intelligence collection programmes. The Gang of Eight—which, in contrast to the Gang of Four, does have a statutory basis—is made up of the same four individuals plus the speaker and opposition leader in each house.[339] The law requires the executive to report to this group on forthcoming 'covert actions', which are defined in US law as 'an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the

[335] Venice Commission Report 2007, p. 34.
[336] See, for example, the German *Bundestag's* Confidential Committee of the Budget Committee, discussed in Annex A of this volume in De With and Kathmann; the Hungarian Parliament's National Security Committee (Hungary, Act No. CXXV of 1995, Section 14 (4)(g)).
[337] Germany, Article 10 Act (G10 Act); see also the role played by the *Bundestag's* Control Panel, with regards to the approval of strategic interception measures (in Annex A of this volume in De With and Kathmann).
[338] Cumming March 2011; see also Cumming 6 April 2011.
[339] United States Code, Title 50, Section 413b; Cumming March 2011.

United States Government will not be apparent or acknowledged publicly'.[340] These processes are aimed at keeping Congress informed and allowing members to raise concerns but this *ex ante* involvement does not imply that Congress has either approval power with regards to such operations or that it can veto them.[341] For the purposes of the EP, it is important to note that we are not aware of examples, in the US or elsewhere, where *ex ante* briefings on operations extend to cooperation or information sharing agreements between intelligence agencies and foreign entities.

Finally, oversight bodies may be briefed on work plans and priorities and have the opportunity to raise concerns (this issue is discussed in more detail in section 4.5.4. on proactive disclosures). This does not, however, imply a veto on such plans or a role in decision making about an agency's programmes and policies.

From this assessment it is evident that there is a clear difference between overseers receiving information about particular programmes or actions before they are implemented, and overseers playing a role in decision making relating to particular activities. While it is standard practice for parliaments to appropriate funds to intelligence agencies (thus, exerting control over an agency), concerns arise when a specialised oversight body exerts control over decisions to undertake particular actions. Such involvement may compromise the capacity of an oversight body to subsequently review an agency's activities. This is because the oversight body has played a direct role in the decision making relating to the given activity—it would have to effectively review its own work. For this reason, many states ensure that any independent body involved in making *ex ante* decisions about particular actions is not the same body as the one which later reviews such actions.

4.4.2. Specific oversight functions

Within the framework of their general mandates, oversight bodies perform a broad range of specific functions. These functions include: the aforementioned role in authorising the use of special powers to collect information, e.g., surveillance, or the use of assumed identities;[342] supervising the use of such powers; handling complaints from members of the public about intelligence agencies;[343] handling disclosures made by whistleblowers from within these agencies; and serving as appeals bodies for denials of security clearance.[344] The country case studies in Annex A provide additional detail on these functions. They will not, however, be discussed here because they are of limited salience for the EP given that, among other things, the AFSJ bodies do not posses special powers

[340] US, National Security Act of 1947, Sec. 503(e), 50 U.S.C. 413b(e).
[341] Cumming 6 April 2011, pp. 5–6.
[342] E.g., Germany's G10 Commission (see De With and Kathmann in Annex A of this volume) and the Swedish SAKINT's Secret Identities Delegation (see Cameron in Annex A of this volume).
[343] See, for example, the Hungarian parliament's National Security Committee (Hungary, Act No. CXXV of 1995, Section 14(4)(c)); see, in Annex A of this volume, Földvary; Sweden's SAKINT (Sweden, Act on Supervision of Certain Crime Fighting Activities, Section 3); Dutch CTIVD (The Netherlands, Intelligence and Security Services Act 2002, Article 64(c)); Belgian Committee I (Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 34); Australian Inspector General for Intelligence and Security (see McGarity in Annex A of this volume).
[344] E.g., the Belgian Committee I (see Van Laethem in Annex A of this volume), the Security Intelligence Review Committee (Canada, CSIS Act, Section 42), and the Hungarian parliament's National Security Committee (see Foldvary in Annex A of this volume).

to collect information and the EU does not administer security clearances. Instead, this sub-section will highlight two functions of oversight bodies (and parliaments more generally) which are likely to be of particular interest to the EP: the oversight of the appointment of agency directors, and what may be termed 'overseeing the overseers'—parliamentary oversight of specialised non-parliamentary oversight bodies.

4.4.2.1. Oversight of the appointment of agency directors

Parliamentary oversight bodies sometimes play a role in the appointment of the directors of intelligence agencies. They are involved in one of three ways. First, the government may simply be required to inform oversight committees of their intention to appoint a particular person as director of an agency.[345] Second, and most commonly, oversight committees are able to hold a hearing with a nominee and can issue a non-binding opinion or recommendation on the proposed appointment. By way of example, the Estonian *Riigikogu's* (parliament) Security Authorities Surveillance Committee is entitled to give an opinion on proposed appointments, and the Hungarian Parliament's National Security Committee must hold hearings and issue opinions on nominees' suitability for the position.[346] Alternatively, this role may be performed by several committees of parliament, e.g., in Portugal, where nominees are heard before the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees; the Foreign Affairs Committee; and the National Defence Committee.[347] Finally, a parliamentary oversight committee (or the plenary of parliament, acting upon their recommendation) may be required to approve the appointment of agency directors, thereby giving them a de facto veto on nominees. For example, the Romanian parliament's 'Joint Standing Committee for the exercise of parliamentary control over the activity of the Romanian Intelligence Service' conducts hearings and reports on the president's nomination for the director of the service; on this basis, the plenary of parliament votes on whether to approve the nomination.[348] The US Senate performs a similar role; the intelligence committee holds a hearing which is followed by a vote in the plenary.[349]

Giving oversight committees a role in scrutinising the appointment of the directors intelligence agencies has three main advantages. Firstly, it provides a safeguard against the appointment of persons likely to promote the political interests of the incumbent government. Requiring a committee to hear and issue an opinion on nominees may help to ensure that persons ultimately appointed enjoy broad support.[350] While the power to veto appointments can be an important power of last resort, in practice governments are unlikely to push through nominations which are strongly opposed by parliament. Secondly, hearings with prospective directors may be used to extract commitments from the nominee and/or the government on, inter alia, commitments to oversight, respect for human rights and the prioritisation of particular security issues.[351] An

[345] For example, the Italian parliament's COPASIR – response to question 2 of the DCAF-EUI questionnaire from the parliament of Italy.
[346] Response to question 2 of the DCAF-EUI questionnaire from the parliament of Estonia; see also Földvary, in Annex A of this volume.
[347] Response to question 2 of the DCAF-EUI questionnaire from the parliament of Portugal.
[348] Responses to questions 2 and 24 of the DCAF-EUI questionnaire from the parliament of Romania.
[349] See, in Annex A of this volume: Martin.
[350] See Földvary's comments on Hungary in Annex A of this volume.
[351] See, for example, in Annex A of this volume: Martin.

oversight committee can subsequently monitor a director's adherence to such commitments. Finally, a hearing with, and even approval by, parliament may serve to give the director legitimacy which may help to increase public confidence in an agency.

In spite of these advantages, the majority of EU Member States have opted not to involve parliament in the appointment of agency directors.[352] Several arguments can be made for this. At a most basic level, it may be submitted that the executive is politically responsible for intelligence agencies and should therefore retain control of the decision on who should run such agencies. In addition, parliamentary involvement may serve to transform the selection of a director, who should be appointed on the basis of expertise, into a partisan matter. Indeed, if incumbent directors need to secure the support of a parliamentary majority to be re-appointed, this is a risk that they may take decisions in order to garner the support of particular parties—the politicisation of intelligence agencies is clearly something that should be avoided. These concerns are less likely to arise if parliament's role in the selection of directors is limited to a specialised committee holding a hearing and issuing a non-binding opinion.

4.4.2.2. 'Overseeing' the overseers

The relationship between parliament and any specialised non-parliamentary oversight body is fundamental to the success of a system of oversight. Beyond their role in legislating to establish such bodies, parliaments engage with them in four main ways.

First, parliaments often play a role in selecting the members and sometimes senior staffers of non-parliamentary oversight bodies (see section 4.3.4 for further information).[353] A parliament can use its role in the appointment process to ensure that people with appropriate expertise are appointed and that incumbent members who fail to perform their functions are not reappointed.[354]

Second, parliaments are responsible for appropriating funds for non-parliamentary oversight bodies. The amount of influence parliament can bring to bear on the resources available to an oversight body depends on whether the body has its own budget or is subsumed under the budget of the executive branch or even the agency which it oversees. If a non-parliamentary oversight body has an autonomous budget, or at the very least a separate budget line, it is easier for parliament to play a direct role in ensuring that overseers have sufficient resources. The responsible parliamentary committee(s) can use hearings with non-parliamentary oversight bodies to determine whether it needs additional resources.

Third, in a number of parliaments that responded to the questionnaire, parliament can request a non-parliamentary oversight body to examine a particular issue.[355]

[352] Responses to question 2 of the DCAF-EUI questionnaire.
[353] Responses to question 3 of the DCAF-EUI questionnaire indicate that in 11 EU member states, parliament plays a role in the appointment of members of non-parliamentary oversight bodies.
[354] E.g., Belgian Committee I and the Norwegian EOS-Utvalget Committee.
[355] Responses to question 3 of the DCAF-EUI questionnaire from Belgium, Estonia, Finland, Germany, Greece, the Netherlands, Poland, Portugal, Sweden, the UK and Romania.

This enables parliament to make use of the bodies to investigate matters which it may not have the time or specialised expertise to address.

Finally, non-parliamentary oversight bodies are usually required to report to parliament either directly or through the executive.[356] This typically includes both periodic reports and reports on thematic issues. Such reporting is usually done to a particular committee of parliament, which is responsible for scrutinising the reports and taking the necessary action within parliament.[357] For example, legislative amendments may be put forward on the basis of the findings of a non-parliamentary oversight body, or parliament may decide to stop funding a particular area of an intelligence agency's work. Parliamentary committees often hold hearings as a follow up to reports from non-parliamentary overseers.[358] These meetings can serve to inform MPs about particular problems concerning intelligence agencies, and may help to inform parliamentary debate on matters of concern.[359] MPs can also use this dialogue to ensure that such bodies are fulfilling their mandates effectively and have sufficient powers and resources in order to do so.

4.4.3. Oversight of selected activities of intelligence agencies

In order to ensure that the analysis of national oversight bodies' mandates and functions is of relevance to the EP, we identified four broad categories of activity that are performed by the AFSJ bodies, and subsequently examined how specialised oversight bodies scrutinise intelligence agencies' performance of comparable activities on the national level. These activities are: information sharing; the collection of open source information; joint analysis and fusion; and the use of personal data.

4.4.3.1. Information sharing

Sharing information with domestic and foreign bodies is a key dimension of intelligence agencies' work. On a national level, agencies share information with, inter alia, the police, customs and border agencies, prosecutors and other similar agencies. The sharing of information, particularly personal data, can give rise to human rights concerns because recipients may take action resulting in the limitation of human rights on the basis of information provided by an intelligence agency.[360] In view of this, overseers scrutinise both the agreements upon which information is shared and, where necessary, examine the content of information shared with other domestic bodies.[361] Specialised oversight bodies typically examine information sharing on a national level through, inter alia, random

[356] Questionnaire responses indicated that non-parliamentary oversight bodies report to parliament in at least 16 member states.
[357] See, for example, Verhoeven in Annex A of this volume on the Dutch CTIVD committee's reporting to parliament.
[358] E.g., the Senate Monitoring Commission in Belgium, which meets Committee I once per quarter (see Van Laethem, in Annex A of this volume) and the Dutch Second Chamber's Home Affairs Committee, which scrutinises public reports of the Review Committee on the Intelligence and Security Services, and the Special ISS Committee examines its classified reports (see Verhoeven, in Annex A of this volume).
[359] See in Annex A of this volume: Verhoeven.
[360] Ibid.
[361] See: United Nations Human Rights Council 17 May 2011, Practice 34; Canada, CSIS Act, Section 17.

checks on or sampling of an agency's files on the basis of complaints and in the context of in-depth investigations into particular files or programmes.[362] Overseers do not, however, play a role in the drafting or approval of information sharing agreements between intelligence agencies and other domestic entities.

Intelligence agencies' sharing of information with foreign entities has given rise to significant concern in recent years.[363] This is largely because established democracies have exchanged an ever increasing amount of information with states that do not respect the same standards on human rights, the rule of law and democratic accountability.[364] In view of this, information sharing with foreign entities clearly needs to be carefully regulated and overseen.[365] Yet, many national oversight bodies are ill equipped to perform this task. Most notably, many oversight bodies do not have a legal mandate to examine information sharing with foreign entities. They are often prohibited from accessing information about agreements and information transfers (see section 4.5.3.). The 'third party rule' is a major obstacle in this regard because overseers are often viewed as third parties and thus barred from viewing information provided by foreign entities.[366] Finally, overseers' jurisdiction is normally limited to their own state's territory, information and personnel.[367] When investigating a particular matter, they cannot usually secure the cooperation of foreign officials.[368]

Oversight bodies have, nevertheless, dedicated significant attention to cooperation with foreign partners and many have conducted thematic investigations in this regard.[369] A number of the specialised oversight bodies examined in this research can scrutinise information sharing with foreign entities on an ongoing basis. In this context, oversight takes four main forms. First, an overseer can review the agreements upon which information sharing and other forms of cooperation are based.[370] The Canadian system is a good example in this regard; the law requires that information sharing agreements between the Canadian Security Intelligence Service and foreign (or domestic) agencies must be copied to the Security Intelligence Review Committee (SIRC, a non-parliamentary body).[371] This practice gives the overseer the opportunity to raise concerns about, e.g., an agreement's safeguards on the use of shared information or data protection guarantees, as well as to evaluate an agency's sharing practices against the criteria established in an agreement. It is important

[362] Responses to the DCAF questionnaire from 18 EU states indicated that specialised oversight bodies play some role in this regard: e.g. Belgium, Bulgaria, Estonia, Finland, France, Germany, Hungary, Italy, the Netherlands, Poland, Portugal, Slovenia, Sweden, Romania and the UK.
[363] See, for example: United Nations Human Rights Council 17 May 2011, p. 16; International Commission of Jurists 2009, pp. 79–85.
[364] For a detailed discussion of the concerns regards information sharing with foreign entities, see: Wills and Born 2011, pp. 277–278 and 280–281; The Arar Inquiry, pp. 431–432.
[365] United Nations Human Rights Council 17 May 2011, pp. 31–34; The Arar Inquiry, p. 501.
[366] Wills and Born 2011, pp. 282–288.
[367] See, for example, in Annex A of this volume: Verhoeven.
[368] Wright 2011, pp. 177–179.
[369] According to Iain Cameron, Sweden's SAKINT is currently examining Swedish agencies' cooperation with foreign partners (see Cameron in Annex A of this volume); Nicola McGarrity states that Australia's Inspector General for Intelligence and Security is conducting similar work (see McGarrity in Annex A of this volume). See also: Netherlands Review Committee for the Intelligence and Security Services 2009.
[370] Questionnaire responses (question 24) from EU national parliaments indicate that the following specialised oversight bodies review cooperation/sharing agreements with foreign entities: Belgium (Committee I), Germany (PKGr/G10), Latvia (National Security Committee) Netherlands (CTIVD), Poland (Special Services Oversight Committee of the *Sejm*), Sweden (SAKINT), Romania (Parliamentary Oversight Committee) and the UK (ISC).
[371] Canada, CSIS Act, Section 17(2); see in Annex A of this volume: Forcese.

to note, however, that neither specialised oversight bodies nor parliaments play a role in the negotiation or adoption of these agreements. In fact, we are not aware of any example where specialised (non)parliamentary oversight bodies review, let alone approve, agency to agency agreements before they are signed—this is seen as the exclusive prerogative of the executive and its agencies.

Second, an oversight body may be able to review the human rights record or data protection standards of the state or agency in question. For example, the SIRC has also reviewed the human rights records of partner countries and flagged information sharing/cooperation relationships which require a high degree of vigilance.[372]

Third, in some states the executive and/or intelligence agencies have an obligation to inform an oversight body about information exchanged with foreign entities. In Germany, for example, the Federal Intelligence Service is required to inform (on a periodic basis) both the Parliamentary Control Panel and the G10 Commission about the transfer of certain forms of information to foreign entities.[373]

Finally, some oversight bodies review outgoing and/or incoming information from foreign entities, insofar as this is relevant to their mandate.[374] By examining this information, overseers can try to ensure that key safeguards are observed, i.e., information sharing complies with applicable agreements and national law.[375] Some overseers have stated that they focus on examining outgoing information,[376] while others have explicitly stated they examine incoming information from foreign entities.[377] Scrutiny of such information does not normally entail examining every piece of information exchanged. More commonly, overseers examine information shared with or by foreign entities in the context of an investigation into a particular case or relationship. What matters is that overseers have the authority to examine such information if they deem it to be necessary (see section 4.5).

4.4.3.2. Collection of open source information

Most national intelligence agencies are authorised to use special powers to collect information, e.g., covert surveillance, the interception of communications and surreptitious removal of objects. However, they collect a far greater proportion of their information through so-called 'open sources'. That is, information which is public and freely available, such as media articles, online blogs and academic studies. Information collected from open sources may include 'strategic' information on particular themes but it may also include personal data which are available in the public domain. It is primarily for this reason that the collection of open source information can have important implications for individuals. Information gleaned from open sources may serve as the basis for opening files

[372] Whitaker and Farson 2009, p. 24.
[373] Germany, G10 Act, Section 7a(5–6); see in Annex A of this volume: De With and Kathmann.
[374] Questionnaire responses (to question 24) from the following states indicated there is some oversight (by specialised oversight bodies) of information sharing with foreign entities: Belgium, Bulgaria, Finland, Germany, Latvia, the Netherlands, Poland, Sweden, Romania and the UK.
[375] See in Annex A of this volume: Cameron; Netherlands Review Committee for the Intelligence and Security Services 2009.
[376] For example, in Annex A of this volume: Verhoeven.
[377] For example, the Belgian Committee I (cited in Annex A of this volume in Van Laethem).

or investigations on individuals, leading to the use of the aforementioned 'special powers', which directly restrict human rights.[378]

Twelve of the national parliaments that responded to the DCAF-EUI questionnaire indicated that, in their state, a specialised oversight body does examine the collection of open source information by intelligence agencies.[379] Such scrutiny normally takes place indirectly; for example, when overseers examine the use of special powers, e.g., the interception of communications, which may have been initiated on the basis of information collected through open sources. Another example is when overseers examine requests regarding access to personal data held in agencies' files, they may review information that was collected through open sources.[380] Finally, some oversight bodies, e.g., Denmark's *Wamberg Committee,* have a role in overseeing the creation of files by intelligence agencies.[381] In this context, they may examine whether or not a file can be created on the basis of information gathered through open sources. However, oversight bodies' scrutiny of information collected through open sources remains indirect and it is clear from the national case studies (see Annex A) that oversight bodies do not dedicate much attention to this issue.

4.4.3.3. Joint analysis and fusion centres

In the past decade, many states have created what are known as 'fusion' or 'joint analysis' centres. These are hubs that draw together information from a number of domestic security, intelligence, law enforcement agencies and other relevant executive bodies with the aim of producing comprehensive analyses of particular threats.[382] Fusion centres usually contain representatives from each of the bodies that contribute information; these individuals work together to produce analysis to support policymaking and their own agencies' work. It is important to note that fusion centres rely upon inputs from other agencies; they do not undertake their own intelligence collection using special powers. From this description it is evident that, in terms of their functions, fusion centres are the national entities which are the most similar to the EU's AFSJ bodies.

Relatively few oversight bodies scrutinise the activities of fusion centres. In fact, only seven EU Member States indicated that their specialised oversight bodies play a role in this regard.[383] Belgium's Standing Intelligence Review Committee (Committee I) is perhaps the best example of an oversight body which scrutinises the work of a fusion centre. In fact, the applicable oversight law was amended to

[378] See in Annex A of this volume: Cameron.
[379] Responses to question 24 of the DCAF-EUI questionnaire.
[380] Response to question 24 of the DCAF-EUI questionnaire from the Swedish SAKINT.
[381] Danish Security and Intelligence Service 2007, Appendix C.
[382] For a comprehensive review of fusion centres in the EU, please see: Belgian Standing Committee I 2010. Examples of fusion centres include Belgium's Coordination Unit for Threat Assessment (CUTA), Canada's Integrated Threat Analysis Centre (ITAC) and the UK's Joint Terrorism Analysis Centre (JTAC).
[383] Responses to question 21 of the DCAF-EUI questionnaire from Belgium, Germany, Lithuania, the Netherlands, Poland (*Sejm*), Portugal and the UK. It is also noteworthy that the Dutch CTIVD has examined the so-called 'Counter-Terrorism Information Box' and Canada's Security Intelligence Review Committee has reviewed the Integrated Threat Assessment Centre (see Verhoeven and Forcese in Annex A of this volume).

require Committee I to examine both the effectiveness and its compliance with the law by the Coordination Unit for Threat Assessment.[384]

There are two possible explanations for the lack of oversight of fusion centres. First and foremost, oversight bodies scrutinise the activities that lie behind the inputs to fusion centres: that is, they oversee the information collection by agencies and, in some cases, information received from foreign entities. Accordingly, there is already a check on the activities that are deemed to entail the greatest restrictions on human rights. It may not be seen as a priority to carry out oversight of analysis and reporting processes. Indeed, Iain Cameron explains that there is no direct oversight of Sweden's Counter Terrorism Cooperation because it is seen as performing advisory rather than operational functions.[385] A second explanation is that fusion centres are often subsumed within intelligence agencies and thus may be overseen within the context of the oversight of these agencies.[386]

4.4.3.4. Use of personal data

Given that information is the lifeblood of intelligence agencies, it is inevitable that use of personal data is one of the main areas in which they restrict and, without proper controls, may violate human rights. The oversight of the use of personal data is therefore essential for ensuring that agencies comply with applicable law on, inter alia, privacy, data protection and non-discrimination.[387] Broadly speaking, overseers assess whether agencies have complied with applicable law on the use of personal data in one or more of the following areas of activity: (1) the collection of information using special powers; (2) the retention and deletion of personal data in agencies' files; (3) the handling of requests to access personal data held by agencies; and (4) the transfer of personal data to domestic and foreign partners (discussed above).[388] We will highlight just some of the situations in which oversight bodies scrutinise the use of personal data across these areas in order to ensure that intelligence agencies comply with the law.

Firstly, overseers may check agencies' files on a given person upon receipt of a query or complaint, including requests from members of the public to access their own personal data.[389] Secondly, oversight bodies may scrutinise personal data held in an agency's files, as well as the basis upon which it was included in the files, in the context of a thematic investigation of a particular issue. For example, oversight bodies may review an agency's work relating to a particular terrorist group, the sharing of information with foreign partners, or transfers of personal data to immigration authorities.[390] Thirdly, overseers may conduct checks on samples of certain processes involving the use of personal data, such as the insertion of data into a particular category of work file or the sharing of

[384] Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 1(2).
[385] See in Annex A of this volume: Cameron.
[386] See Belgian Standing Committee I 2010.
[387] United Nations Human Rights Council 17 May 2010, Practice 25.
[388] For a comprehensive overview of these practices and their implications for human rights see, Cameron 2000.
[389] See, for example: Sweden, Act on Supervision of Certain Crime Fighting Activities, Section 3 and Cameron in Annex A of this volume; the Dutch CTIVD (discussed in Annex A of this volume in Verhoeven.
[390] E.g., The Netherlands Review Committee on the Intelligence and Security Services 2006.

information with other agencies. Fourthly, an oversight body, such as Denmark's 'Wamberg Committee', may be required to scrutinise and approve the proposed establishment of a file on a given person.[391] Finally, some oversight bodies review all information collected from the use of special powers and may order its deletion if, for example, its retention is not absolutely necessary or the process through which it was collected did not comply with the law.[392]

Oversight of the use of personal data by intelligence agencies is generally considered to be highly skilled, time-consuming work.[393] In view of this, oversight normally is carried out by non-parliamentary oversight bodies. Indeed, the oversight of the use of personal data is a key part of the mandate of many non-parliamentary oversight bodies which deal exclusively with intelligence agencies.[394] Some non-parliamentary oversight bodies focus exclusively on the use of personal data by intelligence agencies.[395] While non-parliamentary oversight bodies generally play a role in this regard, they sometimes share jurisdiction with a data protection supervisor/commission, e.g., in Germany.[396] By contrast, in some states, e.g., Portugal, the oversight of the use of personal data by intelligence agencies is the exclusive prerogative of a data protection supervisor/commission, which has jurisdiction far beyond intelligence agencies.[397] While it is difficult to advocate any best practice in terms of the precise division of labour for the oversight of intelligence agencies' use of personal data, it is important that there is at least one institution that has the requisite powers, expertise and access to information to do so. Oversight bodies that focus exclusively on intelligence agencies are often well placed in this regard and, unlike data protection bodies with a general mandate, they can draw links between their oversight of the use of personal data with their scrutiny of other aspects of agencies' work.

[391] Response to question 24 of the DCAF-EUI questionnaire from the parliament of Denmark; see also, Danish Security and Intelligence Service 2007, pp. 16–17.
[392] Germany's G10 Commission is a good example in this regard (see De With and Kathmann in Annex A of this volume).
[393] See, for example, comments by Verhoeven (in Annex A of this volume).
[394] See, for example, Sweden's SAKINT; the Belgian Committee I, the German G10 Commission and the Dutch CTIVD.
[395] See, for example, Denmark's Wamberg Committee.
[396] See in Annex A of this volume: De With and Kathman.
[397] Response to question 24 of the DCAF-EUI questionnaire from the parliament of Portugal.

Table 2: Activities and processes of intelligence agencies that are overseen by specialised committees

STATE	Collection of information using special powers	Collection of information from open sources	Use of personal data	Sharing of information between agencies on a domestic level	Sharing of information with foreign entities	Information sharing and cooperation agreements signed with foreign governments and agencies	Analysis of information and production of reports	Appointments of senior staff	Appointments of oversight bodies within agencies
Austria - *Standing Subcommittee of the Interior Affairs Committee*	No distinction is made/Relevant information may be provided								
Belgium - *Standing Intelligence Agencies Review Committee*	O	O	O	O	O	O	O	O	
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	O	O	O	O	O	O	O		
Cyprus									
Czech Republic - *Permanent Commission on Oversight over the work of the Security Information Service (BIS)*							O		
Denmark - *The Folketing's Committee on the Danish Intelligence Services*			O				O		
Estonia - *Security Authorities Surveillance Select Committee*		O		O			O	O	O
Finland - *The Administration Committee*	O	O	O	O	O	O	O	O	O
France - *Commission des Lois*			O	O					
Germany - *Parliamentary Control Panel (PKGr)*	O	O	O	O	O	O	O		
Germany - *G10 Commission*	O	O	O	O	O	O	O		
Greece - *Special Standing Committee for Institutions and Transparency*	No distinction is made/Relevant information may be provided								
Greece – *Authority for Communication Security and Privacy (ADAE)*	O		O						
Hungary - *Committee on National Security*	O			O				O	

STATE	Collection of information using special powers	Collection of information from open sources	Use of personal data	Sharing of information between agencies on a domestic level	Sharing of information with foreign entities	Information sharing and cooperation agreements signed with foreign governments and agencies	Analysis of information and production of reports	Appointments of senior staff	Appointments of oversight bodies within agencies
Ireland									
Italy - *COPASIR*	O	O	O	O			O		
Latvia - National Security Committee	O	O	O	O	O	O	O	O	
Lithuania - *Committee on National Security and Defence*				O			O	O	
Luxembourg									
Malta									
The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	O	O	O	O	O	O	O		
Poland (Sejm) - *Special Services Oversight Committee*	O		O	O	O	O	O	O	
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*		O	O	O			O		
Romania – *The Committee for Defence, Public Order and National Security*	O	O	O	O	O	O	O		
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	O	O	O	O	O	O	O		
Slovakia - *Committee for the oversight of the Slovak Information Service - Committee for the oversight of the National Security Authority of Slovak Republic*	O		O	O				O	
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	O			O			O		
Spain									
Sweden - *The Committee on Justice*							O		
Sweden - *The Commission on Security and Integrity Protection*	O	O	O	O	O	O	O		
The UK - *Intelligence and Security Committee (ISC)*		O		O	O	O	O		

4.5. Access to classified information by parliaments and specialised oversight bodies

Access to relevant information underpins the oversight of intelligence agencies. Given the secretive nature of these agencies' activities, this implies that overseers need access to classified information in order to scrutinise their work. This section will begin by examining national parliaments' access to information in general terms. This intends to provide the EP with an overview of parliamentary access to information across the EU. This overview will be followed by a detailed analysis of the modalities pertaining to access of information for specialised parliamentary and non-parliamentary oversight committees. This will include a comparative assessment of the types of information overseers need for scrutinising particular activities of intelligence agencies; the scope of oversight bodies' access to information; and common limitations on overseers' access to information.

While information is the lifeblood of oversight bodies, access to information by overseers should never be viewed as an end in itself. Access to relevant information is a means which helps overseers to fulfil their mandates. However, access to information alone does not ensure effective oversight; members and staffers of oversight bodies must also have the willingness, capacity and expertise to identify and make use of this information.[398]

4.5.1. Access to information by parliaments

Table 3 outlines the extent and modalities of parliamentary access to security related classified information in EU Member States that responded to this questionnaire. This table needs to be read with caution because it does not imply that parliaments/MPs which may access classified information of a particular level of classification can do so in regards to all information all of the time. Regardless of the scope and modalities of a parliament's access to classified information, a number of conditions and/or restrictions normally apply. First, the so-called 'need to know' principle—meaning that persons can only access information if their official functions necessitate access to particular information—applies in most parliaments.[399] Second, access to information by parliaments and non-parliamentary oversight bodies is often subject to restrictions (see below, section 4.5.3.) and a significant amount of executive discretion. Indeed, only five parliaments (Finland, Hungary, Lithuania, Slovakia and Sweden) stated that no restrictions can be imposed upon their access to information which would ordinarily be available to them.[400] Finally, while parliamentarians may have the right to access classified information, such access is sometimes subject to the individual concerned having signed a non-disclosure agreement and/or having received security clearance. For example, MPs in Romania must sign a confidentiality agreement before being given access to classified information; and MPs in Lithuania require a security clearance before they can access classified

[398] See, for example, in Annex A of this volume: Martin.
[399] E.g., Responses to question 4 of the DCAF-EUI questionnaire from the parliaments of Cyprus, Portugal, Finland, Lithuania and Romania.
[400] Responses to questions 7a–7b and 8 of the DCAF-EUI questionnaire from the parliaments of Finland, Hungary, Lithuania, Slovakia and Sweden.

information.[401] In practice, such conditions can serve to limit MPs' access to classified information. Some MPs may not wish to be vetted because, for example, they feel this violates the separation of powers, or may not want aspects of their private life examined.[402]

The responses to the DCAF-EUI questionnaire demonstrate that there are four main approaches to parliamentary access to information in EU Member States. For an overview, please refer to Table 3 (below).

[401] Responses to question 2 of the DCAF-EUI questionnaire from the parliaments of Lithuania and Romania.
[402] See in Annex A of this volume: Van Laethem.

Table 3: Parliamentary access to classified information in the field of national security

STATE	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Austria	Members of Particular Committees (*Standing Subcommittee of the Interior Affairs Committee and Standing Subcommittee of the National Defence Committee*)	Members of Particular Committees (*Standing Subcommittee of the Interior Affairs Committee and Standing Subcommittee of the National Defence Committee*)	Members of Particular Committees (*Standing Subcommittee of the Interior Affairs Committee and Standing Subcommittee of the National Defence Committee*)	Members of Particular Committees (*Standing Subcommittee of the Interior Affairs Committee and Standing Subcommittee of the National Defence Committee*)
Belgium	No Members	No Members	No Members	Members of Particular Committees (Monitoring Committee)
Bulgaria	All Members	All Members	All Members	All Members
Cyprus	No information provided on access according to level of classification. Classified information available to Members of Parliament in some circumstances.			
Czech Republic	All Members	All Members	All Members	All Members
Denmark	No Members	Members of Particular Committees (The Committee on Danish Intelligence Services)	Members of Particular Committees (various committees)	All Members
Estonia	All Members	All Members	All Members	All Members
Finland	Members of Particular Committees (various committees)	Members of Particular Committees (various committees)	Members of Particular Committees (various committees)	Members of Particular Committees (various committees)
France	Chairs of Particular Committees (Commission des Lois/ Commission de la Défense)	Chairs of Particular Committees (Commission des Lois/ Commission de la Défense)	Chairs of Particular Committees (Commission des Lois/ Commission de la Défense)	Chairs of Particular Committees (Commission des Lois/ Commission de la Défense)
Germany	All Members	All Members	All Members	All Members
Greece	No information provided on access according to level of classification. Classified information available to Members of Parliament in some circumstances.			
Hungary	Members of Particular Committees (Committee on National Security, Defense and Law Enforcement Committee)	Members of Particular Committees (Committee on National Security, Defense and Law Enforcement Committee)	Members of Particular Committees (Committee on National Security, Defense and Law Enforcement Committee)	Members of Particular Committees (Committee on National Security, Defense and Law Enforcement Committee)
Ireland	No Members	No Members	No Members	No Members
Italy	Members of Particular Committees (Parliamentary committee for the security of the Republic (COPASIR))	Members of Particular Committees (Parliamentary committee for the security of the Republic (COPASIR))	Members of Particular Committees (Parliamentary committee for the security of the Republic (COPASIR))	Members of Particular Committees (Parliamentary committee for the security of the Republic (COPASIR))
Latvia	Classified information available to some Members of Parliament. Detailed internal rules determine which Members of Parliament have access to specific levels of classified information.			
Lithuania	All Members	All Members	All Members	All Members
Luxembourg				
Malta				
The Netherlands	Group Leaders	Group Leaders	Group Leaders	All Members
Poland (Sejm)	Members of Particular Committees (Special Services Oversight Committee) President/Speaker Ad hoc parliamentary committees inquiry	All Members	All Members	All Members
Poland (Senat)	President/Speaker Members designated by the Speaker	All Members	All Members	All Members
Portugal	Members of Parliament often have access to classified information, but no specific rules have formally been established			
Romania	All Members	All Members	All Members	All Members
Slovakia	All Members	All Members	All Members	All Members
Slovenia	All Members	All Members	All Members	All Members
Spain	Ad hoc parliamentary inquiry committees	Chairs of Particular Committees President/Speaker of parliament	Chairs of Particular Committees Party/Group Leaders President/Speaker of parliament	Party/Group Leaders
Sweden	(Information not provided)			
The UK	Members of Particular Committees (Intelligence and Security Committee (ISC))	Members of Particular Committees (Intelligence and Security Committee (ISC))	Members of Particular Committees (Intelligence and Security Committee (ISC))	Members of Particular Committees (Intelligence and Security Committee (ISC))

4.5.1.1. Access by all MPs

There are a surprisingly large number of national parliaments (8) in which any MP can, in principle, have access to classified information up to and including information classified as 'Top Secret.' In a slightly higher number of parliaments (10) all MPs may access information classified 'Secret' (or lower) and in 12 parliaments all MPs may access information classified as 'Restricted' (see Table 3). However, these statistics need to be read with caution; it does not mean that all MPs can access any classified information at will. Conditions and caveats cited above normally apply to access to information by parliamentarians (see also, section 4.5.3.).[403]

4.5.1.2. Access by designated committee(s)

It is common practice for classified information (or certain levels thereof) to only be made available to certain parliamentary committees. These are generally the committees responsible for the oversight of intelligence agencies. For example, in Hungary, classified information (of any level) is only accessible to the National Security Committee, which is the committee mandated to oversee the intelligence agencies. Similarly in Italy, the Parliamentary Committee for the Security of the Republic (COPASIR) is the only committee of parliament that can access classified information. Elsewhere, e.g., in the Danish parliament, access is only limited to a designated committee if it is classified as 'Secret', that is, not one of the two lower levels of classified information 'Restricted' and 'Confidential'. It is axiomatic that if access to classified information is limited to particular committees, this must include any committee which oversees intelligence agencies.

In a number of states, e.g., France, access to classified information is further restricted because it is only made available to the chairs of designated parliamentary committees. This approach is problematic from the point of view of oversight because a committee chair alone cannot easily conduct oversight on the basis of such information. Information given exclusively to a committee chair can obviously not be used by the rest of the committee and is, therefore, of limited value for a committee's functions. Fortunately, such limitations do not generally apply to specialised parliamentary oversight committees.

4.5.1.3. Access by speakers and/or party leaders

In a number EU Member States access to classified information is restricted to party leaders or even the speaker of parliament. This is the case in the Dutch *Tweede Kamer,* where only party leaders are entitled to take part in meetings where information classified above 'Restricted' is discussed. Another example is the Polish *Senat,* where only the speaker can access information classified as 'Top Secret'. However, in this case the speaker is entitled to designate other MPs to receive access to the given information.[404]

Restricting access to classified information to the speaker and/or party leaders in parliament limits the utility of such information from the point of view of oversight. Speakers and group leaders are unlikely to be the MPs that are best placed to use the

[403] E.g., Responses to question 4 of the DCAF-EUI questionnaire from the parliaments of Cyprus, Portugal, Finland, Lithuania and Romania.
[404] Questionnaire response from the Polish *Senat,* question 4.

information to oversee intelligence agencies. This is because they deal with numerous other parliamentary affairs and do not have time to focus on oversight of intelligence agencies. A restriction of this nature means that these individuals are not permitted to discuss the information concerned with their colleagues and yet, they cannot be expected to make effective use of it on their own.

4.5.1.4. No access to classified information for parliamentarians

The parliament of Ireland is the only EU member state national parliament in which no MPs have access to classified information of any level. Elsewhere, there are absolute restrictions on any MP accessing classified information beyond particular levels of classification. In Denmark, for example, no MP can access information classified as 'Top Secret', while in Belgium, no MP can access information classified above the level of 'Restricted'. The impact of such restrictions on parliamentary access to higher levels of classified information likely depends on the extent to which higher levels of classification are used by a given intelligence agency. Classification practices vary greatly between states and the fact that a parliament cannot access any information classified as 'Top Secret' may not affect parliamentary oversight if, for example, most of the information relevant to oversight is classified at levels below 'Top Secret'.

4.5.2. Access to classified information by specialised oversight bodies

Having discussed parliamentary access to information in general terms, we will now turn to examine access to information by specialised parliamentary and non-parliamentary oversight bodies in more detail. Access to classified information by non-parliamentary oversight bodies is almost always regulated by the legislation upon which they are based; in the case of parliamentary oversight bodies, these provisions are usually distinct from those which apply to parliament as a whole.[405] For the purposes of this study, and the ongoing debate about the revision of Regulation 1049 at the EU level, it is imperative to note that regulations on access to information by oversight bodies are entirely decoupled from laws on public access to government documents (e.g., freedom of information legislation).

The framework for access to classified information by specialised oversight institutions can be broadly divided into four components: (1) the right of these bodies to request intelligence agencies, executives and other relevant parties to provide information relevant to their mandate; (2) an accompanying obligation for the executive and agencies to comply with such requests; (3) possible limitations on this right of access to classified information; and (4) a requirement for intelligence agencies and governments to proactively disclose certain types of information to overseers, without being requested to do so. It must be stressed that access to classified information by oversight bodies is inextricably linked to their mandate. Indeed, overseers' information needs should be defined by their mandate because in the absence of this anchorage there is a risk that overseers will either be unable to effectively fulfil their mandates due to a lack of information or will attempt to access information that may be unrelated to their work.

A number of the specialised parliamentary and non-parliamentary oversight bodies examined for this research have virtually unlimited access to classified information—held

[405] See, for example: Germany, Parliamentary Control Panel Act; UK, Intelligence Services Act, Schedule 3; Italy, Law 14/2007; Spain, Ley 11/2002.

by the executive, intelligence agencies, and other public bodies—which they deem to be relevant to the fulfilment of their mandate. This includes all information regardless of its form, level of classification, author or addressee. This can include information from foreign entities, sources and methods; see Table 4 for an overview of the scope of access to classified information by specialised oversight committees.[406] Oversight bodies that have full access to information can request access on their own initiative, as and when they deem necessary.[407] In some states, overseers have recourse to investigate powers and can call upon law enforcement authorities to enforce their right to access all information they deem to be necessary (see section 4.6). A failure to furnish an oversight body with requested information might be criminalised. These formidable powers provide overseers with predictability regarding access to information they need for their investigations, and can save them from having to indulge in endless legal battles to acquire information.

The following provisions from the laws on the Dutch CTIVD and the Canadian SIRC are excellent examples of a legal foundation for access to classified information by overseers:

> The relevant Ministers, the heads of the services, the co-ordinator and furthermore everyone involved in the implementation of this act and the Security Investigations Act will, if requested, furnish all information to the supervisory committee and will render all other assistance the supervisory committee deems necessary for a proper performance of its duties (Article 73(1) of the Dutch Intelligence and Security Services Act 2002).

> […] the Review Committee is entitled [..] to have access to any information under the control of the Service or of the Inspector General that relates to the performance of the duties and functions of the Committee and to receive from the Inspector General, Director and employees such information, reports and explanations as the Committee deems necessary for the performance of its duties and functions (Section 39(2), Canadian Security Intelligence Service Act 1984).

These examples highlight that it is oversight bodies, not the executive or the agencies being overseen, that should determine what information is relevant for their functions.[408] Indeed, this prerogative is fundamental to the effectiveness and independence of an oversight institution. The above examples also illustrate a legitimate circumscription on overseers' access to information: the requirement that the information is necessary for the performance of their functions or mandate. This helps to prevent 'fishing expeditions' by oversight bodies, whereby they cast around for (and gather) information which is irrelevant to their functions. Such provisions also help to guard against the acquisition of information for political purposes. Finally, it should be stressed that a legal right of access does not mean that insisting on access is always appropriate. There can be good grounds for self-restraint.

[406] This is, for example, the case in the Belgian Standing Intelligence Agencies Review Committee (Committee I) (Van Laethem, of Annex A), the US Congressional Intelligence Oversight Committee (Martin, in Annex A) and the Dutch Review Committee on the Intelligence and Security Services.
[407] United Nations Human Rights Council 17 May 2010, Practice 7; Verhoeven, in Annex A of this volume.
[408] See in Annex A of this volume: Verhoeven, and Forcese.

4.5.3. Restrictions on access to information

While it is good practice for oversight bodies to have access to all information which they deem to be necessary to the fulfilment of their mandate, many specialised parliamentary and non-parliamentary oversight bodies are faced with legal and practical restrictions on their access to classified information. In view of this reality, it is important to analyse these restrictions, evaluate the impact they have on the work of oversight bodies, and to consider how any restrictions on overseers' access to information can be limited to the greatest extent possible. Table 4 provides an overall picture of whether restrictions apply to access to particular types of classified information by specialised oversight bodies in EU Member States. This section will outline a number of these restrictions and briefly explain how they might impact on an oversight body's work.

4.5.3.1. General provisions granting the executive broad discretion to restrict access to information

In some states, the law contains very broad provisions which enable the executive and/or directors of intelligence agencies to deny oversight bodies access to information. The following extracts are illustrative of the breadth and vagueness of such provisions:

- In Italy, the executive can deny the Parliamentary Committee for the Security of the Republic access to information if it might 'jeopardise the security of the Republic'. [409]
- In the UK, the directors of the intelligence services can refuse to disclose information because (among other reasons) 'the Secretary of State (responsible minister) has determined that it should not be disclosed'.[410]

While acknowledging that there can be legitimate reasons for limiting access, provisions of this nature grant the executive too much discretion in deciding what an oversight body can and cannot access. There is a risk that a particular minister may interpret provisions very broadly to deny an oversight body access to information, and there may be limited or no recourse to challenge such decisions. It is important to note that the executive is part of the national intelligence system; ministers establish the priorities for the agencies involved, they may be responsible for authorising the use of special powers, and are ultimately the 'customers' for the assessments drawn-up by intelligence agencies. Therefore, the executive forms an important part of the system that is subject to scrutiny by oversight bodies. There is inevitable potential for conflicts of interest if the 'overseen' is also the 'gate-keeper' for access to information by overseers. One way of meeting executive concerns regarding revealing particularly sensitive information is to provide that, in specific cases where such concerns have been expressed, the oversight body may require that specified information may be divulged to it only after a decision by a special qualified majority. For example, in Hungary, two thirds of the parliament's National Security Committee can vote to require the executive/an agency to disclose specific information concerning an intelligence agency's methods.[411] This reduces the risk of inappropriate divulging of information, insisted upon by an individual member of the oversight body—perhaps from a 'maverick' political party.

[409] Italy, Law 14/2007, Article 31(8).
[410] UK, Intelligence Services Act 1994, Schedule 3, Para 3(b)(ii).
[411] Hungary – Act No. CXXV of 1995, Section 16(2).

4.5.3.2. Information pertaining to operations

As Table 4 illustrates, it is relatively common for oversight bodies to be barred from accessing classified information pertaining to the operations of intelligence agencies.[412] Such restrictions are sometimes formulated in general terms, as is the case in France and Australia, where the Parliamentary Joint Committee on Intelligence and Security, 'must not require a person or body to disclose to the Committee operationally sensitive information […]'.[413] Elsewhere, e.g., in Italy, Lithuania and Slovakia, restrictions apply specifically to ongoing operations,[414] meaning that, in theory, an oversight body can access information about operational activities once they have been completed.[415] However, there are problems with this distinction that can make it difficult for overseers to access the necessary information. First, it may be difficult to determine when an operation has finished; some operations might be 'ongoing' for many years, meaning that they remain impermeable to an oversight body.[416] Second, overseers invariably have to defer to an agency's assessment of whether an operation is ongoing or completed; this margin of discretion could be manipulated to shield a particular matter from the gaze of an oversight body. Finally, there is a risk that the area between 'policy' and 'operations', e.g., patterns of targeting and targeting priorities, falls outside the scrutiny.[417]

More commonly, national laws explicitly bar overseers from accessing information relating to the sources[418] and/or methods[419] used by intelligence agencies. Bars on overseers' access to information pertaining to sources are based on the fact that identities and roles of human sources are among the most sensitive aspects of an agency's work. Intelligence agencies are rightly concerned that any leak of a source's identity could jeopardise their personal safety. Information concerning an agency's methods is also extremely sensitive because agencies fear that the dissemination of such information could render methods ineffective, give an advantage to adversaries and/or endanger human sources.

Whether or not specialised oversight bodies have a legitimate need to access information about sources and methods, and operations more generally, depends to a large extent on their mandate. An oversight body with a mandate to oversee an intelligence agency's policies or administrative practices may have little need for this information. By contrast, if an oversight body is required to examine the legality and/or effectiveness of an agency's activities, it may need access to this information, at least on occasion. This is particularly true of methods. Notably, an oversight body may need to check whether a particular method falls within the parameters established by statutory law. While in most instances an oversight body with this type of mandate is unlikely to need to know the identities of sources, there may be some circumstances involving suspected serious

[412] France, Ordonnance n°58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, Article 6 nonies, Créé par Loi n°2007-1443 du 9 octobre 2007 - art. 1 JORF 10 octobre 2007 – alinéa III; Australia, Intelligence Services Act 2001, Schedule 1 (part 1); UK, Intelligence Services Act 1994, Schedule 3, paras. 3–4.
[413] Australia, Intelligence Services Act 2001, Schedule 1 (part 1).
[414] Questionnaire responses from Slovakia and Lithuania, Question 32.
[415] Italy, Law 14/2007, 31(8).
[416] Venice Commission Report 2007, para. 161.
[417] See, for example: the McDonald Commission's 'Second Report' makes reference to the 'policy of operations'.
[418] See, for example: Hungary, Act No. CXXV of 1995, Section 16(1) and Article 31(8); Italy, Law 14/2007, Article 31(8); Spain, Ley 11/2002, Article 11.2; UK, Intelligence Services Act 1994, Schedule 3, paras. 3–4; and De With and Kathmann, in Annex A of this volume.
[419] See, for example: Hungary, Act No. CXXV of 1995, Section 16(1); Spain, Ley 11/2002, Article 11.2; UK, Intelligence Services Act 1994, Schedule 3, para. 3. See also the questionnaire response of Lithuania to Question 32.

criminality, e.g., corruption or human rights violations, in which overseers might need information about sources as part of an investigation.

4.5.3.3. Information from foreign entities

The majority of specialised oversight bodies are faced with either restrictions or absolute bars on their access to information received from foreign entities.[420] Restrictions on oversight bodies' access to information intelligence agencies received from foreign entities are founded upon the 'third party rule', which underpins the sharing of information on domestic and international levels. This rule dictates that, before passing on information received from another entity to a third party, an institution must request permission from this entity. This is based on the notion that the originating party should retain control of information shared with another institution: the principle of 'originator control'.[421] Oversight bodies are often viewed as third parties and cannot therefore be given access to information received from foreign entities without the consent of these entities.[422] In theory, oversight bodies could access information received from foreign entities by demanding that intelligence agencies request permission from the originating entity. However, there is, to the best of our knowledge, no data available on how often such requests are made or indeed whether they are successful.[423]

Restrictions or absolute bars on overseers' access to the information that agencies receive from foreign entities can have profound implications for oversight. As we have already noted, the sharing of information between intelligence agencies on an international level has increased exponentially over the past decade. Intelligence agencies are increasingly reliant upon foreign entities for information and, consequently, an ever greater amount of information in their databases originates from foreign entities. As a result, more and more of the information held by intelligence agencies is deemed to be off-limits to overseers due to the aforementioned restrictions or absolute bars.[424] Needless to say, this has profound implications for the oversight of intelligence agencies.[425]

Some oversight bodies with extensive powers to access information from intelligence agencies have interpreted the third party rule in such a way that it does not prevent them from accessing information which the agencies receive from foreign bodies.[426] They assert that a legal right to access all relevant information leaves no room for exceptions.[427] Nevertheless, where overseers do access information from foreign entities, they exercise caution, mindful of the fact that intelligence agencies are extremely sensitive about their relations with foreign entities.[428]

[420] For examples of legal provisions in this regard, please see: France, Ordonnance n°58-1100 - art. 1 JORF 10 octobre 2007 – alinéa III; Italy, Law 14/2007, Article 31(8); Spain, Ley 11/2002, Article 11.2; UK, Intelligence Services Act 1994, Schedule 3, paras. 3–4; Germany, Parliamentary Control Panel Act, Section 6. See also: The Arar Inquiry, p. 316.
[421] Wills and Born 2011, p. 283.
[422] Ibid., p. 284.
[423] For an in-depth discussion of this issue see: Wills and Born 2011.
[424] See, for example: Roberts 2004, p. 263.
[425] Roberts 2006, p. 147; Wills and Born 2011, pp. 283-284 and 289-292; Sanchez, in Annex A of this volume.
[426] See, for example, the comments of Van Laethem and Verhoeven, in Annex A of this volume.
[427] See, for example, in Annex A of this volume, Verhoeven.
[428] See, for example: Wills and Born 2011, pp. 285–286 and 291; Van Laethem, in Annex A of this volume.

4.5.3.4. Information relating to judicial proceedings or criminal investigations

It is fairly common for oversight bodies to be barred from accessing information pertaining to ongoing judicial proceedings or criminal investigations.[429] These restrictions are applied in order to safeguard both the right to a fair trial and the state's ability to investigate and prosecute crime. They also serve ensure that oversight bodies abstain from examining matters that are subject to criminal or judicial investigations until such investigations have been completed.

4.5.3.5. Jurisdictional limitations on access to information

Oversight bodies are limited by the fact that their authority to access information only extends to agencies and officials of their own state. This has been a significant problem in the context of overseers examining various aspects of cooperation between their own state's agencies and foreign bodies. International intelligence cooperation, such as information sharing and joint-operations, leaves a 'footprint' in at least two states. Yet, oversight bodies can only examine the role played by their own state's agencies. For example, they might be able to see what information was sent to a foreign entity but may have no access to information regarding what the foreign entity requested or what it did with the information received. Equally, oversight bodies cannot require foreign officials to appear before them and have generally been unsuccessful with invitations to appear voluntarily. As a result of these limitations, oversight bodies often have an incomplete view of activities involving their own state's agencies.[430]

4.5.3.6. Practical limitations

Beyond legal restrictions on access to information by overseers, there are a number of practical limitations on their access. Firstly, overseers do not always know what information exists within an intelligence agency; this is perhaps unsurprising given the vast quantities of information held by agencies. This problem may range from not knowing about an entire programme, to not knowing that a particular email was sent or telephone call made. Regardless of their legal powers to access information, oversight bodies cannot access what they do not know about. It is for this reason that the proactive disclosure of certain categories of information is so important (see the following section 4.5.4.). Secondly, overseers cannot obviously access information which was never recorded or was destroyed, e.g., information from face-to-face discussions, telephone calls or notes taken by a field officer. To prevent this from happening, national law should be strict on the need for agencies to record everything and not to delete information without proper supervision.[431] Finally, it can be very hard for overseers to access information which is remotely located. This is particularly pertinent when information is held oversees, e.g., in a liaison office. Many oversight bodies do not have the resources to carry out inspections at all facilities within their own country, let alone overseas. Perhaps more importantly, overseers are unlikely to travel to a location where the agencies they are to oversee are working under cover, as this would obviously increase the likelihood of an agency's work being exposed.

[429] E.g., the SAKINT in Sweden (Cameron, in Annex A of this volume); Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 48(2).
[430] Wright 2011, pp. 177–179.
[431] Charkaoui v. Canada (Citizenship and Immigration), [2008] 2 S.C.R. 326, 2008 SCC 38, para. 64.

Table 4: The scope of access to classified information by specialised oversight committees

STATE	Future operations	Ongoing operations	Completed operations	Ministerial instructions/ directives issued to agencies	Budget and projected expenditure of agencies	Past expenditure	Agreements with foreign governments, agencies, and international organizations	Information received from other domestic agencies	Information received from foreign governments and security agencies	Information received from international organizations (e.g. the UN, EU or NATO)
Austria - Standing Subcommittee of the Interior Affairs Committee	No distinction is made/Relevant information may be provided									
Belgium - *Standing Intelligence Agencies Review Committee*	Unlimited	Unlimited	Unlimited	Restricted	Unlimited	Unlimited	Unlimited	Restricted	Unlimited	Unlimited
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Cyprus										
Czech Republic - *Permanent Commission on Oversight over the work of the Security Information Service (BIS)*										
Denmark - *The Folketing's Committee on the Danish Intelligence Services*	Restricted	Restricted	Restricted	Restricted	No	No	No	No	No	No
Estonia - *Security Authorities Surveillance Select Committee*	Unlimited	Restricted	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Restricted	Restricted
Finland - *The Administration Committee*	Restricted	Restricted	Restricted	Unlimited	Restricted	Restricted	Restricted	Restricted	No	Restricted
France - *Commission des Lois*	No	No	No	No	No	No	No	No	No	No
Germany - *Parliamentary Control Panel (PKGr)*	Restricted	Restricted	Restricted	Restricted	Unlimited	Restricted	Restricted	Restricted	Restricted	Restricted
Germany - *G10 Commission*	Restricted	Restricted	Restricted	Restricted	No	No	Restricted	Restricted	Restricted	Restricted
Greece - *Special Standing Committee for Institutions and Transparency*	No	No	Restricted	Restricted	No	No	No	No	No	No
Greece – *Authority for Communication Security and Privacy (ADAE)*	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted
Hungary - *Committee on National Security*	No	No	Unlimited	Unlimited	Unlimited	Unlimited	No	Unlimited	Unlimited	Unlimited
Ireland										
Italy - *COPASIR*	No	No	Restricted	Unlimited	Unlimited	Restricted	No	(information not provided)	No	No
Latvia - *National Security Committee*	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

STATE	Future operations	Ongoing operations	Completed operations	Ministerial instructions / directives issued to agencies	Budget and projected expenditure of agencies	Past expenditure	Agreements with foreign governments, agencies, and international organizations	Information received from other domestic agencies	Information received from foreign governments and security agencies	Information received from international organizations (e.g. the UN, EU or NATO)
Lithuania - *Committee on National Security and Defence*	No	Restricted	Restricted	Restricted	Unlimited	Unlimited	Restricted	Restricted	No	Restricted
Luxembourg										
Malta										
The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	Unlimited	Unlimited	Unlimited	Unlimited	Restricted	Restricted	Unlimited	Unlimited	Unlimited	Unlimited
Poland (Sejm) - *Special Services Oversight Committee*	Restricted	Restricted	Restricted	Restricted	Unlimited	Unlimited	Restricted	Restricted	Restricted	Restricted
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*	No	Unlimited	Unlimited	N/A	Unlimited	Unlimited	No	Unlimited	No	No
Romania – *The Committee for Defence, Public Order and National Security*	Restricted	Restricted	Restricted	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Restricted	Restricted
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	Restricted	Restricted	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Slovakia - *Committee for the oversight of the Slovak Information Service - Committee for the oversight of the National Security Authority of Slovak Republic*	No	No	No	(Information not provided)	Unlimited	Unlimited	No	No	No	No
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	No	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	No	No
Spain										
Sweden - *The Committee on Justice*	No	No	Restricted	Unlimited	Unlimited	Unlimited	No	No	No	No
Sweden - *The Commission on Security and Integrity Protection*	Restricted	Restricted	Restricted	Unlimited	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted
The UK - *Intelligence and Security Committee (ISC)*	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted

4.5.4. Proactive disclosure of information to oversight bodies

In many states, the power of oversight bodies to request information that they deem necessary is supplemented by a requirement for the executive and its intelligence agencies to proactively provide certain information to overseers. Proactive disclosures contribute to oversight in a number of ways. First, receiving information without having to request it and/or scour electronic and paper archives saves overseers' time; this is particularly valuable for parliamentary oversight committees, which have little time available and may have the detailed knowledge to know what to look for and where to look.[432] Second, proactive disclosures help to focus overseers' attention on particular issues or concerns. Otherwise, overseers may be forced to rely on complaints, whistleblowers or the media to make them aware of issues in the intelligence agencies. Third, intelligence agencies can benefit from proactively informing oversight bodies about threats to national security. This is particularly relevant with regards to parliamentary oversight committees where intelligence agencies can seek the support of MPs to ensure they have the necessary resources and legal powers to meet such threats. Finally, a clear legal provision on the proactive disclosure of information relating to intelligence agencies helps to provide overseers with a level of predictability regarding the information they will receive. We will highlight five types of information which are commonly subject to proactive disclosure.

4.5.4.1. Internal regulations of intelligence agencies and ministerial directives

In a number of the jurisdictions examined in this study, the executive and/or intelligence agencies are required to proactively disclose regulations and directives relating to the work of the agencies.[433] Such documents form part of the regulatory framework for agencies and their staff but are often classified and thus not widely available. An example of a requirement to disclose subsidiary regulations can be found in Belgian law which states that:

> The intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services shall, on their own initiative, send to the Standing Committee I the internal rules and directives, as well as all documents regulating the conduct of the members of these services.[434]

Access to such documents is important for overseers for several reasons. First, it helps them to ensure that subsidiary regulations and instructions comply with the statutory framework adopted by parliament. Second, these documents provide overseers with additional criteria against which they can evaluate the work of intelligence agencies. Finally, in the case of ministerial directives or instructions, overseers may be able to check whether the executive is making appropriate use of intelligence agencies and not, for example, requiring them to undertake tasks to promote political interests.

[432] See in Annex A of this volume: Sanchez.
[433] E.g., Australia, Inspector General of Intelligence Security Act 1986, Section 32B; Canada, CSIS Act, Section 6(2); Hungary, Act No. CXXV of 1995, Section 14 (3); Földvary, in Annex A of this volume.
[434] Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 33.

4.5.4.2. Information sharing and cooperation agreements

The second category of information which may be proactively disclosed to overseers is information sharing and cooperation agreements signed between intelligence agencies and other domestic or foreign entities (see also, sub-section 4.4.3.1.). These agreements regulate, among other things, when, how and under what conditions information may be shared, and the safeguards which apply to the use of shared information.[435] Canada provides one of the few examples of an intelligence agency being required to proactively disclose all such agreements to a specialised oversight body (see section 4.5.4.).[436] Receiving these agreements does not give overseers a say in the negotiation of such agreements or indeed a veto power. It does, however, enable them to (a) ensure that agreements (particularly with foreign entities) comply with statutory requirements, and (b) evaluate which entities an agency is sharing information or otherwise cooperating with. Accordingly, overseers can raise concerns about issues such as the human rights safeguards (or lack thereof) in these agreements. Indeed, several important authorities have recommended that oversight bodies review all international sharing and cooperation agreements in order to ensure improved accountability and human rights compliance.[437]

4.5.4.3. Information on the general activities of agencies and threat assessments

Information on the general activities of security and intelligence agencies is the category of information most commonly subject to proactive disclosure to overseers by governments and their intelligence agencies. This information typically includes an overview of the agencies' priorities, notable operations, and identified threats to national security and public safety.[438] The proactive disclosure of such information, on a periodic basis (typically every six months), is intended to keep overseers up-to-date on the work of security agencies, and thus to give them some idea as to whether the agency is fulfilling its statutory functions properly. Additionally, the disclosure of information about any major threats to national security can serve as an early warning mechanism to alert parliament to issues which require a response, such as the appropriation of additional resources or possible amendments to the law. This practice is used in Hungary where the relevant minister and/or director of the intelligence agency concerned provides a written report on such matters in advance of a hearing with the parliament's Committee on National Security.[439] While the proactive disclosure of general information about the activities of security/intelligence agencies can be useful for overseers, Susana Sanchez cautions against these obligations being vaguely defined.[440] The law should provide some clear guidance on what information must be disclosed within the context of reports or briefings on agencies' activities.

4.5.4.4. Information on the use of particular measures or powers

In some states, the responsible minister or agency director must proactively disclose ex post information about specific categories of activities and the use of particular powers.

[435] The Netherlands, Intelligence and Security Services Act 2002, Articles 37 and 59; The Arar Inquiry, p. 339; Croatia, Act on the Security Intelligence System, Article 59(2).
[436] Canada, CSIS Act, Section 17(2).
[437] United Nations Human Rights Council 17 May 2010, Practice 34; Venice Commission Report 2007, p. 182.
[438] See, for example: Hungary, Act No. CXXV of 1995, Section 14(2) and Section 15(1); Spain, Ley 11/2002, Articles 11.2 and 11.4; Germany, Parliamentary Control Panel Act, Section 4(1).
[439] See in Annex A of this volume: Földvary.
[440] See in Annex A of this volume: Sanchez.

In Germany, for example, the federal government is required to disclose to the *Bundestag's* Parliamentary Control Panel the intelligence services' use of a comprehensive list of powers. Notably, it must inform the Panel (every six months) on, inter alia, the implementation of surveillance measures, requests for information made to private companies, alerts entered into the police information system and certain information sent to foreign public authorities.[441] Furthermore, the law specifies that disclosures to the Panel must include information on the scope, duration and costs of such measures. Elsewhere, in Italy, the government must inform (within 30 days) the Parliamentary Committee for the Security of the Republic on any operations which authorised the intelligence services to commit an illegal act.[442] The proactive disclosure of information on the use of specific measures is primarily relevant when an oversight committee has a specific mandate to assess the legality or efficiency of such measures.

4.5.4.5. Budgetary information

Governments are often legally required to make proactive disclosures to specialised oversight committees about expenditure. These disclosures normally take place in addition to the annual budgetary appropriation and discharge process and are, for example, required by law in Italy and Spain.[443] Similarly, US intelligence agencies are required to make numerous proactive disclosures of financial information; notably, the Director of National Intelligence is required to report to Congress any findings on illegality pertaining to the implementation of the agencies' budgets.[444] Such disclosures can help to strengthen the financial oversight of intelligence agencies by responsible committees in parliament aware of matters that need to be addressed in future budgetary appropriation and discharge processes.

4.6. Methods and powers of specialised oversight bodies

Oversight bodies use a range of methods to conduct oversight and require certain statutory powers in order to do so. For the purposes of this section, these powers will divided into the power to initiate investigations and powers that ensure access to classified information, which are of course intrinsically linked to an oversight body's access to classified information (see section 4.5).

Oversight bodies use many different methods for scrutinising the work of security/intelligence agencies. While a detailed examination of all of these methods would be highly technical and unnecessary for the purposes of this study, we shall highlight some of the main methods that are used before discussing the power of own-initiative investigation, which is of fundamental importance.

Firstly, for some oversight bodies, and particularly parliamentary oversight committees, scrutiny is largely based around periodic hearings or meetings, at which agencies' reports or forthcoming plans are discussed.[445] Second, overseers often examine particular issues

[441] Germany: Article 10 Act (G10), Section 14(1); Federal Act on Protection of the Constitution (BVerfSchG), Section 8(a)(6), Section 17(3) and Section 18(1)(a). See also in Annex A of this volume: De With and Kathmann.
[442] Italy, Law 14/2007, Article 33(4).
[443] See in Annex A of this volume: Fabbrini and Giupponi; Sanchez.
[444] US, National Security Act 1947, Section 102A(c)(7B).
[445] Responses to question 25 of the DCAF-EUI questionnaire showed that almost every oversight body uses such hearings.

in light of a tragedy or a scandal that has surfaced in the media, e.g., the UK Intelligence and Security Committee's work on the 2005 London bombings and the UK services' role in rendition.[446] It is, of course, important that oversight bodies can provide this type of reactive oversight. Yet, it is also important that oversight bodies do not wait for major problems to arise before scrutinising particular aspects of an agency's work. Third, oversight may take place on the basis of requests from other institutions; it is very common for parliament, the executive and even the agencies themselves to be able to refer matters to both parliamentary and non-parliamentary oversight bodies.[447] In this way, parliament, the executive and the agencies can utilise the expertise of an oversight body to get independent assessment of a particular issue. However, in order to preserve the independence of oversight bodies, they should retain the final say on whether or not to examine a particular matter at the request of another institution. Finally, some oversight bodies, particularly non-parliamentary bodies, have a mandate to handle complaints and therefore conduct oversight of the basis of concerns raised by members of the public or employees of intelligence agencies.[448]

4.6.1. Own-initiative investigations

While the aforementioned mechanisms form an important basis for oversight, the position of an oversight body is greatly strengthened if, within the parameters of its mandate, it is empowered to initiate its own investigations as and when it deems necessary.[449] This power is widely regarded as being integral to the independence of oversight bodies and helps to ensure that oversight cannot be constrained by incumbent governments or their agencies.[450] This power extends not only to decisions on what to examine, but also how such investigations will be carried out.[451] It should be noted that overseers' own-initiative powers are sometimes limited by prerequisites, such as the need for the overseer to have evidence of illegal activities before launching an investigation.[452] In our view, it is good practice for no such conditions to be imposed on the right to initiate investigations, so long as the issues examined fall within an oversight body's mandate.

Own-initiative investigations may concern particular events or persons but more commonly are thematic investigations. This means that an oversight body undertakes a detailed examination of a particular aspect of an intelligence agency's work, such as its use of undercover informants, relations with foreign entities, or compliance with its obligation to excise old data.[453] Overseers generally select the subjects for thematic investigations on the basis of a combination of matters that have arisen through the

[446] Please see the ISC's website for further information on these reports: (http://isc.independent.gov. uk/committee-reports/special-reports).
[447] Responses to question 25 of the DCAF-EUI questionnaire indicate that in 15 of the EU member states which responded, the plenary of parliament may request a specialised (non)parliamentary oversight body to investigate particular matters. In 16 states the intelligence agencies can make such requests, and in 12 states the executive may do so. See also: Australia, Inspector General of Intelligence and Security Act 1986, Section 8.
[448] Venice Commission Report 2007, paras. 241–250.
[449] Responses to question 25 of the questionnaire illustrate that an overwhelming majority of the specialised oversight bodies examined in this research possess this power in some form.
[450] The Arar Inquiry, p. 317; see in Annex A of this volume Leigh, and Cameron.
[451] See in Annex A of this volume: McGarrity. Also see Kate Martin on the US Congress' Intelligence Committee staff investigations in this regard.
[452] Hungary, Act No. CXXV of 1995, Section 14(4)(e).
[453] For a list of examples please see: the investigations undertaken by Belgian Committee I (http://www.comiteri.be/index.php?option=com_content&task=view&id=41&Itemid=75&phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb&lang=FR); the Canadian Security Intelligence Review Committee (http://www.sirc-csars.gc.ca/opbapb/lsrlse-eng.html); and the Dutch CTIVD (http://www.ctivd.nl/?English).

types of oversight mentioned in the introduction to this section, as well as on the basis of concerns raised by civil society groups and the media.[454] Thematic investigations by security/intelligence overseers were pioneered by Canada's Security Intelligence Review Committee and have become an integral component of many specialised oversight bodies' work, e.g., Sweden's SAKINT, the Dutch CTIVD, the Belgian Committee I, and the Norwegian *EOS-Utvalget* Committee.[455] The use of thematic investigations is seen to be necessary in view of the fact that overseers cannot scrutinise everything which agencies do and must therefore focus on particular issues.[456] Thematic investigations are, however, highly resource intensive. Consequently, they are more commonly conducted by non-parliamentary oversight bodies which, as we have noted, tend to be better resourced and have more time (see section 4.3.5.).

4.6.2. Powers to ensure access to classified information by overseers

The previous section (4.5) outlined the scope of access to classified information by specialised oversight bodies. As was mentioned, overseers require certain powers and tools at their disposal in order ensure access to classified information from intelligence agencies and executives (see Table 5). Recourse to such powers varies greatly between oversight bodies; this sub-section will outline a number of these.

[454] See in Annex A of this volume: Van Laethem; Martin.
[455] See in Annex A of this volume: Cameron, Verhoeven, and Van Laethem. See also: Australia, Inspector General of Intelligence and Security Act 1986, Section 8.
[456] Canadian Security Intelligence Review Committee (cited in Forcese, in Annex A of this volume).

Table 5: The powers and methods available to specialised oversight committees

STATE	Receive and review annual reports of agencies	Periodic meetings with management of agencies	Invite management to give testimony at other times	Invite external experts	Invite members of the public	Subpoena intelligence officers to testify	Subpoena members of the executive branch to testify	Subpoena agencies to provide evidence	Inspect premises of intelligence agencies
Austria - *Standing Subcommittee of the Interior Affairs Committee*				O	O				
Belgium - *Standing Intelligence Agencies Review Committee*	O	O	O	O	O	O			O
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	O	O	O	O				O	O
Cyprus									
Czech Republic - *Permanent Commission on Oversight over the work of the Security Information Service (BIS)*	O	O	O	O					O
Denmark - *The Folketing's Committee on the Danish Intelligence Services*	O	O							
Estonia - *Security Authorities Surveillance Select Committee*	O	O	O	O	O				O
Finland - *The Administration Committee*	O	O	O	O	O				
France - *Commission des Lois*		O							
Germany - *Parliamentary Control Panel (PKGr)*	O	O	O	O	O				O
Germany - *G10 Commission*		O	O	O	O				
Greece - *Special Standing Committee for Institutions and Transparency*			O						
Greece – *Authority for Communication Security and Privacy (ADAE*			O	O	O				
Hungary - *Committee on National Security*	O	O	O	O	O			O	O
The Irish Republic									
Italy - *COPASIR*	O	O	O	O				O	O

STATE	Receive and review annual reports of agencies	Periodic meetings with management of agencies	Invite management to give testimony at other times	Invite external experts	Invite members of the public	Subpoena intelligence officers to testify	Subpoena members of the executive branch to testify	Subpoena agencies to provide evidence	Inspect premises of intelligence agencies
Latvia - *National Security Committee*	O	O	O	O	O				
Lithuania - *Committee on National Security and Defence*	O	O	O	O	O				
Luxembourg									
Malta									
The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	O	O	O	O	O	O	O	O	O
Poland (Sejm) - *Special Services Oversight Committee*	O	O	O	O	O				
Poland (Senate) - *Human Rights, Rule of Law and Petitions Committee*	O	O	O	O					
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*	O	O	O	O	O				O
Romania – *The Committee for Defence, Public Order and National Security*	O	O	O	O	O				O
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	O	O	O	O	O				O
Slovakia - *Committee for the oversight of the Slovak Information Service - Committee for the oversight of the National Security Authority of Slovak Republic*	O	O		O	O				O
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	O	O	O	O					O
Spain									
Sweden - *The Committee on Justice*	O								
Sweden - *The Commission on Security and Integrity Protection*	O		O	O					
The UK - *Intelligence and Security Committee (ISC)*	O	O	O	O	O				O

4.6.2.1. Meetings with directors and other employees of intelligence agencies

As Table 5 indicates, almost all of the specialised oversight bodies examined in this study can invite directors of intelligence agencies, as well as the relevant ministers, to appear before them. Such meetings take place on a scheduled, periodic basis, as well as on an ad hoc basis when the oversight body deems a meeting to be necessary. This is perhaps the most basic way that an oversight body can get information about the work of intelligence agencies and discuss, inter alia, reports issued by agencies. In many instances, overseers cannot require directors or ministers to appear before them but, in practice, these individuals are unlikely to refuse to meet an oversight body because it would make for extremely bad publicity. Some oversight bodies, however, have the power to subpoena officials to appear before them (see below).

Some oversight bodies can also interview or invite agency employees below the director to appear before them.[457] However, overseers' access to rank and file employees is often more limited and subject to certain conditions, such as a requirement for political approval. For example, the Italian parliament's COPASIR can only invite such persons to appear before the committee after receiving the permission of the prime minister.[458] The French parliament's DPR is not permitted to invite anyone below director level to appear before it.[459] Such limitations can interfere with the capacity of an oversight body to determine how it wishes to examine particular issues, and a 'political filter' on access to rank and file employees could be abused to block access to persons whose information the executive or agency wishes to conceal.

4.6.2.2. Subpoena powers

While most oversight bodies can invite directors and even rank and file employees of intelligence agencies to appear before them, a select few have the power to subpoena relevant persons and/or documents in order to enforce their right to access information (see Table 5).[460] That is, they can require someone to appear before them to answer questions or require an agency to provide a document. Accordingly, non-cooperation with oversight bodies may be criminalised and the oversight body concerned can normally have recourse to law enforcement bodies in order to require a person appear before them or otherwise furnish information.[461] Furthermore, many of these oversight bodies can require that persons testify before them on oath or affirmation.[462] These formidable powers are most commonly held by oversight bodies which have a mandate to oversee the legality of an agency's operational activities. This is partly because operations are among the most secretive and closely guarded aspects of intelligence agencies' work and they may be reluctant to disclose information about these activities, particularly when they have violated the law. Having the option of using subpoena powers is also necessary in the context of investigating complaints about possible violations of an individual's

[457] E.g., the US Congressional Intelligence Committees (cited in Martin, in Annex A of this volume) and the Hungarian Parliament's National Security Committee (cited in Földvary, in Annex A of this volume).
[458] Italy, Law 14/2007, Article 31(2).
[459] See in Annex A of this volume: Lepri.
[460] See, for example: The Netherlands, Intelligence and Security Services Act 2002, Article 74; Australia, Inspector General of Intelligence and Security Act 1986, Sections 18–19. On the US Congressional Intelligence Committees, see Martin, in Annex A of this volume.
[461] See, for example: Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 48; Germany, Parliamentary Control Panel Act, Section 5.
[462] See, for example: Australia, Inspector General of Intelligence and Security Act 1986, Sections 18–19; Belgium, Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment, Article 48.

rights, where it is clearly imperative that an overseer has access to all relevant information.[463] However, in spite of this, specialised oversight bodies rarely need to use the powers described in this paragraph. These powers are best viewed as an option of last resort, in the event that an agency or the executive fails to cooperate with an investigation.

4.6.2.3. Inspections

Many specialised oversight bodies have the power to inspect installations under the control of intelligence agencies.[464] They can often do so on their own initiative, without the permission of the agencies but, in practice, overseers announce inspections to agencies as a matter of courtesy. Inspections are often used as an opportunity to speak to rank and file staff, carry out checks on physical files and, more generally, to improve overseers' awareness of the work of intelligence agencies.

4.6.2.4. Direct access to electronic and paper files

Some oversight institutions, with very extensive access to information, have direct, independent access to the files of intelligence agencies. For example, the Dutch CTIVD and Belgian Committee I both have their own facilities on the premises of the intelligence agencies, which permit them to log in directly to an agency's files.[465] This means that they examine information as and when they deem necessary without any kind of 'filtering' by the agencies. Such powers are only likely to be necessary if an oversight body has a mandate to conduct in-depth oversight of operational activities, as is the case for both the specialised non-parliamentary oversight bodies mentioned above.

4.7. Protection of information handled by specialised oversight bodies

It has been firmly established that overseers of intelligence agencies need access to classified information in order to perform their functions. However, this access comes with obligations regarding the security of information. Oversight bodies have to take steps to ensure that classified information, to which they have privileged access, is handled in a way that does not lead to leaks or other forms of unauthorised disclosure. A failure to handle classified information correctly may, among other things, lead to violations of the right to privacy; compromise the effectiveness of intelligence agencies; put at risk persons working for these agencies; and, ultimately, jeopardise the capacity of the agencies to tackle threats to security and public safety. Equally, unauthorised or accidental disclosures of information by an oversight body may significantly undermine oversight of intelligence agencies. This is because such disclosures are likely to compromise an oversight body's relationship with the agencies it oversees, and may lead to agencies withholding cooperation on access to classified information and/or failing to

[463] For example, Canada's Security Intelligence Service Act explicitly mentions subpoena powers in this context (CSIS Act, Section 50).
[464] See, for example, the German Parliament's Control Panel (cited in De With and Kathmann, in Annex A of this volume); the Italian COPASIR (Italy, Law, Article 31(14–15)); the Australian Inspector General for Intelligence and Security (Australia, Inspector General of Intelligence and Security Act 1986, Section 9b, 18–19); and the Dutch Parliament's Intelligence and Security Services Committee (The Netherlands, Rules of Procedure of the Dutch Second Chamber 1994, Chapter 7, Paragraph 5).
[465] See in Annex A of this volume: Verhoeven, and Van Laethem.

take account of future recommendations by the oversight body.[466] As Canada's Justice O'Connor stated in the Arar Inquiry: 'the ability to maintain secrecy is viewed as vital to the ability of a review agency to gain the trust of the agencies that it reviews and the executive branch of government'.[467] That said, on the national level there is little evidence that oversight bodies are the source of unauthorised disclosures of information relating to intelligence agencies. [468]

This section will outline the procedures that specialised oversight bodies put in place to ensure that classified information is handled correctly and not accidentally or intentionally disclosed. We will focus on three main mechanisms in this regard: (1) measures to ensure that appropriate persons are appointed as members and staffers of oversight bodies; (2) penalties for unauthorised disclosure of classified information; and (3) physical measures to protect information.

4.7.1. Measures to ensure appropriate persons are appointed to oversight bodies

Security clearances are one of the cornerstones of policies to prevent the unauthorised disclosure of information. A security clearance process involves an intelligence agency or the police vetting a prospective member or staffer of an oversight body to check whether there are any underlying affiliations, interests or vulnerabilities which could lead them to disclose classified information for*,* inter alia*,* money, political and business interests, or through blackmail. This vetting procedure provides a risk assessment and it is usually the prerogative of another institution, such as the executive or the oversight body itself, to decide whether, on the basis of the assessment, someone should be granted security clearance and appointed. It is good practice (as is the case for the Hungarian parliament's National Security Committee) for the oversight body itself to take the final decision on whether to appoint someone on the basis of a vetting report.[469] This serves to prevent the intelligence agencies or the executive from using security clearance processes as a means for controlling the membership of oversight bodies which scrutinise their work.

It is, however, important to be mindful that granting a person security clearance does not mean that they will not make an unauthorised disclosure of classified information. Nevertheless, security clearance can be viewed as a confidence building mechanism which builds trust—and probably encourages the flow of information—between oversight bodies and the intelligence agencies they oversee. In fact, it has been argued that oversight bodies whose members are subject to security clearance receive better access to information. [470]

There is a notable divergence in practice between parliamentary and non-parliamentary oversight bodies with regards to security clearance (see Table 6). With the exception of some post-authoritarian EU Member States (e.g., Estonia, Hungary, Lithuania and Poland) members of parliamentary oversight bodies in the EU (and parliamentarians more generally) are not subject to security clearance.[471] This is can be explained by the fact that in many states, the security clearance of parliamentarians would be considered

[466] Venice Commission Report 2007, p. 36.
[467] The Arar Inquiry, p. 316.
[468] See in Annex A of this volume: Leigh, and Martin.
[469] Hungary, Act No. CXXV of 1995, Section 19. See also Földvary, in Annex A of this volume.
[470] Venice Commission Report 2007, p. 49.
[471] This is also the case in Australia, Canada and the US.

to be a violation of the separation of powers.[472] It may be argued that it is inappropriate for an executive branch agency to delve into the private affairs and past activities of a democratically elected representative, particularly if there are concerns that information derived from these processes may be used for political purposes, e.g., to smear political opponents. Moreover, parliamentarians are often considered to be security cleared by virtue of their position as elected representatives; Kate Martin and Charlotte Lepri explain that this is the case in the US Congress and French parliament, respectively.[473]

By contrast, members of non-parliamentary oversight bodies are generally required to have security clearance irrespective of their status as, e.g., former judges and even incumbent parliamentarians (see Table 6). While practices regarding the vetting and security clearance of members of oversight bodies vary, it is a near universal requirement for staffers of both parliamentary and non-parliamentary oversight bodies to require security clearance before being appointed.

Another measure for ensuring that appropriate persons are appointed to oversight bodies (and thus given access to classified information) is the selection processes outlined in section 4.3.4. of this chapter. For example, when overseers (both parliamentary and non-parliamentary) are appointed by a majority of parliament, this helps to ensure that only persons deemed to be suitable are appointed—the majority of parliament is unlikely to appoint someone who is viewed as a security risk. Equally, in systems where party leaders in parliament and/or the speaker of parliament select MPs for parliamentary oversight committees, it is likely that they will choose people who are viewed as being responsible and acceptable to other parties and the executive. Finally, when the executive appoints members of oversight bodies, it can be reasonably assumed they will not select anyone who is seen to be a security risk.[474]

[472] This is, for example, the case in the Netherlands (see Verhoeven in Annex A of this volume).
[473] See in Annex A of this volume: Martin and Lepri.
[474] See in Annex A of this volume: Leigh.

Table 6: Security clearance for members and staff of specialised oversight committees

		Members		Staff	
STATE	**Type of Oversight Committee**	**Access to Classified Information**	**Security Clearance Required**	**Access to Classified Information**	**Security Clearance Required**
Austria - *Standing Subcommittee of the Interior Affairs Committee*	Parliamentary Committee	YES	NO	YES	NO
Belgium - *Standing Intelligence Agencies Review Committee*	Non-parliamentary committee	YES	YES	YES	YES
Bulgaria - *Foreign Affairs and Defence Committee (Standing subcommittee)*	Parliamentary Committee	YES	NO	YES	YES
Cyprus					
Czech Republic - *Permanent Commission on Oversight over the work of Military Intelligence*	Parliamentary Committee	YES	NO	YES	NO
Czech Republic - *Permanent Commission on Oversight over the work of the Security Information Service (BIS)*	Parliamentary Committee	YES	NO	YES	NO
Denmark - *The Folketing's Committee on the Danish Intelligence Services*	Parliamentary Committee	YES	NO	YES	YES
Estonia - *Security Authorities Surveillance Select Committee*	Parliamentary Committee	YES	YES	YES	YES
Finland - *The Administration Committee*	Parliamentary Committee	YES	NO	NO	NO
France - *Commission des Lois*	Parliamentary Committee	NO (only the Chair)	YES	NO	NO
Germany - *Parliamentary Control Panel (PKGr)*	Parliamentary Committee	YES	NO	YES	YES
Germany - *G10 Commission*	Non-parliamentary committee	YES	YES (if they are not Members of Parliament)	YES	YES
Greece - *Special Standing Committee for Institutions and Transparency*	Parliamentary Committee	YES	NO	NO (only the Committee secretary and the minute clerks of the Parliament)	NO
Greece – *Authority for Communication Security and Privacy (ADAE*	Non-parliamentary committee	YES	NO	YES	NO
Hungary - *Committee on National Security*	Parliamentary Committee	YES	YES	YES	YES
Ireland					

		Members		Staff	
STATE	**Type of Oversight Committee**	**Access to Classified Information**	**Security Clearance Required**	**Access to Classified Information**	**Security Clearance Required**
Italy – *COPASIR*	Parliamentary Committee	YES	NO	YES	NO
Latvia - *National Security Committee*	Parliamentary Committee	YES	YES	YES	YES
Lithuania - *Committee on National Security and Defence*	Parliamentary Committee	YES	YES	YES	YES
Luxembourg					
Malta					
The Netherlands - *Review Committee on the Intelligence and Security Services (CTIVD)*	Non-parliamentary committee	YES	YES	YES	YES
Poland (Sejm) - *Special Services Oversight Committee*	Parliamentary Committee	YES	YES	YES	YES
Poland (Senate) - *Human Rights, Rule of Law and Petitions Committee*	Parliamentary Committee	YES	NO	YES	YES
Portugal - *Council for the Oversight of the Intelligence System of the Portuguese Republic*	Non-parliamentary committee	YES	NO	NO	NO
Romania – *The Committee for Defence, Public Order and National Security*	Parliamentary Committee	YES	NO	YES	YES
Romania - *The Joint Standing Committee for the exercise of parliamentary control over the activity of the SRI*	Parliamentary Committee	YES	NO	YES	YES
Slovakia - *Committee for the oversight of the Slovak Information Service* **-** *Committee for the oversight of the National Security Authority of Slovak Republic*	Parliamentary Committee	YES	NO	YES	YES
Slovenia - *Commission for the Supervision of Intelligence and Security Services*	Parliamentary Committee	YES	NO	YES	YES
Spain					
Sweden - *The Committee on Justice*	Parliamentary Committee	YES	NO	YES	YES
Sweden - *The Commission on Security and Integrity Protection*	Non-parliamentary committee	YES	YES	YES	YES
The UK - *Intelligence and Security Committee (ISC)*	Non-parliamentary committee	YES	NO	YES	YES

4.7.2. Penalties for unauthorised disclosure of classified or otherwise confidential information

In the vast majority of states, the law provides for the same sanctions for unauthorised disclosures of classified information by members and staffers of oversight bodies as apply to any other person with access to such information.[475] In at least 23 of EU Member States whose parliaments responded to the questionnaire for this study, unauthorised disclosures of information by oversight bodies are criminalised.[476] This applies to both parliamentary and non-parliamentary oversight bodies. While members of oversight bodies may be prosecuted for making unauthorised disclosures, we are not aware of any recent examples of the prosecution of such persons.

It is important to note that in most states parliamentarians do not normally enjoy immunity from prosecution for unauthorised disclosures of information—there is strict liability for such disclosures. However, possible immunity may be assessed on a case-by-case basis because some disclosures may fall within the scope of actions for which parliamentarians have immunity from prosecution.[477] Alternatively, parliament may have to waive an MP's immunity before any prosecution can proceed; this is the case, for example, in Poland.[478] The application to parliamentarians of criminal law provisions on unauthorised disclosure remains a highly contentious issue. Indeed, the possibility of criminal penalties for unauthorised disclosures may be seen as interfering with parliamentarians' right to free speech, as well as the parliamentary privilege which ordinarily provides immunity for anything which is said in the context of parliament.[479] There is evidence that in the U.S. Congress, the threat of sanctions for disclosing classified information has led some members to abstain from accessing it altogether.[480] This is clearly undesirable from the point of view of promoting effective oversight.

Beyond criminal penalties, there are a number of other sanctions which may be applied to members and staffers of oversight bodies in the event that they disclose classified information without proper authorisation. Firstly, members of both parliamentary and non-parliamentary oversight bodies may have their membership suspended or revoked.[481] Secondly, a person's security clearance may be revoked meaning that they can no longer access classified information.[482] Thirdly, some parliaments, such as the Spanish *Cortes*, can dock parliamentary allowances or even deny a member the right to vote for breaches of rules of procedure, such as the unauthorised disclosure of classified information.[483] Finally, some parliaments, e.g., the Lithuanian *Seimas*, have the power to impeach MPs for the unauthorised disclosure of classified information.[484] Such sanctions may, for example, be used if the disclosure is not deemed to be sufficiently serious to warrant criminal proceedings or if there are doubts about whether a case can be successfully prosecuted due to immunities such as the parliamentary privilege.

[475] See by way of example: Australia, Intelligence Services Act 2001, Schedule 1, part 2, (9, 10, 12) and Italy, Law 14/2007, Article 36, as well as Fabbrini and Giupponi in Annex A of this volume; Germany, G10 Act, Sections 17–18; UK, Intelligence Service Act 1994, Section 11(2).
[476] Responses to question 35 of the DCAF-EUI questionnaire.
[477] Response to question 35 of the DCAF-EUI questionnaire from the parliament of the Czech Republic.
[478] Response to question 35 of the DCAF-EUI questionnaire from the Polish *Sejm*.
[479] See in Annex A of this volume: Van Laethem.
[480] Milligan 2006.
[481] This is, for example, the case in Spain under the Spanish *Cortes'* Rules of Procedure (see Sanchez, in Annex A of this volume). See also Fabbrini and Giupponi, Annex A of this volume, on the Italian parliament's COSAPIR and Van Laethem on the Belgian Committee I (in Annex A of this volume).
[482] Responses to question 35 of the DCAF-EUI questionnaire from the Romanian Chamber of Deputies, the Polish *Sejm,* the Dutch CTIVD and the Belgian Committee I.
[483] See in Annex A of this volume: Sanchez.

4.7.3. Physical measures to protect classified information

It is beyond the scope of this study to provide a detailed overview of the technical measures which oversight bodies take to protect classified information. Instead, we will provide an overview of a number of the principal mechanisms which are used.

4.7.3.1. In camera meetings

Perhaps the most basic measures which most oversight bodies take is to hold most, if not all, of the meetings *in camera*.[485] Such meetings are not accessible to the public and, in the case of parliamentary oversight bodies, MPs who are not members of the committee are excluded. This is often regarded as being necessary in order to protect classified information and to ensure that the identities of intelligence agency employees who testify before oversight bodies are kept secret. However, it may be seen as particularly problematic for parliamentary oversight committees to have a policy of holding all meetings behind closed doors. This is because secret meetings militate against the principle of transparency which is meant to pervade parliaments. Parliamentarians represent their constituents and are accountable to the public for their work in parliament. It is difficult for the public to monitor the work of their representatives if this work takes place entirely behind closed doors.

The US Congress' intelligence committees are notable for taking a more open approach to their meetings. They have managed to strike a balance between the competing demands of protecting classified information and transparency by adopting a policy that meetings should be open unless it is necessary to 'close' them because classified matters are under discussion. As Kate Martin argues, this is a very good policy because it ensures that hearings attract media interest, and enable civil society groups to engage in particular issues.[486] Conversely, holding public meetings risks politicising oversight; as Martin observes, public meetings provide an opportunity for members of an oversight committee to make statements or take positions for political gain.[487] *In camera* meetings do not give overseers the opportunity to 'play' to an audience and therefore it is perhaps more likely that they will focus on scrutinising the work of intelligence agencies.

If oversight bodies hold all of their meetings *in camera*, it is essential that they issue comprehensive public reports on their work. In the absence of public meetings, reporting and/or some form of public minutes are the only ways that overseers can inform the general public about their work, and the principal means for them to engage with the media and civil society.[488]

4.7.3.2. Other measures to protect information

A significant number of parliamentary and non-parliamentary oversight bodies can have access to classified information on their own premises, rather than having to view it on the

[484] Response to question 35 from the Lithuanian *Seimas.*
[485] All specialised oversight bodies cited in responses to the DCAF-EUI questionnaire hold meetings behind closed doors.
[486] See in Annex A of this volume: Martin.
[487] Ibid.
[488] Almost all of the specialised oversight bodies cited in responses to the DCAF-EUI questionnaire produce public reports.

premises of intelligence agencies.[489] This applies to both 'physical' documents and information in an electronic format. Accordingly, oversight bodies use a raft of different measures to protect information. These measures range from secure meeting rooms which have controlled access to measures designed to shield premises from remote communication devices, highly secure IT systems, and encrypted communications channels. Broadly speaking, the measures used to protect information are similar to those used by intelligence agencies themselves. In order to build confidence regarding the protection of information, some oversight bodies, such as the Australian parliament's Joint Standing Committee on Intelligence and Security, are required to consult with the agencies in order to ensure that their security of information arrangements meet appropriate standards.[490] This type of consultation is a good idea given that intelligence agencies have significant expertise in these matters.

4.8. Conclusion

This chapter has provided a detailed insight into the oversight of intelligence agencies by national parliaments and specialised non-parliamentary bodies. We have focussed on six important issues in this regard, including: the rationale for oversight of intelligence agencies; the configuration of systems for oversight of these agencies; the mandates of specialised parliamentary and non-parliamentary oversight bodies; access to classified security related information by these bodies and parliaments more generally; the powers and methods of specialised oversight bodies; and the protection of information handled by overseers. Our analysis has demonstrated that the legal and institutional frameworks for oversight by parliamentary and non-parliamentary oversight bodies vary greatly between states. There is no single 'best' approach to organising and conducting parliamentary and specialised oversight of intelligence agencies. Yet, this chapter has shown that there are practices which are notable for promoting comprehensive and robust scrutiny of intelligence agencies, thus helping to ensure that these agencies not only comply with applicable law but also perform their statutory functions effectively. It must be stressed that not all of the practices discussed in this chapter are of relevance to the European Parliament in the development of its oversight of the EU's AFSJ bodies. We shall however, conclude by underlining several of the principles and practices discussed in this chapter, which may be particularly salient for the EP; chapter five will draw on many of these points to formulate recommendations for developing the EP's oversight of the AFSJ bodies.

Throughout this chapter we alluded to a number of general principles of successful oversight of intelligence agencies, we shall reiterate just three of these. Firstly, oversight bodies – be they parliamentary or non-parliamentary – require access to information that is relevant to their mandate, as well as recourse to appropriate powers and methods to gain access to such information. This is fundamental to both the effectiveness and credibility of oversight bodies. Secondly, oversight requires an appropriate balance between the demands of transparency and the need to protect classified information. This is essential for, on the one hand, ensuring that the work of oversight bodies is relevant beyond the 'ring of secrecy,' and on the other, ensuring that oversight bodies are both trusted and accepted by the agencies they oversee. Finally, oversight must be based on an appropriate respect for the separation of the roles and responsibilities of oversight bodies, and those of agencies and the executive branch. Notably, it is not the prerogative of the agencies or the executive to determine what should be overseen or which information is relevant to the

[489] See in Annex A of this volume: Sanchez and McGarrity.
[490] Australia, Intelligence Services Act 2001, Schedule 1 (part 3, 22).

scrutiny of particular matters. Equally, it is not the role of oversight bodies to meddle in the management or direction of the activities of intelligence agencies.

In addition to these general principles, this chapter identified a number of specific practices and findings that may be of interest to the EP:

- Many national parliaments have opted to establish specialised oversight committees because committees with jurisdiction over broad policy areas such as justice and home affairs do not have the time or resources to engage in ongoing oversight of intelligence agencies;
- In many states there is one specialised parliamentary oversight body responsible for scrutinising all intelligence agencies, or specific intelligence functions regardless of which public bodies perform them;
- It is difficult to advocate a 'best' approach or practice in regard to the subject(s) of an oversight body's mandate. Ultimately, what matters is that all dimensions of an intelligence agency's work are overseen by a body which is independent from the agencies and the executive;
- In some Member States, parliaments can request a non-parliamentary oversight body to examine a particular matter, but the latter body has the final decision on whether or not they will examine an issue at the request of parliament or any other entity;
- It is standard practice for specialised oversight committees of national parliaments to be able to summon the member of the executive responsible for a particular intelligence agency;
- Some national parliamentary oversight committees include of *ex officio* members of other parliamentary committees that have jurisdiction over related matters;
- The majority of parliaments are not involved in the appointment of the directors of intelligence agencies;
- The review of information sharing agreements by oversight bodies is seen as a good practice which has been adopted by several states;
- Regulations on parliamentary access to information are almost always separated from regulations on public access to information;
- In almost every state analysed in this study, parliaments have privileged access to classified information to enable them to, inter alia, oversee intelligence agencies;
- On the national level, specialised committees responsible for the oversight of intelligence agencies are almost always one of the bodies (or the only body) in parliament which has access to classified information in the security domain;
- It is preferable for the law to provide oversight bodies with a general right to request access to classified information which it deems to be relevant to its mandate and functions, rather than promulgating a specific list of the types of information an oversight body can have access to;
- It is common practice for intelligence agencies and/or the executive to be required to proactively disclose information on threats to national security to parliament;
- In the majority of European Union states, MPs are not subject to security clearance;
- Most states criminalise unauthorised disclosure of classified information by MPs and other overseers.

CHAPTER 5. RECOMMENDATIONS FOR STRENGTHENING OVERSIGHT OF THE AFSJ BODIES BY THE EUROPEAN PARLIAMENT

5.1. Introduction

The final chapter of this study will formulate recommendations which might be useful for the forthcoming debate on how the European Parliament's oversight of the AFSJ bodies could be strengthened. These recommendations are developed on the basis of the main findings from chapters two (on the current mandates and powers of the AFSJ bodies), three (on the oversight of AFSJ bodies by the EP, JSBs and national parliaments) and four (on the role of national parliaments and non-parliamentary bodies in overseeing intelligence agencies). This chapter is divided into four main sections. The first addresses appropriate limitations on the EP's mandate to oversee the AFSJ bodies, that is, the aspects of their work that should not be directly overseen by the EP. The second section outlines the general parameters of the EP's oversight mandate of the AFSJ bodies and, on this basis, highlights a number of specific oversight functions which the EP could perform. In the third section of this chapter, we will discuss two essential conditions for strengthening the EP's oversight of the AFSJ agencies: the development of a legal framework for access to classified information by the EP, and the adoption of appropriate procedures to protect classified information handled by the EP. The final section of this chapter will consider some of the institutional mechanisms that the EP could use to fulfil its oversight mandate and functions. This discussion includes the option of creating a sub-committee of the LIBE Committee, which responds to the EP's explicit request for this study to provide recommendations on the establishment of its own 'oversight body' (see chapter one).

While the national practices discussed in chapter four have been used extensively to inform the recommendations to the EP, we have also drawn upon past proposals put forward by the EP and the Commission, as well as extensive interviews with officials at EU institutions and AFSJ bodies. Although much can be learned from studying the oversight of intelligence agencies at the national level, we should remain cautious about transplanting practices from the national level (examined in chapter four) to the European level. This is because there are important differences between national intelligence agencies and the AFSJ bodies, as well as between national parliaments and non-parliamentary oversight bodies and the EP. Unlike national intelligence agencies, the AFSJ bodies do not have recourse to special powers to collect information. They cannot, for example, use covert agents to gather information, intercept communications or conduct surveillance operations. Equally, the AFSJ agencies do not perform the same functions or possess the same coercive powers as their contemporaries on a national level: police services, prosecutors and border agencies. Notably, they cannot question, arrest or detain suspects. The AFSJ bodies' 'operational powers' primarily consist of two elements: 1) coordinating and supporting the work of national agencies; and 2) processing, storing and transferring personal data.

Some of the recommendations outlined in this chapter apply to the EP's oversight of all AFSJ bodies discussed in this study (i.e. Europol, Eurojust, Frontex and Sitcen); however, most focus exclusively on the AFSJ agencies (i.e. Europol, Eurojust, Frontex). This is because the EP has an explicit treaty mandate to oversee Eurojust and Europol, and will be a co-legislator for new regulations on these agencies and Frontex. The development of

parliamentary oversight of the Sitcen will have to proceed along a different track because Sitcen falls under the Common Foreign and Security Policy (CFSP), an area in which the EP has fewer powers. The recommendations pertain to the oversight of the AFSJ bodies as they exist in May 2011. Oversight arrangements should be developed in tandem with any changes to the mandates and powers of these bodies, and should remain commensurate with the activities being overseen.

In developing legal and institutional frameworks for parliamentary oversight of the AFSJ bodies the EP and other relevant stakeholders should remain mindful that oversight arrangements should not have the effect of dissuading member states from using these bodies to cooperate in the AFSJ. Most EU member states are now convinced of the added value that agencies such as Europol and Eurojust can have in supporting their own work.[491] Yet, there is a risk that if oversight arrangements place too great a burden on the AFSJ bodies and/or national authorities, some member states may simply revert to bilateral channels of cooperation, which are less heavily regulated and perhaps not subject to the same levels of scrutiny.[492] Any moves in this direction would undermine the capacity of the AFSJ bodies to contribute successfully to promoting freedom, justice and security in the EU.

Recommendation 1: The European Parliament should ensure that any new arrangements for the oversight of the AFSJ bodies do not serve to dissuade member states from using these bodies as platforms for cooperation.

5.2. Limitations on the scope of the European Parliament's oversight of the AFSJ bodies

Before going on to discuss the scope of the EP's oversight mandate and functions, we will highlight several factors which should circumscribe the EP's oversight of the AFSJ bodies. These primarily relate to oversight of the AFSJ bodies' operational activities. Firstly, the intergovernmental nature of the AFSJ bodies and the relationship between actions of the AFSJ bodies and Member States has important implications for oversight. Member States' police, prosecutorial, border and (to a much lesser extent) intelligence agencies are both the principal suppliers and the main customers of the AFSJ bodies. The AFSJ bodies function primarily on the basis of information provided by national agencies and their principal output is information and analysis that is sent to these agencies. National agencies may take action, including the use of coercive powers, on the basis of such information, including within the context of operations coordinated by an AFSJ body such as Europol or Frontex. As we noted in chapter two, such action remains the exclusive responsibility of national authorities. The implication of this is that both the inputs to AFSJ bodies and actions taken on the basis of the outputs of these bodies are regulated by national law and should be overseen by appropriate national authorities. It is widely accepted inside the EP and in Member States that it is not the prerogative of the EP to oversee how national agencies collect information that might be shared with AFSJ bodies and/or action undertaken on the basis of information provided by AFSJ bodies.

Secondly, the AFSJ bodies consist of a mix of personnel seconded by the Member States and EU staff members. National liaison officers at Europol, national border guards that participate in a Frontex-coordinated operation, or seconded intelligence officers at Sitcen are paid by Member States and cooperate with the agencies in accordance with national

[491] Interviews 18, 19.
[492] Ibid.

laws. As such, their cooperation with and contributions to an AFSJ body are more appropriately overseen by national oversight mechanisms. It was outside the scope of the mandate of this study to examine in detail how Member States oversee national authorities' performance of these activities. Indeed, this topic would merit an in-depth study of its own. Nevertheless, these institutional realities are a crucial factor that should be taken into account in developing an oversight mechanism at the European Parliament. Indeed, this intergovernmental element of the AFSJ bodies requires that the EP works closely with national parliaments in ensuring that appropriate oversight arrangements are in place.

Thirdly, Europol and Eurojust are authorised to process, store and transfer personal data within the parameters of their mandates. These are activities which interfere with the right to privacy and may serve as the basis for use of coercive or special powers—which have particularly significant human rights implications—by member or third states' authorities. In view of this, these activities clearly need to be subject to oversight by an independent body. Accordingly, the EU has established specialised non-parliamentary oversight bodies—the Joint Supervisory Bodies (JSBs) of Europol and Eurojust—for this purpose. The JSBs have access to all files and premises related to the processing of personal data and are in a strong position to ensure that any practices which violate data protection regulations are corrected. In our view, the JSBs are an appropriate oversight mechanism for scrutinising the use of personal data by the AFSJ agencies. Accordingly, their activities do not need to be duplicated by the EP. Equally, the EP would not need to oversee Frontex's future role in processing personal data because it is envisaged that the European Data Protection Supervisor would perform a similar function to the JSBs.

There are several other arguments against involving the EP in the oversight of the AFSJ bodies' operational activities on an ongoing basis. First, as we noted in chapter four, this is extremely time consuming and requires specialised expertise and resources which many parliaments do not possess. A number of the MEPs and staffers interviewed for this study indicated that the EP would not have the time, resources, or inclination to scrutinise the operational activities of the AFSJ bodies.[493] Oversight can be conducted more effectively by a 'professional' oversight body, such as the JSBs, that focuses exclusively on the oversight of an agency's operational activities. Second, giving the EP a mandate to oversee information processing would require the parliament to have access to personal data in these files, which would raise significant privacy concerns. Finally, parliamentary scrutiny of the operational aspects of the AFSJ bodies' work might adversely impact upon the effectiveness of these bodies. This is because many states are opposed to giving the EP a role in this regard and may reduce information sharing with the AFSJ bodies if the EP was given such a role.[494]

5.3. The European Parliament's oversight mandate and functions

There was widespread agreement among our interlocutors at various EU institutions and bodies that the EP should play a role in overseeing the AFSJ bodies. Oversight of the AFSJ bodies by parliament and bodies created by parliament is important for the reasons outlined in chapters one and four. Perhaps most importantly, the EP is now a co-legislator in the AFSJ and will have a pivotal role in defining the future mandate and powers of the AFSJ agencies in particular. Therefore, it is essential that the EP plays a role in ensuring

[493] Interviews 1, 4, 11, 13, 17, 18, 28 and 29.

that these agencies fulfil their mandates effectively and in a manner which complies with relevant legislation. In addition, the AFSJ agencies are funded to a large extent with EU funds that are appropriated to them by the EP. As the budgetary authority, the EP must have a role in ensuring that such money is used both correctly and efficiently.

These rationales for parliamentary oversight of the AFSJ agencies do not, however, imply that the EP should play a role in their management. When discussing the EP's role in the oversight of AFSJ bodies, we should remain mindful of the separation of powers and responsibilities in this regard. This is particularly important in relation to Eurojust because it works with judicial bodies. Oversight of the AFSJ bodies should also not be conflated with controlling or co-managing an agency—this is not the role of a parliament. The AFSJ bodies are meant to serve as repositories of expertise which exist to provide a professional service to the EU and its Member States. It is not the role of parliamentarians to meddle in the management of this work; such functions are primarily the prerogative of the agencies' directors and their management boards. Meanwhile, the Commission and/or Council provide political direction to AFSJ bodies and assume political responsibility for them. For these reasons, the involvement of the EP in matters such as the appointment of management board representatives, or even as part of the management boards of the AFSJ agencies is not recommended. Indeed, the involvement of the EP in these decision-making processes would obfuscate its oversight functions, making it extremely difficult to subsequently review independently the actions of agencies and their management boards.

Recommendation 2: The European Parliament should not be part of the management boards of Europol or Frontex, or of the College of Eurojust.

In chapter four we argued that it is difficult to advocate a 'best' approach or practice in regard to the subject(s) of an oversight body's mandate. Ultimately, what matters is that all dimensions of an intelligence agency's work are overseen by a body which is independent from the agencies and the executive. In the case of the EU, this means independent from the AFSJ bodies, the Council and the Commission. In chapter four, we showed that the subject of oversight can be broadly divided into four areas: operations, policy, administration and finance. In view of the foregoing comments on the role of the JSBs and national authorities in overseeing the operational activities of the AFSJ bodies, it is clear that the EP should focus on overseeing the policies, administration and finance of these bodies. This is, however, without prejudice to the EP's powers of inquiry (discussed in chapter three), under which the EP could of course examine allegations that any activities of these agencies violate EU law.

Recommendation 3: The European Parliament's oversight of the AFSJ agencies should focus on their policies, administration and finance.

5.3.1. Oversight of the finances of the AFSJ agencies

Chapter three demonstrated that the EP has considerable powers with regards to the appropriation and discharge of the AFSJ agencies' budgets. The EP can make better use of these powers in its oversight of the AFSJ agencies by ensuring a continued link between the oversight of agencies' policies and administration and Parliament's budgetary appropriation and discharge functions. The entire budget cycle requires close cooperation between the LIBE Committee (or any newly created body with a mandate to oversee the AFSJ agencies),

[494] Council of the European Union 22 February 2011.

the Committee on Budgets (BUDG) (with a mandate to approve the budget of the AFSJ bodies) and the Committee on Budgetary Control (CONT), which is mandated to discharge the budgets of the AFSJ bodies. There are four main ways in which the EP can effectively continue and improve the use of its budgetary oversight powers in this regard. First, the EP needs to continue to strengthen the cooperation between CONT, BUDG and the LIBE Committee throughout the budget cycle to ensure that there are links between the oversight of the AFSJ agencies' finances and other areas of their work. Second, some members of the LIBE Committee need to be made more aware of the formidable budgetary and discharge powers at the EP's disposal and how LIBE can work with the BUDG and CONT committees to more effectively use these powers in the fulfilment of its mandate. Third, the power of the purse (both the reserve procedure and the power to withhold or delay discharge of a budget) can be used as a tool for requesting a change in the policies, procedures or activities of the AFSJ agency concerned. Finally, as we mentioned in chapter three, the reserve procedure may, in some exceptional circumstances, be used as a tool to persuade an AFSJ agency to disclose information in any area that is financed from the EU budget. This should not however, be necessary if a new legal framework for access to classified information by the EP is adopted (see below).

Recommendation 4: The European Parliament should ensure its budgetary appropriation and discharge functions are fully linked to other aspects of its oversight of AFSJ agencies.

5.3.2. Keeping the European Parliament informed about security threats

The European Parliament needs to be informed about threats to the security of the EU and its member states in order to fully evaluate the measures that are needed to counter such threats. Without this information, it is hard for the EP to fully assess whether the AFSJ bodies may, for example, need new powers (i.e., requiring legislative amendments), additional resources or new cooperation agreements with particular third states. Indeed, this is an excellent example of an area in which the EP should ensure that there is a close relationship between its role as a legislator, budgetary authority and overseer. Making the EP aware of pertinent threats may also be in the interests of the agencies because in this way they can make MEPs aware of their need for additional legal powers or resources; MEPs may be useful allies in this regard (see chapter four). The EP could, for instance, be provided risk assessments and threat analyses from Frontex, the full version of Europol's Organised Crime Threat Assessment, or terrorist threat assessments from the Sitcen (see chapter two). Such assessments are classified and would therefore, need to be provided to the body within the EP designated to receive classified information (see section 5.5). In this context, the responsible body could hold *in camera* discussions with relevant officials from the AFSJ bodies.

Chapter four indicated that, on the national level, it is common practice for intelligence agencies and/or the executive to be required to proactively disclose – to a designated committee – information pertaining to security threats. This usually takes place on a periodic basis (typically every 6 months), and is intended to keep overseers up-to-date on the threats intelligence agencies are facing, and to give them some idea as to whether an agency is fulfilling its functions effectively.

Recommendation 5: The European Parliament should receive threat assessments from the AFSJ bodies. This would enable Parliament to better assess whether these bodies have the necessary legal mandate, powers and financial resources to address such threats.

5.3.3. The European Parliament's relationship with the Joint Supervisory Bodies

As we noted in chapter three, the EP currently has very limited engagement with the two JSBs. Closer engagement with the JSBs could begin with inviting their chairpersons to discuss their biennial and thematic reports with the relevant body within the EP (see the options discussed in section 5.5.). This dialogue would allow the chairs of the JSBs to express any concerns about their mandate, powers or the resources available to them. Meetings between the EP and JSBs could also serve as a forum to discuss the implementation of JSBs' recommendations. On this basis, the EP could use its political clout to raise any concerns with agency directors or management boards, and it could use its budgetary powers to address such matters. More regular engagement with the JSBs could also benefit MEPs in the carrying out of their work. Indeed, on a national level, the expertise of non-parliamentary oversight bodies is to be of great value to parliaments, which can use their reports to inform their own oversight and legislative work.[495] The JSBs are repositories of significant amounts of knowledge and expertise which could benefit MEPs when, for example, preparing for hearings with agency directors or drafting own-initiative or legislative reports on Europol and Eurojust. MEPs and their staffers may benefit from this expertise not only through periodic hearings but also by reviewing the JSBs' reports and holding informal discussions with members of the JSBs and their secretariat.

In the context of closer engagement between the EP and the JSBs (or other specialised non-parliamentary oversight bodies that are created), a body of MEPs may need to be given access to the inspection reports of the JSBs. What the EP will not need is access to data inputted into Europol's databases or Eurojust's CMS, and/or personal data shared with national authorities or third states. Access to this data would give rise to serious privacy concerns.[496] If, in the context of its oversight functions, the EP does have access to documents which contain personal data, personal data should be deleted from these documents, as is foreseen under Annex Two of the 2010 Framework Agreement between the Commission and the Parliament.[497]

The EP could consider adopting the practice used in some Member States whereby parliament can request a non-parliamentary oversight body to examine a particular matter (see chapter four). This is a more direct means by which a parliament can take advantage of both the expertise and independence of a non-parliamentary oversight body in order to examine particular aspects of an agency's work. To our knowledge, the EP cannot currently make such requests to the JSBs. Any provisions of this nature would need to be carefully formulated to ensure that the independence of a non-parliamentary oversight body, such as the JSBs, could not be compromised by such requests from the EP. Accordingly, much can learned from the good practice on a national level, namely that non-parliamentary oversight bodies have the final decision on whether or not they will examine an issue at the request of parliament or any other entity (see chapter four).

Recommendation 6: The European Parliament should engage in regular dialogue with the Joint Supervisory Bodies (JSBs) of Europol and Eurojust, and should make use of the reports and expertise of the JSBs in its own oversight of the AFSJ agencies.

[495] See, for example, Nick Verhoeven, Annex A.
[496] Interviews 18, 19, 30 and 31.
[497] Interinstitutional Agreement of 20 November 2010 between the European Parliament and the European Commission, *Framework Agreement on relations between the European Parliament and the European Commission*, Article 3.2.2 of Annex 2.

5.3.4. Standardisation of the European Parliament's right to summon the directors of AFSJ agencies

The EP currently has the power to require the Director of Europol and the Chairperson of the Europol Management Board to appear before it.[498] This power should be extended to Frontex (the Director and Chair of the management board) and Eurojust (the Administrative Director and President of the college). While the European Parliament does not have these powers with respect to Eurojust and Frontex, it needs to be stressed that, in practice, directors of the AFSJ agencies often appear before the parliament upon its request and are aware that refusing to appear before parliament would make for bad publicity.[499]

The power to summon agency directors and chairpersons of the management boards/college could be particularly useful outside the context of agency directors presenting an agency's annual report. It would, for example, enable the EP to require the appearance of a director in the event of a particular problem or scandal coming to light. However, the right to summon the director of an AFSJ body may be of limited value unless the MEPs involved have the right to discuss classified matters. Under existing procedures, directors cannot or choose not to answer questions which would entail disclosing classified information.[500] This further illustrates the need to formulate a proper framework for parliamentary access to classified information before developing other oversight mechanisms (see below).

As chapter four illustrated, it is standard practice for specialised oversight committees of national parliaments to be able to summon the member of the executive responsible for a particular intelligence agency. Similarly, most oversight committees can summon the director of an intelligence agency. In Chapter four, we noted that in some cases this power also extends to any member of an intelligence agency's staff. This can help to ensure overseers are able to speak to the member of an agency's staff best qualified to discuss a particular issue. The power to summon members of staff below the directors is, however, normally attached to oversight institutions that oversee the operational activities of agencies and it is most commonly available to oversight bodies responsible for examining the legality of particular actions (see chapter four). In view of the oversight role the EP is likely to play, we do think that it would be necessary for it to posses this power.

We have opted to confine this recommendation to the AFSJ agencies, i.e., not to include the director of Sitcen. It is difficult to envisage how this formal power could be extended to the director of Sitcen because it is not an autonomous agency. The EP can, however, request the High Representative for Foreign and Security Policy, under whom Sitcen falls, to appear before it.

Recommendation 7: The European Parliament's power to summon the director of Europol and the chairperson of the Europol Management Board should be extended to the equivalent persons at Eurojust and Frontex.

5.3.5. Oversight of the appointment of agency directors

Currently, the EP does not play any role in the appointment of AFSJ agency directors or the director of Sitcen. Yet, the EP has long expressed a desire to be involved in the

[498] Article 48 of the Europol Decision.
[499] Interview 33.
[500] Interviews 14, 22, 32.

appointment of directors of these bodies. Chapter four's survey of the role of national parliaments in the appointment of directors of intelligence agencies demonstrated that the majority of parliaments are not involved in the appointment of the directors of intelligence agencies. However, chapter four also showed that some parliaments do play a role in this regard; we shall highlight two approaches to involving parliaments in the appointment of agency directors, which may be of interest to the EP.

Firstly, some parliaments—through their specialised oversight committees—are able to hold a hearing with a nominee and can issue a non-binding opinion or recommendation on the proposed appointment (see chapter four). This is an option which has periodically been proposed in various contexts at the EU level. As far back as 2002, the Commission proposed making formal appointments of candidates for the post of the Europol director dependent upon a hearing before the EP.[501] However, it is noteworthy that the Commission later rejected the idea of giving the EP this role in its 2010 communiqué on Europol.[502] The EP has also recommended this option in the context of past discussions on Europol's legal framework.[503] Moreover, in 2004 the EP proposed amendments to the Council Decision on Frontex, which would have required candidates for the position of executive director to appear before the EP.[504] In both cases, the EP's suggestions were dismissed and not included in the final Council decisions. Finally, there is precedent for the EP's AFET Committee holding an exchange of views with proposed candidates in the context of the selection of delegation heads for the newly established EEAS.[505] This format could be extended to prospective directors of Sitcen.

This option would entail the EP holding a hearing with the proposed candidate in order to solicit their views on pertinent issues such as the priorities of the AFSJ body and/or the body's relations with third states. The responsible committee could draft an opinion on the suitability of a proposed candidate on the basis of such discussions. These hearings could be held by the LIBE Committee or the LIBE Sub-committee discussed below (in the case of the directors/president of Europol and Frontex and the president of Eurojust), and by the AFET Committee (in the case of Sitcen). The right to hold a hearing and issue a report/opinion on prospective directors would not entail a veto power but would nevertheless influence the Council's (or High Representative's in the case of Sitcen) final decision on whom to appoint.

A second way in which a few national parliaments are involved in the appointments of the directors of intelligence agencies is through a vote to approve (or reject) nominees. This, of course, gives parliament a veto in the appointment process (see chapter four). It is interesting to note that the EP has requested this power with respect to the appointment of the director of Sitcen but not in regard to the AFSJ agencies.[506] This procedure would operate in much the same way as the first option with the difference being that the EP would vote on whether or not to approve a nominee, rather than simply issuing a non-binding recommendation.

There are a number of drawbacks associated with involving the EP in the appointment of directors; these are broadly similar to arguments outlined in chapter four. First and

[501] Commission of the European Communities 11 December 2002, p. 11.
[502] European Commission 17 December 2010, p. 16.
[503] European Parliament 14 March 1996; De Mera 15 November 2007, Amendment 40.
[504] von Boetticher 24 February 2004, Amendment 37. It should be noted that this proposal was not taken up in the final decision on Frontex and the EP has not included this mechanism in the ongoing discussions on the legal framework for Frontex.
[505] De Witte and Rijpma, Annex B.
[506] European Parliament 4 April 2007, para. 54.

foremost, involving the EP in the appointment of directors risks politicising the work of agencies which are meant to be non-political. This concern would be magnified if parliament's role in the appointment of directors were to include the power to approve or reject a nominee. This concern was expressed by a number of persons interviewed for this study and was cited by the Commission in its 2010 Communiqué on Europol.[507] Secondly, the current process for selecting the directors/president of Europol, Frontex and Eurojust is already protracted and cumbersome because it involves representatives of 27 Member States seeking to find a compromise candidate. Adding the EP to this process would serve to further complicate and drag out an already lengthy process. Moreover, the fact that 27 states are already involved in the selection of directors ensures that there are inbuilt checks and balances, which prevent any single party appointing a director to promote their interests. This removes one of the main reasons for which national parliaments are involved in the appointment of the directors of intelligence agencies: to prevent the incumbent government appointing someone to promote and protect partisan political interests.

All things considered, the authors are not persuaded that the European Parliament should be given a role in the appointment of directors of the AFSJ bodies. The parliament should, however, be kept informed regarding appointment processes. This should include information on the identity and credentials of proposed candidates.

Recommendation 8: The European Parliament should not be given a role in the appointment of the directors/president of the AFSJ bodies.

5.3.6. A role for the European Parliament in providing assessments on the human rights records of AFSJ bodies' cooperation partners

While the JSBs provide an opinion on the legal and institutional frameworks for data protection in third states, they do not examine the broader human rights record of particular foreign partners, such as a police agency in a third state. There is, therefore, no independent assessment of whether or not agencies with which AFSJ bodies share information use techniques which violate human rights. As was discussed in chapter four, this is relevant to both incoming and outgoing information as foreign partners may collect information through e.g., torture or arbitrary detention and then share this information with AFSJ bodies. On the other hand, they may use information provided by AFSJ bodies as part of activities which violate human rights. These concerns are primarily relevant to the sharing of personal data.

Although the AFSJ bodies' own due diligence processes should prevent this from happening, it is good practice for an independent oversight body to provide some form of human rights assessment of the general human rights record/compliance of partner agencies in third states. There is precedence for this at the national level (see, for example, the role played by Canada's Security Intelligence Review Committee) and this is a role which could be performed by the EP or another independent body. If the EP were to assume this role, it would make sense to involve the AFET Committee's Sub-Committee on Human Rights, which has expertise in examining human rights matters outside the European Union. Such assessments would not be binding but could serve to inform the Council and AFSJ agencies' management boards in the context of entering into information sharing agreements with third states.

[507] European Commission 17 December 2010, p. 16.

Recommendation 9: The European Parliament should ensure that either a (sub)committee of parliament or a specialised non-parliamentary body provides independent assessments of the general human rights records/compliance of agencies in third states with which the AFSJ bodies cooperate. Such assessments could take place before an information sharing or other cooperation agreement is signed with a third state, and during the implementation of these agreements.

5.3.7. A role for the European Parliament in reviewing the AFSJ bodies' information sharing agreements and memoranda of understanding

While we do not believe that the EP should play a role in overseeing the content of information sharing between the AFSJ bodies and/or between AFSJ bodies and third states or organisations, it is important for the EP to have access to the agreements upon which such sharing is based. Chapter two indicated that the European Parliament has access to some information sharing agreements concluded between the AFSJ bodies and third states, notably Europol's and Eurojust's agreements with third states. It does not, however, have access to, for example, the memoranda of understanding Frontex has concluded with foreign entities, or any agreement of Sitcen.

Information sharing agreements are an important part of agencies' policy and should therefore, be subject to review by the EP. Indeed, it is important that the EP is aware of the terms upon which the AFSJ bodies cooperate with each other, and with foreign entities. In our view, the EP should not play a role in the formulation or approval of agency to agency information sharing agreements or memoranda of understanding (which are distinct from agreements between the EU and third states, such as the SWIFT agreement). However, a designated body of parliament should be able to review, ex post, agreements that have been concluded and to raise questions or concerns regarding, inter alia, the content and implementation of such agreements. It is not sufficient for the EP to be simply made aware that such agreements exist. Accordingly, the AFSJ bodies should be required to forward agreements and memoranda of understanding to relevant bodies in parliament, even if such agreements are considered to be classified (see section 5.4.1.2). Chapter four identified the review of information sharing agreements by oversight bodies as being a good practice which has been adopted by several states, and endorsed in UN standards on intelligence oversight.

Recommendation 10: The European Parliament should have access to information sharing agreements and other memoranda of understanding concluded between AFSJ bodies within the European Union, as well as between AFSJ bodies and third states or organisations.

5.4. Access to and the protection of classified information

As our analysis of oversight of intelligence agencies at the national level demonstrated, information is the oxygen that sustains oversight; a mandate to oversee an agency's work is of limited use unless it is accompanied by access to the relevant information. It will be extremely difficult to strengthen parliamentary oversight of the AFSJ bodies without clear and predictable rules and procedures for the EP to access relevant information from these bodies, the Commission and the Council. While access to relevant information is fundamental to oversight, the professional handling of this information by overseers is also crucial for effective oversight. Accordingly, improved access to classified information by the

EP will need to be accompanied by the development of appropriate procedures for the protection of this information, as well as an ongoing commitment from MEPs to handle classified information properly. This section will address these two issues in turn.

5.4.1. Improving the European Parliament's access to classified information in the AFSJ

The development of an appropriate legal and institutional framework for parliamentary access to classified information is of fundamental importance to strengthening the EP's oversight of the AFSJ bodies. The discussion of the EP's access to classified information must take place alongside deliberations on the evolution of the EP's mandate to oversee the AFSJ bodies; indeed, we have argued throughout this study that an oversight body's information needs are inextricably linked to its mandate. Yet, regardless of which aspects of the AFSJ bodies' work the EP wishes to oversee and which institutional mechanism is chosen to carry out this oversight, access to relevant classified information will be crucial. This is because various aspects of the work of AFSJ bodies are classified and/or involve the processing or creation of classified information. This section will outline a number of options for improving the EP's access to classified information in the AFSJ; the modalities and mechanisms for granting the EP access will be discussed later in this chapter (see section 5.5). It should be noted that the following discussion relates to the access to classified information on an ongoing basis in the context of the EP's 'regular' oversight functions; this is without prejudice to the EP's access to information under its powers of inquiry, which may be used on an ad hoc basis to investigate alleged breaches of EU law (see chapter three).

In chapter three, we argued that the current framework for granting the EP access to classified information in the AFSJ field (and beyond) is inadequate: it is characterised by ad hoc mechanisms and uncertainty. There is no clear legal framework in place for the EP to access AFSJ-related information from the Council, Europol, Eurojust, Frontex or the EEAS. Instead, access to classified information by the EP tends to take place on an ad hoc basis and pursuant to exchanges of letters between the chair of the LIBE Committee and the General Secretariat of the Council.[508] Frequently, the LIBE Committee cannot be certain if and when it will be given access to documents it deems to be relevant to its functions – this is a very weak basis for oversight.

The EP has already made some important progress regarding its access to classified information. Notably, the 2010 Framework Agreement (Annex Two) between the EP and the Commission represents significant progress in terms of extending the EP's right to access classified information (including in the AFSJ field) from the Commission, as well as setting out detailed modalities for such access. However, the progress made with the Commission has not yet been matched by similar advances in codifying rules for parliamentary access to classified information from the AFSJ bodies or the Council.

As discussed in chapter three, parliamentary access to classified information is currently being discussed in the context of deliberations regarding the revision of Regulation 1049—legislation which is ostensibly about public access to information from EU entities. The EP's rapporteur on this matter, Michael Cashman, has opted to include provisions on parliamentary access to information in the broader draft legal framework for public access to EU documents.[509] This approach has several advantages. First, it is aimed at ensuring that there is a general framework for the EP's access to classified information from all EU

[508] Interview 22.
[509] Committee on Civil Liberties, Justice and Home Affairs 12 May 2010.

entities and across all policy domains. This may be preferable to a fragmented legal framework for parliamentary access to information based on inter-institutional agreements across different fields. The effects of this current framework are that the EP has access to classified information from, e.g., the Council, in some fields but not others and that different modalities apply to access classified information in different policy domains. Second, the inclusion of provisions on the EP's access to classified information as part of broader legislation on public access to information could help to ensure that these rules have the status of legislation rather than being enshrined in inter-institutional agreements, which are of a subordinate legal status.

In spite of these advantages, we are of the view that parliamentary access to classified information should be decoupled from provisions on public access to information. This is supported by practice on the national level, where freedom of/access to information laws are separated entirely from regulations on parliamentary access to information. Parliamentary access to classified information implies access to the specific categories of information which are justifiably exempt from public access, e.g., information regarding the work of intelligence agencies. It is precisely because such information is beyond the reach of public access that it must be available to certain parliamentarians and institutions established by parliaments for overseeing, inter alia, intelligence agencies. In almost every state analysed in this study, parliaments have privileged access to classified information to, inter alia, enable to them oversee intelligence activities. This is premised on the notion that parliamentarians are elected by a population to hold governments and their agencies to account. In order to do this, they require privileged access to information which is not necessarily available to members of the public. Therefore, rules governing parliamentary access to classified information are set out in law and are disconnected for general freedom of/access to information laws.

Recommendation 11: New regulations on the European Parliament's access to classified information should be decoupled from legislation on public access to information.

5.4.1.1. The legal basis for access to information by the European Parliament

The EP could pursue a number of options with regards to developing a new legal framework for parliamentary access to classified information in the AFSJ and beyond. First, provisions on parliamentary access to classified information could be integrated in the new regulations on Europol, Eurojust and Frontex. Such provisions would be developed alongside regulations on parliamentary oversight of these agencies, thus ensuring that the EP's access to classified information from and relating to each agency is clearly tied to its oversight mandate and functions with regards to each agency. It is important to note that these regulations would need to extend to the EP's access to classified information from the Council because the Council has 'ownership' of a significant amount of information relating to the AFSJ agencies.[510] This is the approach most commonly used at the national level, where provisions on overseers' access to classified information are often enshrined in legislation regulating intelligence agencies and their oversight. One notable drawback to this approach is that the EP will need improved access to classified information from and about all three AFSJ agencies; however, new legislation on each agency—and the EP's role in overseeing them—will not be dealt with at the same time. Consequently, there is a risk that the extent of the EP's access to classified information, as well as the mechanisms for such access, would not be uniform across the AFSJ. In addition, new legislation on these

[510] Interview 21.

agencies will not be adopted for several years, yet there is a need for improved parliamentary access to classified information in the short-term.

Second, the EP could attempt to negotiate a specific inter-institutional agreement with the Council covering the AFSJ. An agreement with the Council covering the AFSJ could help to ensure a uniform set of regulations on parliamentary access as well as one mechanism for such access (e.g., the special committee or sub-committee option mentioned in section 5.5). It is not clear, however, whether an agreement with the Council could extend to parliamentary access to information from the agencies themselves. There may therefore be a need for some form of agreement between the EP and each of these three agencies regarding parliamentary access to information. This would likely require some form of amendment to the existing legislation on each agency, which is unlikely to happen given that the legislative basis for all three agencies is due to change within the next three years.

Third, as noted above, the EP's access to classified information in all policy areas could be regulated by overarching legislation that also deals with public access to EU documents. Under the current proposals, the EP could request access to classified information through, inter alia, the chair of the committee with responsibility for a given subject, e.g., LIBE for the AFSJ. If granted, the information would be made available to a special committee composed of seven members appointed by the EP's Conference of Presidents. The membership of the committee could consist of a core—comprised, for instance, of the leaders of the political groups—but it would not be a committee with a fixed membership.[511] The merits of this particular institutional mechanism will be discussed in more detail below. However, for reasons stated above, regulations on the EP's access to classified information should not be included in legislation on public access to information.

Recommendation 12: New legislation on the AFSJ agencies (Europol, Eurojust and Frontex) should include provisions on the European Parliament's access to classified information from and pertaining to these agencies. Such provisions should be anchored to the EP's mandate to oversee these agencies, which will be outlined in the same legislation.

As discussed in chapter three, the legal framework regulating the EP's access to information relating to the fourth AFSJ body addressed in this study, Sitcen, needs to be dealt with separately. This is because—in spite of Sitcen performing some functions which are relevant to the AFSJ—it falls in a different policy domain (CFSP) in which the EP has fewer powers. Unlike the AFSJ agencies, it does not have its own legislative basis and there are no plans to 'Lisbonise' its legal basis. The EP's existing special committee for the CSFP field may be able to access information pertaining to Sitcen but has never made use of this opportunity.[512] The 2002 inter-institutional agreement between the Council and EP will probably need to be re-negotiated in view of the fact that the Lisbon Treaty has made profound changes to the CSFP field. For the purposes of this study, the most relevant change is that Sitcen is no longer exclusively a creature of the Council because it now falls under the EEAS structure. Chapter three noted that the High Representative envisages that, inter alia, the existing inter-institutional agreement between the Council and EP, which regulates the EP's access to classified information in the CFSP field, will continue to apply. However, the modalities of the EEAS are so different that it seems likely there will be a need for a new agreement on the EP and EEAS, which would include provisions on parliamentary access to classified information. Yet, in view of the inter-governmental character of Sitcen the Council may continue to be the gatekeeper to any parliamentary

[511] Interview 6.
[512] Interviews 17 and 21.

access to information regarding this body. Hence, the existing 2002 agreement between the EP and Council or an updated version thereof may continue to apply.

Recommendation 13: The European Parliament should consider negotiating an inter-institutional agreement with the European External Action Service, which would include provisions on parliamentary access to classified information.

5.4.1.2. The scope of the European Parliament's access to classified information from the AFSJ agencies

Rather than enumerating a specific list of the types of information the EP could have access to, it would be preferable for legislation to grant the EP a general right to request access to classified information which it deems to be relevant to its (new) oversight mandate and functions. In chapter four, we noted that this is a common good practice on the national level and helps to ensure that the responsibility for determining what information is relevant should, in the first instance, be the prerogative of the overseer. In the context of the EP's oversight of the AFSJ agencies, classified information would be requested by and made available to one of the institutional mechanisms outlined below (see section 5.5). Access to classified information on the basis of requests would, however, be subject to appropriate limitations such as those outlined in Annex Two of the 2010 Framework Agreement between the EP and the Commission.

Recommendation 14: Legislative provisions on the oversight of the AFSJ agencies by the European Parliament should include a general right for a designated body of Parliament to access classified information it deems to be relevant to its oversight mandate and functions.

While the EP needs a general right to request access to classified information relevant to its mandate to oversee the AFSJ agencies, access to relevant information may be better ensured by requirements for the agencies to make proactive disclosures of particular categories of information. Chapter four highlighted that proactive disclosure is a common practice on the national level and helps to ensure that oversight bodies have consistent and predictable access to information. This approach would be particularly advantageous in the context of the EP's oversight of AFSJ agencies because it would reduce the need for MEPs and staffers to expend time identifying and requesting relevant information. Perhaps more importantly, it would reduce the continuous inter-institutional battles that have characterised access to classified information by the EP. Again, the precise nature of proactive disclosure obligations would need to be tailored to the specific oversight mandate and functions outlined in forthcoming legislation. On the basis of what is advocated in this chapter, the following types of information could, for example, be subject to proactive disclosure:

- Annual work plans of the AFSJ agencies
- Threat assessments produced by the agencies
- Cooperation and information sharing agreements between the AFSJ agencies
- Cooperation and information sharing agreements between the AFSJ agencies and third states
- All information pertaining to budgeting and past expenditure

The proactive disclosure of these types of information is broadly in line with similar provisions which apply to proactive disclosures to oversight bodies on the national level (see chapter four).

Recommendation 15: New legislative provisions on the oversight of the AFSJ agencies by the European Parliament should enumerate specific categories of information, including classified information that must be proactively disclosed to a designated body of parliament.

5.4.2. The protection of information handled by the European Parliament

Improved access to classified information by the European Parliament will have to be accompanied by the concomitant development of rules and procedures pertaining to the protection of classified information handled by the EP. The failure to handle classified information in an appropriate manner may not only harm particular security interests but may also undermine the work of oversight bodies (see chapter four). Unauthorised disclosure of information by oversight bodies causes agencies to lose trust in them and may result in a withdrawal of cooperation, i.e., a failure to grant overseers access to information in future.

There will be a need to limit the number of MEPs who have access to classified information in AFSJ. In this chapter, we will recommend two main mechanisms through which access could be limited to relatively small groups of MEPs: special committees and a sub-committee. This takes account of the 'need to know' principle which was discussed in chapter four and is also enshrined in the 2010 Framework Agreement between the Commission and the EP; this means that MEPs are only given access to classified information if they have a demonstrable need to know the information in order to fulfil their functions, e.g., as a member of a particular committee.

In chapter four, we explained that there are three principal mechanisms used to ensure that members of oversight bodies do not disclose classified information without proper authorisation. The EP may wish to consider each of these. Firstly, measures need to be taken to ensure that appropriate persons are selected for positions in which they will have access to classified information. One very simple way of doing this, which can be applied within the EP, is by group leaders carefully selecting MEPs to be members of bodies with access to classified information. The EP could follow the practice used in some national parliaments whereby members of committees that have access to classified information are selected by their peers, thus ensuring cross-party support (see chapter four). There is however, no precedent for this at the EP.

Vetting and security clearance processes are also used by some oversight bodies. While EP staffers should certainly be subject to security clearance before being granted access to classified information, the situation for MEPs is more complex. Chapter four illustrated that in the majority of (but not all) EU states, MPs are not subject to vetting and security clearance processes. This divergence in national practices has posed a problem for the EP because security clearance processes (of MEPs) have to be conducted by national authorities and, in many EU states, parliamentarians cannot be subject to security clearance. For this reason, the 2010 Framework Agreement between the EP and Commission left some scope for divergent Member State practices by inserting the phrase '*appropriate* personal security clearance'.[513] In view of the sensitivities associated with security clearing parliamentarians, it would be advisable for the EU institutions to follow this approach in developing the legal framework for access to classified information by MEPs from other EU institutions and bodies. However, it should be stressed that security clearance can be seen as a confidence building measure which can make it easier for overseers to gain access to classified information.[514] In view of this, MEPs who are part of

[513] Interinstitutional Agreement of 20 November 2010 between the European Parliament and the European Commission, *Framework Agreement on relations between the European Parliament and the European* Commission, Annex II, Article 2.5.2.
[514] See Cameron in Annex A of this volume.

bodies that have access to classified information may wish to consider obtaining a security clearance, even when MPs in their state are not normally subject to security clearance.

Secondly, most states criminalise unauthorised disclosure of classified information by MPs and other overseers. At the EU level, penalties for unauthorised disclosure are complicated by the fact any prosecution of an MEP would have to take place under national law. The EP does, however, have its own disciplinary procedures which could be used in the event of an MEP making unauthorised disclosures of classified information. An assessment of the adequacy of these procedures is beyond the scope of this study. Indeed, more research is required on whether or not these procedures are effective, as well as on how national criminal law provisions would apply to unauthorised disclosures of classified information by MEPs or staffers. Ideally, there should be pan-EU consistency in this regard, in order to avoid the problem that MEPs are treated differently depending on their nationality.

Finally, physical protection measures and procedures play an important role in ensuring that classified information is not disclosed either accidentally or deliberately. An EP working group is currently drafting new security procedures which will enable the EP to handle classified information. This is taking place within the context of the implementation of Annex Two of the 2010 Framework Agreement between the EP and the Commission. While the development of these security procedures has been driven by an agreement that will facilitate the EP's access to classified information from the Commission, these procedures could be applied to information received from the Council, EEAS and AFSJ bodies. Given the highly technical nature of information protection procedures, the EP may benefit from discussions with national parliaments and non-parliamentary oversight bodies with experience in dealing with these matters.

It is important to note that these procedures alone will not be sufficient to persuade the AFSJ bodies, the Council, Commission and Member States that the European Parliament can be trusted with classified information. A relationship based on trust will need to gradually develop over time and will be greatly assisted by MEPs demonstrating that they will not disclose information without proper authorisation.

5.5. Oversight mechanisms

The foregoing sections of this chapter outlined recommendations on how the EP's oversight of AFSJ bodies could be strengthened, as well as the need for oversight to be founded upon both access to and the protection of information. In this final section, we will put forward different options regarding the mechanisms or bodies within parliament that could undertake the oversight functions discussed in this chapter. These are also the mechanisms through which the EP should be able to access classified information in the AFSJ.

As we noted in chapter three, the EP's LIBE Committee's mandate covers the AFSJ agencies and the Sitcen falls under the jurisdiction of the AFET Committee. These committees are analogous to the 'general parliamentary committees' which exist on the national level and were briefly discussed in chapter four. The EP does not, however, have the equivalent of the specialised oversight committees discussed in chapter four. The terms of reference for this study imply that some elements in the EP are considering the creation of such a committee. Accordingly, this section will consider the creation of a sub-committee which would serve as the EP's specialised body for the oversight of the AFSJ agencies. However, this is not the only mechanism which the EP could use to perform many of the oversight

functions envisaged in this chapter. We will also consider the option of giving these responsibilities to the LIBE committee, as well as using various 'special committee' options along the lines of the special committee which currently exists for the CFSP field. Lastly, we will discuss options for strengthening cooperation between the EP and national parliaments in the context of overseeing the AFSJ agencies.

Before embarking on a discussion of these various options, two general points should be stressed. First, it is preferable for the body that is given primary responsibility for the oversight of the AFSJ agencies to be the same body which has access to classified information in the AFSJ. Chapter four demonstrated that on the national level, specialised oversight committees are almost always one of the bodies (or the only body) in parliament that have access to classified information in the security domain (see Table 3). Having one mechanism for parliament to access information relating to AFSJ agencies and a separate body—without the same level of access to such information—for overseeing such bodies would seriously undermine oversight of these agencies. The reasons for this are self evident: bodies with a mandate to conduct oversight need access to relevant information, and bodies that have access to information relating to particular agencies but no clear mandate to oversee such agencies cannot make effective use of their privileged access to information.

Recommendation 16: The European Parliament body responsible for the oversight of the AFSJ agencies should also be the body of Parliament which has access to classified information in the Area of Freedom, Security and Justice.

Second, it is preferable for the EP to have one body (e.g., the LIBE Committee or a newly created sub-committee) that plays the lead role in the parliament's oversight of the AFSJ agencies. In order to ensure that the EP takes a coherent and coordinated approach to the oversight of the AFSJ agencies, there should be one body which has primary responsibility for all oversight functions vis-à-vis all AFSJ agencies. This responsibility should include not only the EP's own oversight mandate and functions but also cooperation with national parliaments and non-parliamentary oversight bodies such as the JSBs. An important exception to this is the financial oversight of the agencies which will, of course, remain the responsibility of the Budgets and Budgetary Control Committees. Nevertheless, whichever body has primary responsibility for the oversight of the AFSJ agencies should be closely involved in the work of the BUDG and CONT committees with respect to these agencies. It should be stressed that the 'body' discussed in this paragraph cannot be given primary responsibility for the oversight of Sitcen because it is situated in the Common Foreign and Security Policy field, under the High Representative. The practice of vesting all or most (parliamentary) oversight functions in one body was highlighted (in chapter four) as being a good practice on the national level—the German *Bundestag's* Parliamentary Control Panel is a useful example in this regard.[515]

Recommendation 17: The European Parliament should ensure that there is *one* body within parliament that has primary responsibility for the oversight of the Area of Freedom, Security and Justice (AFSJ) agencies.

[515] See also, in Annex A of this volume, Forcese.

5.5.1. The performance of additional oversight functions by the LIBE Committee

The EP's LIBE Committee is the committee which is currently responsible for overseeing the AFSJ agencies, and is a logical starting point when considering which body within the EP should assume the oversight mandate and functions outlined in this chapter. Vesting such responsibilities in the LIBE Committee would perhaps be the most straightforward solution because it would not require the creation of any new bodies or mechanisms. Moreover, the LIBE Committee in the current parliament includes some MEPs with considerable interest and expertise in various matters relating to the AFSJ agencies, and the Committee's secretariat houses the parliament's 'institutional memory' in this field. The Committee also has the advantage that it has developed relationships with its contemporaries in national parliaments, which are useful for inter-parliamentary cooperation in the oversight of AFSJ agencies.

There are, however, a number of reasons why the LIBE Committee is not well suited for many of the oversight functions we have discussed. By far the most significant problem—from which other difficulties arise—is that it is not an ideal forum for accessing and/or discussing classified or otherwise sensitive information. In common with most committees of the EP, the LIBE Committee is very large and consequently the agencies and the Council are reluctant to share or discuss classified information (particularly of higher levels of classification) with the full committee.[516] These concerns exist not only when LIBE meetings are public but also when they are held behind closed doors.[517] With so many MEPs involved, it is difficult to control the use of information and agencies are concerned that information discussed within the Committee may be further disseminated. Equally, LIBE Committee meetings are not seen as an ideal setting for open, frank exchanges about sensitive matters. Several persons interviewed for this study suggested that agency directors are very unlikely to make candid statements about failures of their agency or serious problems facing their agency in the context of a full committee meeting, regardless of whether or not it is held *in camera*.[518] Holding committee meetings *in camera* does not seem to be a sufficient measure to assuage the concerns which the AFSJ agencies and the Council may have about confidentiality.

A second reason for which the LIBE Committee may not be an ideal body for conducting the oversight functions outlined in this section is that it has a mandate to address a wide range of other important issues that it may not have time to engage in additional oversight of the AFSJ agencies. In chapter four, we explained that many national parliaments have opted to establish specialised oversight committees because committees with jurisdiction over broad policy areas such as justice and home affairs do not have the time or resources to engage in ongoing oversight of intelligence agencies. If the EP wishes to follow suit, the logical outcome would likely be the creation of a sub-committee of the LIBE (see below). Whether or not this is necessary will likely depend on the nature and scope of any extension of the EP's oversight of the AFSJ agencies. Ultimately, the LIBE Committee will need to determine whether or not it has sufficient time and resources to assume additional oversight functions.

[516] It is, for example, much larger than the vast majority of the specialised parliamentary oversight committees discussed in chapter four (see also Table 1).
[517] Full committee meetings may be attended by as many as 55 MEPs, numerous staffers, the media and members of the public. We were told that persons attending committee meetings may even include representatives of foreign embassies in Brussels. Interviews 16 and 17.
[518] Interviews 16 and 32.

The development of a new body or mechanism within the EP is likely to be a complex and protracted process requiring the agreement of numerous other actors. Depending on which type of mechanism the EP opts to establish, it may not be possible until new legislation on Europol and Eurojust is drafted and there is a legal framework in place which regulates the EP's access to classified information in the AFSJ area. In view of this, it is necessary for the LIBE Committee to develop procedures that make it better suited to serving as a forum for the oversight of AFSJ agencies, at least on an interim basis.

One relatively straightforward option is for the bureau of the LIBE Committee to hold off-the-record briefings with directors/president of the AFSJ agencies and/or representatives of the management board (in the case of Europol & Frontex) and the College (in the case of Eurojust). This option could be utilised to permit MEPs to discuss sensitive matters with these individuals in small, private meetings. Matters under discussion could include anything which falls within the broader mandate of the LIBE Committee. For example, directors could use such meetings to brief bureau members on sensitive strategic issues or problems in the operation of their agency. During the course of our interviews, it became clear that some MEPs and the directors of the agencies would welcome the opportunity for more confidential meetings when particularly sensitive matters need to be discussed.[519] Such meetings could be initiated at the request of the chair of the LIBE Committee, by directors/president of the AFSJ agencies, and/or by relevant figures from the management boards/college. While small, off-the-record meetings could be a useful option for ad hoc discussions on some issues, they would not serve as a mechanism for many of the oversight functions discussed above.

Recommendation 18: The European Parliament's LIBE Committee should develop procedures that make it better suited to serving as a forum for the oversight of AFSJ agencies, at least on an interim basis. For this purpose, the LIBE Committee could use off-the-record meetings between its Bureau and directors (or president in the case of Eurojust) of the AFSJ agencies and/or representatives from the agencies' management boards (or the College of Eurojust) to address sensitive issues which cannot be discussed in meetings of the full committee.

5.5.2. Special committee options for the Area of Freedom, Security and Justice (AFSJ)

In chapter three, we introduced the European Parliament's 'Special Committee'—a small group of MEPs drawn primarily from the AFET Committee—used to enable the parliament to address matters which involve classified information in the CFSP field (hereafter, the 'Common Foreign and Security Policy - CFSP Special Committee'). There are a number of options for extending this committee's remit or using a similar model for the oversight of the AFSJ bodies.

5.5.2.1. Extending the existing Special Committee's remit to the AFSJ

The EP's existing special committee established on the basis of an inter-institutional agreement between the EP and the Council for the exclusive purpose of enabling the EP to access classified information in the CFSP field (see chapter three) from the High Representative. The remit of this special committee could potentially be extended, through an amended inter-institutional agreement, to the AFSJ field in order to allow the EP to address matters involving classified information relating to, inter alia, the AFSJ agencies.

[519] Interviews 16 and 32.

The same MEPs could discuss AFSJ matters involving classified information with relevant persons from the Council and, potentially, the agencies' directors. Such meetings would take place upon the request of the chair of the LIBE Committee rather than the chair of the AFET who, under the current arrangements, can request meetings between the High Representative and the special committee. The main advantage of this approach is that there is already an arrangement in place and all of the MEPs on the existing special committee have now received their security clearances insofar as this is permissible under their states' national law and practice.[520] Accordingly, it would not be necessary to endure lengthy waits for selected members of the LIBE Committee to be security cleared. There are, however, several major drawbacks to this option; these will be discussed below.

5.5.2.2. The establishment of a special committee for the AFSJ

The EP and the Council could agree to create a special committee in the AFSJ along the lines of the CFSP special committee model. Accordingly, a small, ad hoc committee or grouping would be created, drawn primarily from the membership of the LIBE Committee. The special committee could include approximately six members (and substitutes) representing each political group, who would be security cleared by their national authorities insofar as this is permitted by national law.[521] If an AFSJ special committee followed the example of the existing CFSP Special Committee, the membership would be fixed, i.e., it would not change on an issue-by-issue basis. The membership selection process would need to be determined by the LIBE Committee but it seems likely that members would be nominated by their political groups on the basis of their seniority. However, it may be preferable to select LIBE members with expertise on the agencies whose work would be discussed by the committee. This could help to ensure that committee members would have the necessary knowledge to enable them to ask relevant questions and seek access to pertinent information. The special committee would need to be supported by security-cleared members of the LIBE secretariat.

A 'special committee' in the AFSJ could hold discussions with both the relevant authority within the Council and the director/president of the AFSJ agency concerned. The special committee's meetings could take place on a periodic basis or upon a request from the chair of the LIBE Committee to the relevant party. Members of the special committee would be given the right to request access to classified information in the form of briefings or by viewing particular documents. They would also be able to ask questions and receive answers to questions which could entail agency and Council officials revealing classified information, which they may not do in the context of hearings with the LIBE Committee. As is the case with the CFSP Special Committee, this arrangement would likely be used on an ad hoc basis to enable the LIBE Committee, through its special committee, to discuss matters that are considered to require the discussion of classified information. For example, members could be briefed on negotiations with third states, problems relating to information sharing with third states, or could discuss threat assessments pertaining to issues such as terrorism.

It is noteworthy that the EP's Rapporteur on the revision of Regulation 1049 has proposed a slight variation to the special committee option discussed here. Under his proposals, the EP would establish a 'special oversight committee composed of 7 members appointed by its

[520] Interview 17.
[521] This number is taken from the special committee in the CFSP field. Please refer to the above discussion on the debate about subjecting MEPs to security clearance processes.

Conference of Presidents' to access classified information across all policy areas.[522] We were informed that the Rapporteur foresees that this committee would have a flexible membership which could change depending on the issue under discussion.[523] This committee would presumably be able to discuss such information with relevant officials from the Council, Commission or agencies.

Both special committee options have a number of significant drawbacks. Several individuals with experience of the CFSP special committee counselled against exporting the model to other fields such as the AFSJ.[524] A first problem is that a special committee of this nature is ultimately only a vehicle for its parent committee, in this case the LIBE Committee, to have some access to classified information. Neither the existing special committee nor the proposed special committee for the AFSJ (as conceived of here) would have a specific oversight mandate. If it were to be given a specific mandate, it would make sense to pursue the option of a security cleared permanent sub-committee instead (see below). Moreover, given that a special committee would be a small group of MEP's without its own secretariat and meeting on an occasional basis, it is difficult to see how it could undertake the various oversight functions outlined in this chapter.

Secondly, there are doubts about whether a special committee could make effective use of the classified information to which it had access in the context of discussions with Council and/or agency officials. Given that the special committee would not have a specific mandate or the capacity to produce reports, it is unclear what purpose would be served by it having access to classified information. Indeed, as we pointed out in chapter four, access to classified information is not an end in itself; it should serve as a means to conduct oversight. In this context, information is of limited use unless it can serve as a basis for performing specific oversight functions. It is noteworthy that this was highlighted as one of the main weaknesses of the CFSP special committee.[525] Furthermore, members would obviously be prohibited from transmitting or referring to classified information in discussions with their colleagues in the LIBE Committee. This would make it difficult for the LIBE Committee to make use of the special committee's privileged access to classified information in its own work. For this reason, the use of a special committee in the AFSJ would be inconsistent with Recommendation 16 which stresses the need for the body responsible for oversight of the AFSJ agencies to be same body that has access to classified information relating to these agencies.

Thirdly, if members of a special committee for the AFSJ were not experts on the subjects and agencies being discussed, they may not have the relevant knowledge to ask the most relevant questions and/or seek access to relevant information. According to one respondent, this has been a major weakness of the CFSP special committee.[526] This eventuality seems likely if members were to be selected on the basis of their seniority within political groups. The risk of a special committee possessing insufficient specialised knowledge would be significantly increased if the EP and Council selected the option of extending the mandate of the existing CFSP special committee. This is because its members and staffers are primarily drawn from the AFET Committee and may not have specific knowledge or expertise relevant to the AFSJ.

[522] Committee on Civil Liberties, Justice and Home Affairs 12 May 2010, Amendment 33, Article 3a.
[523] Interview 6.
[524] Interviews 17 and 21.
[525] Interview 17.
[526] Interview 17.

Finally, a special committee arrangement for the AFSJ (and similar arrangements in other policy areas) would not obviate the need for a comprehensive legal framework on the EP's access to information in the AFSJ field and beyond.[527] There is a risk that by granting access to classified AFSJ information to a special committee of MEPs, the Council may attempt to bypass the need for a fundamental reconsideration of the framework for parliamentary access to information.

Recommendation 19: The European Parliament should not seek to extend the existing Special Committee's mandate to include the Area of Freedom, Security and Justice (AFSJ), or to create a new special committee for the AFSJ.

5.5.2.3. Oversight of the European Union's Situation Centre by the existing Common Foreign and Security Policy Special Committee

As we have already discussed, the EP's existing CFSP Special Committee may address CFSP matters, which include the discussion of classified information with the High Representative. Given that Sitcen falls under the purview of the High Representative, the CFSP Special Committee could use its meetings with her to address issues relating to Sitcen. Such discussions could be initiated by a request from the chair of the AFET Committee.[528] Members of the CFSP Special Committee could, for example, seek to learn more about the composition of Sitcen, its current priorities, or the role it plays in providing assessments on threats to the EU's internal security. There is, of course, no guarantee that the High Representative would be willing to discuss these issues given that Sitcen's work remains highly sensitive due to the presence of seconded officers from national intelligence agencies. To date, the special committee has not discussed the Sitcen with either the former High Representative (Javier Solana) or the current High Representative (Catherine Ashton).[529] This can probably be explained by the fact that the work of Sitcen has not been viewed as a priority for the AFET Committee.[530]

Once again, the use of a special committee has a number of significant drawbacks. First, giving a very select group of MEPs access to information on the work of Sitcen may do little to raise broader awareness of the role of Sitcen amongst MEPs and staffers. The potential for such discussions to contribute to broader awareness of Sitcen's role would also depend on how much of the information discussed in a special committee meeting on Sitcen is deemed to be classified. Second, the success of this option would depend on the willingness of the chair of the AFET Committee to take up the issue of Sitcen's internal security functions with the High Representative; this may be unlikely given that the AFET does not deal with internal security matters and has numerous other priorities to be addressed with the High Representative. In spite of these drawbacks, the CFSP special committee is currently the only mechanism available to the EP for discussions about the work of Sitcen. As we have consistently stated, the EP is in a weaker position vis-à-vis Sitcen than it is with regards to the AFSJ agencies for a variety of reasons: e.g., Sitcen is not an autonomous agency funded from the EU budget, the EP doesn't have powers of co-legislation in the CFSP, and it doesn't have a clear treaty-based mandate to directly oversee Sitcen. The CFSP Special Committee is therefore, the only mechanism through which the EP may be able to conduct some limited oversight of the Sitcen.

[527] Interviews 11 and 21.
[528] Interview 17 and 21.
[529] Interview 17. However, it should be noted that the previous director of the Situation Centre appeared on an ad hoc basis before the Sub-Committee on Defence. Interview 11.
[530] Interviews 1, 11, 17.

Recommendation 20: The European Parliament should use its existing Special Committee to examine the work of the European Union's Situation Centre. The Special Committee could use its privileged access to classified information to address the role played by the Situation Centre in the Area of Freedom, Security and Justice.

5.5.3. Creation of a LIBE Sub-Committee for the oversight of the AFSJ agencies

The EP could consider establishing a sub-committee of the LIBE Committee to oversee the AFSJ agencies. This would be a permanent body, established in accordance with the EP's Rules of Procedure. We shall first put forward some suggestions regarding the modalities of such a sub-committee before outlining the reasons for which we believe this may be an effective mechanism for developing the EP's oversight of the AFSJ agencies.

Mandate

The mandate of any sub-committee would need to remain within the broad parameters of the LIBE Committee's mandate, which states that 'the Committee on Civil Liberties, Justice and Home Affairs Committee is responsible for […] Europol, Eurojust, Cepol and other bodies and agencies in the same area'.[531] Within this context, the sub-committee would assume primary responsibility for the oversight of AFSJ agencies by the European Parliament. We envisage that the sub-committee's jurisdiction would extend to all of the AFSJ agencies which currently fall under the remit of the LIBE Committee. Under the current division of responsibilities in the EP, the sub-committee of the LIBE could not directly oversee the Sitcen because it is part of the EEAS, which falls under the jurisdiction of the AFET Committee. It could nevertheless cooperate closely with the AFET Committee, its Sub-Committee on Defence and the CFSP Special Committee on matters relating to the activities of the Sitcen which are relevant to the AFSJ.

The sub-committee could, for example, be given the task of performing the oversight functions mentioned in this chapter and any other functions which the EP deems to be relevant. If the functions and powers of the AFSJ agencies were to evolve, the sub-committee's mandate would be amended accordingly. On the basis of the oversight mandate and functions outlined earlier in this chapter, the sub-committee's mandate may include, but should not be limited to:

xi. Serving as the forum for periodic and ad hoc meetings with, inter alia, the directors/president of the AFSJ agencies; representatives of the management boards/college; relevant officials from the Commission and Council;
xii. Receiving and reviewing the annual work plans and reports of the AFSJ agencies;
xiii. Receiving threats assessments from the AFSJ agencies;
xiv. Relations with the Joint Supervisory Bodies and any other specialised non-parliamentary oversight bodies which are created to oversee the AFSJ agencies. This role would include reviewing the annual and thematic reports of the JSBs and maintaining regular dialogue with them;
xv. Drafting the LIBE Committee's own initiative and legislative reports on matters relating to the AFSJ agencies;
xvi. Performing the advisory functions of the LIBE Committee with regards to the appropriation and discharge of the budgets for the AFSJ agencies, thereby providing

[531] European Parliament March 2011b.

expert opinions to support the work of the Budgets and Budgetary Control Committees;

xvii. Cooperation with other committees of the European Parliament which have jurisdiction over matters related to the AFSJ agencies. Notably, the sub-committee could maintain dialogue with the AFET and the CFSP Special Committee regarding the Sitcen. If the EP decides to take up the option of drafting opinions on the human rights record of the AFSJ agencies' partners in third states, the sub-committee should consult with the AFET's Sub-Committee on Human Rights on this matter;

xviii. Reviewing certain aspects of the AFSJ agencies' cooperation with third states and international organisations, including scrutinising the information sharing agreements concluded in this context;

xix. Reviewing relationships between AFSJ agencies, including their memoranda of understanding; and

xx. Coordinating relations with national parliaments and representing the European Parliament in inter-parliamentary meetings which are relevant to the AFSJ.

In line with our earlier comments regarding the role of the EP in overseeing the AFSJ agencies, we do not believe that the sub-committee should duplicate the work of the JSBs in examining the legality of the use of personal data by certain AFSJ agencies. Moreover, it would not play a role in examining other operational activities of the agencies, e.g., their work files or the joint operations which they coordinate. Equally, the sub-committee should not encroach upon the jurisdiction of national parliaments and other oversight bodies responsible for scrutinising the work of national authorities that is connected to the AFSJ agencies.

Membership

The membership of the sub-committee would need to be determined in accordance with the guidelines established under Rules 186 and 190 of the European Parliament's Rules of Procedure. The existing sub-committees (of the Foreign Affairs Committee) on Security and Defence, and Human Rights have 28 members and 28 substitutes, and 30 members and 21 substitutes, respectively. These MEPs generally (but not necessarily) hold concurrent membership in the Foreign Affairs Committee.

It is our view that these numbers are too large considering the fact that two of the principal reasons for proposing a sub-committee are: (1) the need for a small, confidential forum for discussions with the heads of the agencies and management boards; and (2) the need for MEPs to have access to some classified information relating to the agencies. A committee with as many as 50 members and substitutes would not fulfil these needs. Indeed, many of the aforementioned concerns which the agencies (and the Council and Commission) have about the confidentiality of discussions and protection of classified information would not be addressed if the sub-committee contained so many MEPs. Aside from concerns about the protection of classified information, a sub-committee arrangement would need to create conditions in which, inter alia, agency directors would feel confident that they could raise concerns or sensitive issues with a group of MEPs, without the content of such deliberations being further disseminated. Ultimately, agency directors and officials from the Council, Commission and JSBs are likely to abstain from discussing sensitive issues with the EP if they are not confident that discussions will remain confidential.

On the national level, the overwhelming majority of specialised parliamentary oversight committees include five to fifteen MPs (see Table 1 in chapter four). As we have seen, such committees are normally smaller than other parliamentary committees for reasons of

maintaining confidentiality. Accordingly, it is our view that a sub-committee should contain no more than 15 MEPs (including substitutes). This may, however, be difficult to accomplish in view of the requirement that the composition of EP committees and sub-committees reflects the overall composition of the parliament.

It would be beneficial if members of the sub-committee were either full or substitute members of the LIBE Committee. This would increase the likelihood that sub-committee members would have sufficient knowledge of the AFSJ agencies to enable them to contribute effectively to the sub-committee's functions. Finally, the EP could consider including some MEPs that are members of other (sub)-committees that deal with matters related to the AFSJ agencies and/or have other expertise which is relevant to the oversight of AFSJ agencies. These MEPs could include members of the Budgetary Control Committee, the Foreign Affairs Committee and its Sub-Committee on Human Rights. Chapter four illustrated that there is precedence for the inclusion of *ex officio* members (of other parliamentary committees) in national parliamentary oversight committees. This can help to ensure that there is proper coordination between committees that deal with related matters.

Access to information

All members of the sub-committee and its staffers would have the right to access classified information within the parameters of the sub-committee's mandate. In addition, certain categories of information could be subject to proactive disclosure to the sub-committee by the agencies, their management boards/college and, where appropriate, the Council and Commission (see above). The sub-committee would not, however, need to have access to information held in the agencies' databases or any personal data. The sub-committee would be required to implement the measures to protect information, which were discussed earlier in this chapter.

Resources

The sub-committee would need to be supported by full-time security cleared staff. This is particularly essential in view of the fact that MEPs are frequently members of several committees and have to divide their time between work in their own states, Brussels and Strasbourg. Staffers are also essential to developing the parliament's institutional knowledge and expertise on the AFSJ agencies; they ensure that such knowledge is retained even when MEPs move to other committees or leave the EP.

Assessment

Whether or not the European Parliament needs to establish a LIBE sub-committee to oversee the work of the AFSJ agencies depends to a large extent on how its mandate to oversee these agencies is defined in the forthcoming legislation on Europol, Eurojust and Frontex. If the EP's oversight mandate and functions remain broadly similar to the way they are now, i.e., relatively limited, it is not clear that a sub-committee would be necessary. If, however, the EP assumes additional oversight functions along the lines of the options presented in this chapter, there is a strong case for the establishment of a sub-committee. There are four main reasons for which we believe a sub-committee could be created.

First, we have argued there is a need for the EP to have access to classified information from and pertaining to the AFSJ agencies, as well as the possibility of holding confidential,

off-the-record discussions with agency directors and other relevant stakeholders. Yet, the EP's existing institutional arrangements for oversight are not well suited to such functions because too many MEPs are involved and there is no precedent for smaller, confidential discussions with the agencies. We have cautioned against solving this problem by using a mechanism or body which simply has access to classified information regarding the AFSJ agencies without an accompanying mandate to use this information as part of oversight processes. It is worth reiterating that access to information by a body of parliament is not an end in itself: it must be a means to enable parliament to oversee particular agencies. For this reason, we were critical of the possible use of a special committee model for the AFSJ. The need to link access to classified information with a clear mandate for oversight is one of the main arguments in favour of creating a sub-committee.

A second argument in favour of the creation of a sub-committee is that the LIBE Committee might not have the time to engage in many of the proposed oversight functions outlined in this chapter. If the EP wishes to play an increased role in the oversight of the AFSJ agencies, the creation of a sub-committee could be a persuasive choice.

Third, a sub-committee would correspond with our earlier recommendation that the EP should have one body which has primary responsibility for all areas of parliamentary oversight of the AFSJ agencies. The sub-committee would be able to draw together its findings from various oversight functions and ongoing dialogue with the agencies, Council, Commission, JSBs and national parliaments. This would enable the EP to produce recommendations which can improve the work of the agencies, while also providing inputs to feed into other aspects of its own work. Notably, the insights of the sub-committee could help to ensure that the various roles which the EP plays vis-à-vis the AFSJ agencies are fully connected. For example, the EP's co-legislation functions would be closely informed by the findings and recommendations of its oversight work, and the sub-committee's oversight would also inform the use of the EP's budgetary powers.

Finally, the creation of a sub-committee would enable the EP to gradually develop more detailed knowledge and expertise on the AFSJ agencies. In our view, this is something which is currently lacking within the EP, and yet is crucial if the EP is to play a more active role in scrutinising the work of the AFSJ agencies.

Recommendation 21: The European Parliament should create a LIBE Sub-Committee for the oversight of the AFSJ agencies. The precise scope and content of the sub-committee's mandate would be defined in accordance with the Parliament's rules of procedure but would be closely tied to the oversight functions given to the EP by new legislation on Europol, Eurojust and Frontex.

5.5.4. Strengthening cooperation between the European Parliament and national parliaments in the oversight of AFSJ agencies

The Lisbon Treaty specifically requires that national parliaments should be involved in the oversight of Europol and Eurojust. While the precise nature and scope of national parliaments' role differs between states, this study highlighted three main ways in which national parliaments already exercise some oversight of these agencies (see chapter three). First, some national parliaments oversee the work of their own government's representatives at the Council and on agency management boards, i.e., they scrutinise national inputs to AFSJ agencies. Secondly, national parliaments can engage with AFSJ agencies directly by, for example, holding hearings with directors and other senior officials,

and producing reports on the agencies. This engagement has typically been aimed at generating awareness of the agencies' work rather than any direct review or scrutiny of the agencies' activities. Moreover, parliaments are part of national systems of oversight which scrutinise actions taken by national authorities such as the police. The modalities of such oversight are the prerogative of national bodies, and it is beyond the scope of this study to issue recommendations in this regard. The third dimension of national parliamentary involvement in the oversight of the AFSJ agencies is cooperation with other parliaments and the EP (see chapter three); this will be our focus here.

In our view, the aims of inter-parliamentary cooperation should primarily focus on strategic matters rather than any specific operations of the AFSJ agencies. There are three areas in which inter-parliamentary cooperation could be particularly useful. Firstly, national parliaments and the EP could benefit from further discussions, as well as exchanges of information, experiences and good practices, on their oversight of national authorities' activities that are connected with the AFSJ agencies. For example, there is a clear need for further information on how, if at all, national parliaments and other relevant national oversight bodies (such as judicial bodies) oversee: (a) national contributions or inputs to the AFSJ agencies, such as information sent to AFSJ agencies; and (b) the actions of national authorities taken on the basis of information provided and/or operations coordinated by these bodies, such as arrests and questioning of persons suspected of involvement in serious criminal activity. National overseers could use such information to inform their own approaches to scrutinising activities of, for example, the police or border agencies, which have a nexus with the AFSJ agencies. Secondly, national parliaments and the EP could, insofar as national law would allow, exchange information about particular problems (within their jurisdictions) related to aforementioned activities of national authorities' activities that are linked to the work of AFSJ agencies. Finally, national parliaments and the EP could work together to evaluate whether new and existing regulations relating to the AFSJ agencies comply with the principles of subsidiarity and proportionality.

There are different views as to whether this cooperation should be institutionalised through some form of permanent inter-parliamentary body or whether it should proceed more informally through existing inter-parliamentary fora. For example, in its communication of December 2010, the Commission made proposals for involving national parliaments in the oversight of Europol. The Commission proposed setting up a joint or permanent inter-parliamentary forum in which both national and European members of parliament would be represented, along the lines of Articles 9 and 10 of the Protocol on the Role of National Parliaments in the European Union. It furthermore suggested that such a forum could establish a sub-group to liaise directly with Europol. The forum would be able to invite the Europol director and it could meet regularly and establish a sub-group responsible for liaising with Europol directly.[532] The Commission's proposals have received some support from national parliaments.[533] However, the added value of the creation of such an inter-parliamentary forum has been questioned by a number of EU member states and national parliaments.[534] All of the forms of cooperation discussed above could potentially take place within the context of existing forums for inter-parliamentary dialogue.

[532] European Commission 17 December 2010, pp. 23 and 24.
[533] See for example, Italian Senate 14th Standing Committee on European Union Policies 2011; Hellenic Parliament 2011.
[534] See for instance, Council of the European Union, Outcome of proceedings of CATS on 10 & 11 February 2011, 6847/11. Brussels, 22 February 2011; House of Lords European Scrutiny Committee 2010-2011, p.58; and National Assembly of France 2011, Article 1.2.

Perhaps more significantly, it is highly doubtful that a permanent body including representatives from all national parliaments could be workable. National parliaments' positions on, levels of interest in, and knowledge of AFSJ related matters vary greatly across the EU. It would therefore, be very challenging to reach consensus on issues such as an agenda for oversight, let alone on more substantive questions. A forum which included so many actors with different agendas could be unworkable and yet, it would be difficult to devise a formula for a smaller forum because it would inappropriate to exclude any national parliaments. In addition national parliaments have both different levels of access to information – from national authorities – and access to different types of information on the AFSJ agencies. They may therefore, be starting from very different positions in terms of their awareness of particular matters.

In view of these challenges, we do not recommend the establishment of a permanent forum for inter-parliamentary cooperation on oversight of the AFSJ agencies. It would be preferable for national parliaments and the EP to address the AFSJ agencies in the context of existing inter-parliamentary forums. These include joint meetings/hearings between the LIBE Committee and relevant committees of national parliaments, as well as the COSAC. In fact, the AFSJ, the political monitoring of Europol and the evaluation of Eurojust's activities have become regular items on the COSAC agenda.[535] A majority of COSAC's members have supported the idea of COSAC debates on Europol and Eurojust to be preceded by a hearing of the directors of the respective agencies and experts.[536] A potential role for COSAC in the political monitoring of JHA agencies is founded on Article 10 of TFEU Protocol No 1 on the role of national parliaments. This article stipulates that COSAC should promote the exchange of information and best practices between national parliaments and the European Parliament, including their special committees, and may organise inter-parliamentary conferences on specific topics. COSAC could continue to provide a useful venue for the types of cooperation discussed above.

Recommendation 22: Inter-parliamentary cooperation on the oversight of the AFSJ agencies should take place within the context of existing forums for cooperation between the European Parliament and national parliaments. The European Parliament does not need to establish a new permanent inter-parliamentary body.

[535] COSAC 2010, p. 8.
[536] COSAC 2010b, p. 8.

5.6. Summary of recommendations

Recommendation 1: The European Parliament should ensure that any new arrangements for the oversight of the AFSJ bodies do not serve to dissuade member states from using these bodies as platforms for cooperation.

Recommendation 2: The European Parliament should not be part of the management boards of Europol or Frontex, or of the College of Eurojust.

Recommendation 3: The European Parliament's oversight of the AFSJ agencies should focus on their policies, administration and finance.

Recommendation 4: The European Parliament should ensure its budgetary appropriation and discharge functions are fully linked to other aspects of its oversight of AFSJ agencies.

Recommendation 5: The European Parliament should receive threat assessments from the AFSJ bodies. This would enable Parliament to better assess whether these bodies have the necessary legal mandate, powers and financial resources to address such threats.

Recommendation 6: The European Parliament should engage in regular dialogue with the Joint Supervisory Bodies (JSBs) of Europol and Eurojust, and should make use of the reports and expertise of the JSBs in its own oversight of the AFSJ agencies.

Recommendation 7: The European Parliament's power to summon the director of Europol and the chairperson of the Europol Management Board should be extended to the equivalent persons at Eurojust and Frontex.

Recommendation 8: The European Parliament should not be given a role in the appointment of the directors/president of the AFSJ bodies.

Recommendation 9: The European Parliament should ensure that either a (sub)committee of parliament or a specialised non-parliamentary body provides independent assessments of the general human rights records/compliance of agencies in third states with which the AFSJ bodies cooperate. Such assessments could take place before an information sharing or other cooperation agreement is signed with a third state, and during the implementation of these agreements.

Recommendation 10: The European Parliament should have access to information sharing agreements and other memoranda of understanding concluded between AFSJ bodies within the European Union, as well as between AFSJ bodies and third states or organisations.

Recommendation 11: New regulations on the European Parliament's access to classified information should be decoupled from legislation on public access to information.

Recommendation 12: New legislation on the AFSJ agencies (Europol, Eurojust and Frontex) should include provisions on the European Parliament's access to classified information from and pertaining to these agencies. Such provisions should be anchored to the EP's mandate to oversee these agencies, which will be outlined in the same legislation.

Recommendation 13: The European Parliament should consider negotiating an inter-institutional agreement with the European External Action Service, which would include provisions on parliamentary access to classified information.

Recommendation 14: Legislative provisions on the oversight of the AFSJ agencies by the European Parliament should include a general right for a designated body of Parliament to access classified information it deems to be relevant to its oversight mandate and functions.

Recommendation 15: New legislative provisions on the oversight of the AFSJ agencies by the European Parliament should enumerate specific categories of information, including classified information that must be proactively disclosed to a designated body of parliament.

Recommendation 16: The European Parliament body responsible for the oversight of the AFSJ agencies should also be the body of Parliament which has access to classified information in the Area of Freedom, Security and Justice.

Recommendation 17: The European Parliament should ensure that there is *one* body within parliament that has primary responsibility for the oversight of the Area of Freedom, Security and Justice (AFSJ) agencies.

Recommendation 18: The European Parliament's LIBE Committee should develop procedures that make it better suited to serving as a forum for the oversight of AFSJ agencies, at least on an interim basis. For this purpose, the LIBE Committee could use off-the-record meetings between its Bureau and directors (or president in the case of Eurojust) of the AFSJ agencies and/or representatives from the agencies' management boards (or the College of Eurojust) to address sensitive issues which cannot be discussed in meetings of the full committee.

Recommendation 19: The European Parliament should not seek to extend the existing Special Committee's mandate to include the Area of Freedom, Security and Justice (AFSJ), or to create a new special committee for the AFSJ.

Recommendation 20: The European Parliament should use its existing Special Committee to examine the work of the European Union's Situation Centre. The Special Committee could use its privileged access to classified information to address the role played by the Situation Centre in the Area of Freedom, Security and Justice.

Recommendation 21: The European Parliament should create a LIBE Sub-Committee for the oversight of the AFSJ agencies. The precise scope and content of the sub-committee's mandate would be defined in accordance with the Parliament's rules of procedure but would be closely tied to the oversight functions given to the EP by new legislation on Europol, Eurojust and Frontex.

Recommendation 22: Inter-parliamentary cooperation on the oversight of the AFSJ agencies should take place within the context of existing forums for cooperation between the European Parliament and national parliaments. The European Parliament does not need to establish a new permanent inter-parliamentary body.

REFERENCES

Australia (1 October 2001), *Intelligence Services Act 2001*, available at (http://www.comlaw.gov.au/Series/C2004A00928).

Australia (17 October 1986*), Inspector-General of Intelligence and Security Act 1986*, available at (http://www.comlaw.gov.au/Series/C2004A03342).

Belgian Standing Committee I (ed.) (2010), *Fusion Centres throughout Europe - All Source Threat Assessments in the Fight against Terrorism*, Antwerpen, Intersentia.

Belgium (18 July 1991), *Act Governing Review Of The Police And Intelligence Services And Of The Coordination Unit For Threat Assessment*, available at (http://www.comiteri.be/images/pdf/engels/w.toezicht%20-%20l.contrle%20-%20engelse%20versie.pdf).

von Boetticher Christian Ulrik (24 February 2004), 'Report on the proposal for a Council regulation establishing a European Agency for the Management of Operational Cooperation at the External Borders', A5-0093/2004.

von Boetticher Christian Ulrik and Maurizio Turco (7 April 2003), 'Recommendation to the Council on the future development of Europol', 2003/2070(INI), A5-0116/2003, available at (http://www.europarl.europa.eu/ sides/getDoc.do?type=REPORT&reference=A5-2003-0116&language=RO).

Born Hans and Aidan Wills (2011), 'International Responses to the Accountability Gap: European Inquiries into Illegal Transfers and Secret Detention' in Hans Born, Ian Leigh and Aidan Wills, eds., *International Intelligence Cooperation and Accountability,* Routledge, London, pp. 202–227.

Born Hans and Ian Leigh (2005), *Making Intelligence Accountable,* Storting Publishing House, Oslo.

Buzek Jerzy (11 March 2010), 'Relations between the European Parliament and the Council - International agreements', 7465/10, available at http://register.consilium.europa.eu/pdf/en/10/st07/st07465.en10.pdf

Cameron Iain (2000), *National Security and the European Convention on Human Rights,* Kluwer Law International, Cambridge.

Canada (1985), *Canadian Security Intelligence Service Act (CSIS Act)*, RSC 1985 c C-23, available at (http://www.laws-lois.justice.gc.ca/PDF/C-23.pdf).

Caparini Marina (2007), 'Controlling and Overseeing Intelligence Services' in Born Hans and Marina Caparini, eds., *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Ashgate Publishing Limited, Hampshire, pp. 3-24.

Charkaoui v Canada (Citizenship and Immigration), [2008] 2 SCR 326, 2008 SCC 38.

Commission of the European Communities (11 December 2002), 'COMMUNICATION FROM THE COMMISSION: The operating framework for the European Regulatory Agencies', COM(2002) 718 final, available at (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0718:FIN:EN:PDF).

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (2006), 'A new review mechanism for the RMCP's national security activities', Ottawa, Gilmore Print Group.

Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (1981), *Second Report: Freedom and Security under the Law*, Ottawa.

Committee on Budgets (9 March 2010), 'REPORT on the guidelines for the 2011 budget procedure', Rapporteur: Helga Trüpel, A7-9999/2010, available at (http://www.europarl.europa.eu/document/activities/cont/201003/20100311ATT70460/20100311ATT70460ET.pdf).

Committee on Civil Liberties, Justice and Home Affairs (12 May 2010), 'DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (recast)', COM(2008)0229 – C6-0184/2008 – 2008/0090(COD).

Conference of the Speakers of the Parliaments of the EU (2011), *Presidency Conclusions,* Brussels, 4–5 April 2011.

Corbett Richard, Jacobs Francis and Michael Shackleton (2005), *The European Parliament*, Sixth Edition, John Harper Publishing.

'Corrigendum to the Decision of the European Parliament, the Council and the Commission of 6 March 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry', *Official Journal* L 113, 19/05/1995.

COSAC (2010), *Thirteenth bi-annual report: Developments in the European Union – procedures and practices relevant to parliamentary scrutiny,* XLIII Conference of Community and European Affairs Committees of Parliaments of the European Union, Madrid, 31 May–1 June 2010.

COSAC (2010b), *Fourteenth Bi-annual Report: Developments in European Union Procedures and Practices Relevant to Parliamentary Scrutiny*, Brussels, 25–26 October 2010.

Council Act of the Joint Supervisory Body of Eurojust of 23 June 2009 laying down its rules of procedure (2010/C 182/03).

Council Act of the Joint supervisory Body of Europol of 22 June 2009 laying down its rules of procedure (2010/C45/02), n° 29/2009.

Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU).

Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ L 121 of 15.5.2009.

Council Decision of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. 2009/426/JHA, OJ L138/14, 4.6.2009.

Council Decision of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, 2003/659/JHA, OJ L 245/44, 29.9.2003.

Council Decision of 17 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention), 2000/641/JHA, OJ L 271/1, 24.10.2000, available at (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000: 271:0001:0003:EN:PDF).

Council Doc. 9387/11, 'Joint Eurojust-Europol paper on judicial-police co-operation in operational cases' (not public).

Council of the European Union (25 March 2011), 'Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)', Doc 7961/11.

Council of the European Union (22 February 2011), 'Outcome of proceedings of CATS on 10 & 11 February 2011', 6847/11.

Council of the European Union (25 January 2011), 'Draft Scorecard – Implementation of the JHA Agencies Report', available at (http://www. statewatch.org/news/2011/feb/eu-council-cosi-jha-agencies-scorecard-5676-11.pdf).

Council of the European Union (15 May 2009), 'COUNCIL REGULATION (EC) No 371/2009 of 27 November 2008 amending Regulation (Euratom, ECSC, EEC) No 549/69 determining the categories of officials and other servants of the European Communities to whom the provisions of Article 12, the second paragraph of Article 13 and Article 14 of the Protocol on the Privileges and Immunities of the Communities apply', OJ L121/1.

Council of the European Union (15 February 2008), 'Conclusions from the Expert Meeting on the Follow-up of the Joint Frontex Europol Report on the High Risk Routes of Illegal Migration in the Western Balkan Countries within the Frontex Risk Analysis Network', available at (http://register.consilium.europa. eu/pdf/en/08/st05/st05685.en08.pdf).

Council of the European Union (13 December 2004), 'The Hague Programme: strengthening freedom, security and justice in the European Union', Council doc 16054/04 JAI 559.

Council of the European Union (28 February 2002), *Consolidated Eurojust Decision*, available at (http://www.eurojust.europa.eu/official documents/ Eurojust Decision/2009/consolidated/EJDecision-consolidated-2009-EN.pdf).

Council of the European Union (26 July 1995), *Council Act of 26 July 1995 drawing up the Convention on the protection of the European Communities' financial interests*, OJ C 316 , 27/11/1995 P. 0048-0048.

Council Regulation of 26 October 2004 establishing a European Agency for the Management of Operations Cooperation at the External Borders of the Member States of the European Union ('Frontex Regulation'), No 2007/2004, available at (http://www.statewatch.org/news/2011/mar/eu-council-summary-of-positions-on-frontex-regulation-7961-11.pdf).

COWI (January 2009), *External evaluation of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union: Final Report*, P-69209-A, available at (http://www.frontex.europa.eu/download/Z2Z4L2Zyb250ZXgvZW4vZGVmYXVsdF9vcGlzeS82Mi8xLzE/cowi_report_final.doc).

Croatia (30 June 2006), *Act on the Security Intelligence System*, available at (https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf).

Cumming Alfred (6 April 2011), 'Sensitive Covert Action Notifications: Oversight Options for Congress', Congressional Research Service, Washington DC.

Cumming Alfred (March 2011), '"Gang of Four" Congressional Intelligence Notifications', Congressional Research Service, Washington DC.

Danish Security and Intelligence Service (2007), 'Wamberg Committee's Mandate 1964' in *Annual Report 2006–07,* Copenhagen.
Danish Security and Intelligence Service (2007), *Annual Report 2006–07,* Copenhagen.

De Mera Agustin Diaz (15 November 2007), 'Report on the proposal for a Council decision establishing the European Police Office', A6-0447/2007.

Ellerman J. (2002), 'Von Sammler zum Jäger: Europol auf dem Weg zu einem "europäischen FBI"', *Zeus: Zeitschrift für Europarechtliche Studien* Vol. 4, pp. 561–585.

EU Institute for Security Studies (Summer 2010), 'Crisis response to the Haiti earthquake – an EU Sitcen perspective', *CSDP Newsletter*, Issue 10.

EU Observer (28 February 2011), 'MEP: Swift "secrecy" may hamper new data deals with US'.

Eurojust, Eurojust Work Programme 2011.

Eurojust, Eurojust Work Programme 2010.

Eurojust-Europol Joint Press Release (8 February 2011), 'Large international operation against illegal immigrant smuggling networks', available at (http://www.eurojust.europa.eu/press_releases/2011/08-02-2011.htm).

European Commission (21 March 2011), 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC) No 1049/2001 regarding

public access to European Parliament, Council and Commission documents', COM (2011) 137 final.

European Commission (17 December 2010), 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the procedures for the scrutiny of Europol's activities by the European Parliament, together with national Parliaments', COM(2010) 776 final, available at (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0776:FIN: EN:PDF).

European Commission (20 April 2010), 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Delivering an area of freedom, security and justice for Europe's citizens: Action Plan Implementing the Stockholm Programme', COM (2010) 171, available at (http://eur-lex.europa. eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF).

European Commission (30 April 2008), 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL regarding public access to European Parliament, Council and Commission documents', COM (2008) 229 final.

European Commission (20 December 2006), 'Proposal for a Council Decision establishing the European Police Office (EUROPOL)', COM (2006) 817 final.

European Commission for Democracy Through Law (2007), 'Report on the Democratic Oversight of the Security Services', adopted by the Venice Commission at its 71st plenary meeting, Venice, 1–2 June 2007.

European Court of Human Rights (June 2006), *Weber & Saravia v Germany*, Decision on Admissibility, Application no. 54934/00.

European Parliament (March 2011), 'Rules of Procedure of the European Parliament, ANNEX IX: Detailed provisions governing the exercise of the European Parliament's right of inquiry', available at (http://www.europarl.europa.eu/sides/getLastRules.do?language=EN&reference=ANN-09).

European Parliament (March 2011b), 'Rules of Procedure of the European Parliament, ANNEX VII: Powers and responsibilities of standing committees', available at (http://www.europarl.europa.eu/sides/getLastRules.do?language= EN&reference=ANN-07).

European Parliament (24 March 2011), 'Answer given by High Representative/Vice President Ashton on behalf of the Commission', E-010368/2010, available at (http://www.europarl.europa.eu/sides/ getAllAnswers.do?reference=E-2010-010368&language=EN).

European Parliament (17 November 2010), 'Answer given by High Representative/Vice-President Ashton on behalf of the Commission, available at (http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-8273&language=EN).

European Parliament decision of 20 October 2010 on the revision of the framework agreement on relations between the European Parliament and the European Commission, 2010/2118(ACI), available at (http://www.europarl. europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0366+0+DOC+XML+V0//EN&language=EN#BKMD-1).

European Parliament (3 May 2010), 'Reply to parliamentary question E-1131/2010', available at (http://www.europarl.europa.eu/sides/getAllAnswers. do?reference=E-2010-1131&language=EN).

European Parliament (16 November 2009), 'Report on the draft Council decision determining the list of third States and organisations with which Europol shall conclude agreements', Doc. A7-0069/2009, 11946/2009–C7-0107/2009–2009/0809 (CNS).

European Parliament (4 April 2007), 'REPORT on the annual report from the Council to the European Parliament on the main aspects and basic choices of CFSP, including the financial implications for the general budget of the European Communities (point H, paragraph 40, of the Interinstitutional Agreement of 6 May 1999) - 2005', A6-0130/2007, available at (http://www.europarl. europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2007-0130&language= EN).

European Parliament (30 January 2007), 'Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners', A6-0020/2007.

European Parliament (7 September 2006), 'Meeting Document: "What Future for Europol? Increasing Europol's Accountability and Improving Europol's Operational Capacity"'.

European Parliament (11 July 2001), 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)', A5-0264/2001.

European Parliament (1999), 'Tampere European Council 15 and 16 October 1999, Presidency Conclusions'.

European Parliament (14 March 1996), 'Resolution on Europol', A4-0061/1996.

European Parliament Committee on Budgetary Control (7 February 2011), 'Draft Report on the 2009 discharge: performance, financial management and control of EU agencies', Rapporteur: Georgios Stavrakakis (S-D), available at (http://www.europarl.europa.eu/document/activities/cont/201102/20110221ATT14018/20110221ATT14018EN.pdf).

European Parliament Directorate General Internal Policies (2010), 'Annex IV: Specification of the services to be provided under the service contract IP/C/LIBE/IC/2010-081'.

European Parliament LIBE Committee (2011), 'DRAFT REPORT on organised crime in the European Union', 2010/2309(INI), Rapporteur Sonia Alfano, 29.3.2011.

European Parliament LIBE Committee (16 March 2011), 'SWIFT implementation report: MEPs raise serious data protection concerns', available at (http://www.europarl.europa.eu/en/pressroom/content/20110314IPR15463/html/SWIFT-implementation-report-MEPs-raise-serious-data-protection-concerns).

European Parliament LIBE Committee (14 February 2011), 'WORKING DOCUMENT on the European Union's internal security strategy', Rapporteur Rita Borsellino, PE458.598v01-00, available at (http://www.europarl.europa.eu/RegData/commissions/libe/document_travail/2011/458598/LIBE_DT%282011%29458598_EN.pdf).

European Parliament LIBE Committee (11 April 2011), 'Minutes of the meeting of 11 April 2011', LIBE_PV(2011)0411_1, available at (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-464.719+01+DOC+PDF+V0//EN&language=BG).

European Parliament LIBE Committee (2010), 'Interparliamentary committee meeting on the democratic accountability in the area of freedom, security and justice: evaluating Europol, Eurojust, Frontex and Schengen', with the participation of national parliaments, Brussels, 4–5 October 2010.

European Parliament LIBE Committee (7 July 2008), 'Report on the initiative of the Kingdom of Belgium, the Czech Republic, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Poland, the Portuguese Republic, the Republic of Slovenia, the Slovak Republic and the Kingdom of Sweden with a view to adopting a Council Decision on the strengthening of Eurojust and amending Decision 2002/187/JHA', Rapporteur Renate Weber, available at (http://www.europarl.europa.eu/sides/getDoc.do?language=EN&reference=A6-0293/2008).

European Union and the United States of America (27 July 2010), 'AGREEMENT between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program', O.J. L. 195/5.

Europol (2011), 'Final Budget and Staff Establishment Plan 2011', available at (http://www.europol.europa.eu/publications/Budget/Budget_2011.pdf).

Europol (20 May 2011), 'General Report on Europol's Activities 2010', available at (http://register.consilium.europa.eu/pdf/en/11/st10/st10244.en11.pdf).

Europol (8 April 2011), 'Europol Activities in Relation to the TFTP Agreement Information: Note to the European Parliament, 1 August 2010–1 April 2011'.

Europol (28 March 2008), 'Strategic co-operation agreement between the European Agency for the management of operational cooperation at the external borders of the member states of the European Union and the European Police Office', available at (http://www.europol.europa.eu/legal/agreements/Agreements/Strategic%20cooperation%20agreement%20Frontex.pdf).

Fägersten B. (2010), 'Bureaucratic Resistance to International Intelligence Cooperation - The Case of Europol', *Intelligence and National Security*, Vol. 25, Issue 4, pp. 500-520.

France (9 October 2007), *Loi n°2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement*.

France (9 October 2007), *Ordonnance n°58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires*, Article 6 nonies, Créé par Loi n°2007-1443 du 9 octobre 2007.

Frontex (2011), 'Budget 2011', available at (http://www.frontex.europa.eu/gfx/frontex/files/budget/budgets/budget_2011.pdf/).

Frontex (2009), 'External evaluation of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union - Final Report 2009', available at (http://www.frontex.europa.eu/download/Z2Z4L2Zyb250ZXgvZW4vZGVmYXVsdF9vcGlzeS82Mi8xLzE/cowi_report_final.doc).

Frontex (25 June 2009), 'Management Board Decision no. 22/2009 of 25 June 2009 laying down rules on the secondment of national experts (SNE) to Frontex'.

Germany (2009), *Parliamentary Control Panel Act* (PKGrG), as revised on 29 July 2009, *Federal Law Gazette I*, p. 2346.

Germany (1990), *Federal Act on Protection of the Constitution (BVerfSchG)*, Act of 20 December 1990, *Federal Law Gazette I*, p. 2954, 2970, last amended by Article 1a of the Act of 31 July 2009 (*Federal Law Gazette I*, p. 2499, 2502).

Gill Peter and Mark Phythian (2006), *Intelligence in an Insecure World,* Polity Press, Cambridge.

Hayes B (2002), *The activities and development of Europol: towards an unaccountable 'FBI' in Europe*, Statewatch, London.

Hellenic Parliament (2011). 'Minutes of the Joint Meeting of the Special Standing Committee for Foreign Affairs and the Standing Committee for Public Administration, Public Order and Justice.' 3 February 2011.

House of Lords (21 January 2009), 'Examination of Witnesses (Questions 92–99)', Q95, available at (http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/43/09012106.htm).

House of Lords (21 January 2009b), 'Examination of Witnesses (Questions 120–122)', Q120, available at (http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/43/09012108.htm).

House of Lords (21 January 2009c), 'Examination of Witnesses (Questions 100-119)', available at (http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/43/09012107.htm).

House of Lords European Union Select Committee (2008), 'Europol: coordinating the fight against serious and organised crime', 29th Report of Session 2007–08.

House of Lords European Union Select Committee (5 March 2008), 'FRONTEX: the EU external borders agency', HL Paper 60, 9th Report of Session 2007–08, available at (http://www.publications.parliament.uk/pa/ld200708/ldselect/ ldeucom/60/60.pdf).

House of Lords Select Committee on European Union Home Affairs (Sub-Committee F) (6 December 2010), *Inquiry on the EU internal security strategy*.

House of Lords European Scrutiny Committee (2010-2011), 'National parliaments' scrutiny of Europol', 18th Report of Session 2010-2011.

Hungary (1995), Act No. CXXV of 1995, available at (http://www.fas.org/irp/world/hungary/1995law.pdf).

Hustinx P. (11 April 2005), Speech at farewell of data protection commissioner of Sachsen-Anhalt, Magdeburg, available at (http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2005/05-04-11_Magdeburg_EN.pdf).

Interinstitutional Agreement of 20 November 2010 between the European Parliament and the European Commission, *Framework Agreement on relations between the European Parliament and the European Commission*, OJ L304/47, available at (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:304:0047:0062:EN:PDF).

Interinstitutional Agreement of 20 November 2002 between the European Parliament and the Council concerning access by the European Parliament to sensitive information of the Council in the field of security and defence policy, 2002/C 298/01, OJ C 298/1.

International Commission of Jurists, Eminent Jurists Panel (2009), *Assessing Damage Urging Action,* ICJ, Geneva.

Italian Senate 14th Standing Committee on European Union Policies (2011), 'Resolution on the communication from the Commission to the European Parliament and Council on the procedures for the scrutiny of Europol's activities by the European Parliament, together with national parliaments.' 30 March 2011.

Italy (3 August 2007), *Law 14/2007*.

Justice (September 2002), 'Written evidence to the House of Lords EU Select Committee, sub-committee F, on the Danish Proposal for Amendments to the Europol Convention'.

Kamer Tweede (17 February 2011), *Motie Van Nieuwenhuizen/Cörüz over inzetten van alle middelen voor Frontex.*

Krieger Wolfgang (2009), 'Oversight of Intelligence: A Comparative Approach' in Gregory F. Treverton and Wilhelm Agrell, eds., *National Intelligence Systems: Current Research and Future Prospects*, Cambridge University Press, Cambridge.

Kvistholm Per (21 April 2009), 'The role of Frontex in Return Operations Sector', Euromed Working Group Nuremberg, 21st of April 2009, available at (http://www.euromed-migration.eu/e1152/e1537/e2138/e2279/e1258/e1366/ENpresentationfrontexwg3s32022042009_eng.pdf).

Labayle H. (2009), 'Principles and procedures for dealing with European Union classified information in the light of the Lisbon Treaty', Study for the European Parliament's LIBE Committee, European Parliament.

Lords Hansard, 25 Jun 2009: Column 1756, available at http://www.publications.parliament.uk/pa/ld200809/ldhansrd/text/90625-0013.htm#090625490007.

Lund Commission (1996), 'Report to the Storting from the commission which was appointed in order to investigate allegations of illegal surveillance of Norwegian citizens', Oslo.

Management Board of Europol (29 March 2007), 'Decision of The Management Board of 20 March 2007 laying down the rules governing the arrangements regulating the administrative implementation of the participation of Europol officials in Joint investigation Teams', 2007/C 72/16, available at (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:072:0035:0036:EN:PDF).

Milligan Susan (6 August 2006), 'Classified Intelligence Bills Often are Unread; Secret Process can Discourage House Debate', *Boston Globe*.

Mitsilegas, V. (2009), *EU Criminal Law*, Oxford, Hart Publishing.

National Assembly of France (2011), 'Motion for a European Resolution on Parliamentary Scrutiny of Europol.' 9 March 2011.

National Commission on Terrorist Attacks Upon the United States (2004), *The 911 Commission Report*, Washington DC, available at (http://www.gpoaccess.gov/911/pdf/fullreport.pdf).

Netherlands Review Committee on the Intelligence and Security Services (2009), 'Review Report on the Cooperation of GISS with Foreign Intelligence and/or Security Services', CTIVD No 22A, The Hague.

Netherlands Review Committee on the Intelligence and Security Services (2006), 'Supervisory Report on the investigation by the Supervisory Committee into the official messages issued by the AIVD in the period from January 2004–October 2005', CTIVD, The Hague.

The Netherlands (1994), *Rules of Procedure of the Dutch Second Chamber 1994*.

OECD DAC Guidelines and Reference Series (2005), 'Security System Reform and Governance', OECD, Paris.

Parliamentary Assembly of the Council of Europe (2005), 'Democratic oversight of the security sector in member states', Resolution 1713(2005).

Regulation (EC) No 863/2007 of the European Parliament and of the Council of 11 July 2007 establishing a mechanism for the creation of Rapid Border Intervention Teams and amending Council Regulation (EC) No 2007/2004. ('Rabit Regulation'), available at (http://www.frontex.europa.eu/gfx/frontex/files/rabit_regulation-863-2007.pdf).

Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105/1, 13.4.2006.

Rettman Andrew (12 April 2011), 'EU Intelligence bureau sent officers to Libya', *EU Observer*, available at (http://euobserver.com/9/32161?print=1).

Rettman Andrew (14 September 2010), 'Competition heating up for EU intelligence chief job', *EU Observer*, available at (http://euobserver.com/9/ 30794).

Roberts Alasdair (2006), *Blacked Out: Government Secrecy in an Information Age,* CUP, Cambridge.

Roberts Alasdair (2004), 'ORCON Creep: Information Sharing and the Threat to Government Accountability', *Government Information Quarterly* Vol. 21, No 3, p. 263.

Sánchez Javier Moreno (11 November 2008), 'Report on the evaluation and future development of the FRONTEX Agency and of the European Border Surveillance System (EUROSUR)', 2008/2157(INI), A6-0437/2008, available at (http://www.europarl.europa.eu/sides/getDoc.do?language=EN&reference=A6-0437/2008).

Shapcott William (2007), 'Taking EU intelligence into the 21st century' in A .Ricci and Eero Kytoèmaa, eds., *Faster and more united*? *The debate about Europe's crisis response capacity*, Office for Official Publications of the European Communities, Brussels.

South African Ministerial Review Commission on Intelligence (2008), *Intelligence in a Constitutional Democracy,* Pretoria.

South African Truth and Reconciliation Commission, *Report*, Vol. 5, Chap. 8.

Spain (6 May 2002), *Ley 11/2002, Reguladora del Centro Nacional de Inteligencia*.

Peers Steve (2002), 'The exchange of personal data between Europol and the USA', available at (http://www.statewatch.org/news/2002/nov/analy15.pdf).

Statewatch (20 December 2002), 'EU-USA Proposed exchange of personal data between Europol and USA evades EU data protection rights and protections', available at (http://www.statewatch.org/news/2002/nov/12eurousa.htm).

Sweden (22 November 2007), Act on Supervision of Certain Crime Fighting Activities, SFS 2007:980.

Treaty of Nice (10.3.2001), OJ C 80/1, available at (http://eur-lex.europa.eu/en/treaties/dat/12001C/pdf/12001C_EN.pdf).

United Kingdom (1994), Intelligence Services Act 1994, available at (http://www.legislation.gov.uk/ukpga/1994/13/contents).

United Nations Human Rights Council (17 May 2010), 'UN compilation of good practice on the legal and institutional framework for intelligence agencies and their oversight', A/HRC/14/46, available at (http://www.fas.org/irp/eprint/unhrc. pdf).

United States (1947), *National Security Act of 1947*, PL 235 - 61 Stat. 496; U.S.C. 402

United States Code, *Title 50–War and National Defense*.

United States Senate (1976), 'Intelligence activities and the rights of Americans, Book II, Final report of the select committee to study governmental operations with respect to intelligence'., U.S Government Printing Office, Washington DC.

Whitaker Reg and Stuart Farson (2009), 'Accountability in and for National Security', *IRPP Choices*, Vol. 15, No 9.

Williams Kieran and Dennis Deletant (2001), *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia and Romania*, Palgrave MacMillan, London.

Wills Aidan (2010), *Understanding Intelligence Oversight*, DCAF, Geneva.

Wills Aidan (2010b), 'European Parliament and Parliamentary Assembly of the Council of Europe inquiries into intelligence and security issues' in Stuart Farson and Mark Phytian, eds., Commissions of Inquiry and National Security, Praeger, Santa Barbara.

Wills Aidan and Hans Born (2011), 'International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions' in Hans Born, Ian Leigh and Aidan Wills, eds., *International Intelligence Cooperation and Accountability*, Routledge, London.

Wright, Andrea (2011), '"Fit for purpose": Accountability challenges and paradoxes of domestic inquiries' in Hans Born, Ian Leigh and Aidan Wills, eds., *International Intelligence Cooperation and Accountability,* Routledge, London.

ANNEXES

ANNEX A:

COUNTRY CASE STUDIES ON PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN EU MEMBER STATES AND OTHER MAJOR DEMOCRACIES

ANNEX B:

THEMATIC STUDIES ON OVERSIGHT OF THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE (AFSJ) BODIES

ANNEX C:

QUESTIONNAIRE FOR OVERSIGHT INSTITUTIONS OF CIVILIAN SECURITY AND INTELLIGENCE AGENCIES IN EU MEMBER STATES

ANNEX D:

MEMBERS OF THE PROJECT ADVISORY BOARD

ANNEX E:

AUTHORS OF THE ANNEXED BACKGROUND STUDIES

ANNEX A: COUNTRY CASE STUDIES ON PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN EU MEMBER STATES AND OTHER MAJOR DEMOCRACIES[537]

EU MEMBER STATES

I. **Belgium** by Wauter Van Laethem

II. **France** by Charlotte Lepri

III. **Germany** by Hans De With & Erhard Kathmann

IV. **Hungary** by Gábor Földváry

V. **Italy** by Federico Fabbrini & Tommaso F. Giupponi

VI. **The Netherlands** by Nick Verhoeven

VII. **Spain** by Susana Sanchez Ferro

VIII. **Sweden** by Iain Cameron

IX. **United Kingdom** by Ian Leigh

OTHER MAJOR DEMOCRACIES

X. **Australia** by Nicola McGarrity

XI. **Canada** by Craig Forcese

XII. **United States** by Kate Martin

[537] The opinions expressed in the annexed studies are the responsibility of their respective authors, and do not necessarily reflect the views of the Geneva Centre for the Democratic Control of Armed Forces, or the European University Institute.

ANNEX A: COUNTRY CASE STUDIES

I. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN BELGIUM

WAUTER VAN LAETHEM[538]

1. INTRODUCTION

In 1991, exactly twenty years ago, the Belgian legislature created an independent body to permanently review the functioning of the intelligence and security services[539]: the Standing Intelligence Agencies Review Committee, also known as Standing Committee I. With the passing years, Standing Committee I was entrusted with various additional assignments with regard to more specific aspects of the functioning of the intelligence services.

In the present contribution, we detail the initial review assignment of the Committee, together with the role of the Belgian Parliament and its specific Monitoring Commissions. However, the Belgian external oversight landscape is far richer. There are numerous other external institutions that can (directly or indirectly) supervise (specific aspects) of the functioning of the Belgian intelligence community:

- The Appeal Body for Security Clearances, Certificates and Advice acts as an independent administrative court where one can appeal when his/her security clearance or certificate is refused or withdrawn, or if negative security advice is issued;540
- The Federal Ombudsman can conduct investigations after receipt of complaints from individuals or on the request of the House of Representatives against any 'federal administrative service', and thus—in theory—the intelligence services;
- The Commission for the Protection of Privacy can examine whether or not the requirements of the Data Protection Act are met by the intelligence services when processing personal data;
- The Court of Audit supervises the use of financial resources[541] and can—on its own initiative or at the request of Parliament—initiate an investigation of the good financial governance of departments;

[538] Legal Advisor, Standing Committee I. The positions expressed in this study reflect the personal opinion of the author.
[539] Further in the text, the words 'intelligence services' are used to refer to the 'security and intelligence services'.
[540] Van Laethem 2008a.
[541] For reasons of confidentiality, a part of the budget of State Security and of the General Intelligence and Security Service of the Armed Forces (i.e., the 'special funds' with expenses dedicated to operations and informants) is not supervised by the Court of Audit. As regards State Security, the review on these expenses is performed by the Principal Private Secretary of the Minister of Justice. This historic practice of course results in the absence of any external review on this important aspect of the functioning of the intelligence services. Since 2006, the review on the special funds of the military intelligence service has been even less transparent: the expenses were reviewed by the head of the Army without any intervention of the Minister of Defence. As suggested by the Court of Audit, the control by the head of the Army now is being performed in the presence of the Chairman of Standing Committee I.

- The Administrative Commission for Monitoring Specific and Exceptional Intelligence Collection Methods controls the legality of methods such as telephone tapping, searching, and computer system intrusions;[542]
- The Council of State, the highest administrative court in Belgium, indirectly reviews the activities of the intelligence services in some specific cases; and
- The Judiciary can intervene if a fundamental right is violated or if somebody has suffered harm as a result of unlawful or careless acts of intelligence services.

Given the scope of this study, these elements are not developed further.

2. THE BELGIAN PARLIAMENT AND THE MONITORING COMMISSIONS OF THE SENATE AND THE HOUSE OF REPRESENTATIVES

The Belgian Constitution vests the Legislative branch (i.e., the House of Representatives, the Senate and, to a limited extent, the King) with the power to elaborate general legal norms. Besides this, it exerts political control over the Executive branch. Various tools are put at the legislator's disposal in order to fulfil this double assignment. He can ask questions to the Ministers, introduce motions of distrust, (dis)approve the annual budgets and expenditures and conduct parliamentary inquiries. These instruments also apply to parliamentary control on the intelligence services. In the late 1980s, however, it became clear that such a general control on this specific area would no longer suffice.

A first legislative initiative was taken in this respect in 1988: a 'permanent parliamentary monitoring commission' of five Deputies and five Senators was to be established. The Minister of Justice would hold the chair. The Commission was to advise both the Minister and the Parliament on the functioning of the intelligence services. But the Council of State found the bill unconstitutional: the political control of the Parliament has indeed to be exerted through the competent ministers and not through direct control on the services. The bill was thus removed.

The debate was reopened barely two years later. At that time, the results of a parliamentary inquiry commission into the functioning of the police and intelligence services in the fight against terrorism and organised crime were made public.[543] This commission concluded that Parliament did not exert any real control over these services and that an external review became more than necessary because the efficiency of these services and the manner in which they coordinated their activities were far from optimal.

The government perfectly captured the conclusions of the inquiry commission. In its famous 'White Sunday Plan' dated 5 June 1990,[544] it foresaw a series of measures. They were first aimed at ensuring better efficiency and coordination of the police and intelligence services. But in return, the rights and freedoms of the citizens had to be safeguarded.[545] Also, the trust of the public in the intelligence services had to be restored. One of the measures taken was the creation of two external review bodies which, differently from the

[542] Rapaille and Van Laethem (forthcoming).
[543] http://www3.dekamer.be/digidoc/DPS/K2044/K20442499/K20442499.pdf. See page 374.
[544] Fijnaut and Lauwaert 1995.
[545] 'Efficiency', 'coordination' and 'the protection of rights and freedoms' also became the criteria upon which Standing Committee I assesses the functioning of the intelligence services (see Section 3.4).

Parliament itself, could permanently and directly follow up this complex matter: Standing Committee P and Standing Committee I were born.[546]

Ad hoc commissions were established simultaneously within the House and the Senate. These commissions were responsible for monitoring the functioning of the Committees. Yet in 1999, the assignments were somehow divided up: the commission of the House would monitor Standing Committee P and the commission of the Senate was converted into a 'Monitoring Commission responsible for monitoring the Standing Committee I'.

This Senatorial Monitoring Commission consists of five Senators. The Speaker of the Senate chairs the Commission; the Senate appoints the four other members. The opposition is, surprisingly enough, not necessarily represented. In the Monitoring Commission of the House—which consists of eight members—there is, however, proportional representation. But the role that this Commission de jure and de facto performs with regard to the monitoring of Standing Committee I and the intelligence services is significantly less important.

What are the competences of the Senatorial Commission? Firstly it can give Standing Committee I an investigation assignment into the intelligence services or ask to issue advice on a draft bill relating to intelligence work. The Commission in the House has the same competences.[547] Importantly, only the Senatorial Commission is entitled to examine all investigation reports that Standing Committee I produces. Although monitoring the intelligence services is not the first task of this parliamentary Commission, its members can obviously better perform their political control by systematically perusing all the reports drafted by Standing Committee I.

Secondly, both Commissions can in theory have any investigation file of Standing Committee I sent for the purpose of preparing their work. 'In theory' because since the Classification Act of 1998, one assumes that also the MPs from the Monitoring Commission must hold a security clearance and have a need to know in order to consult classified data.[548] Most investigation files contain such data. None of the current (and former) members of the Commission hold such a clearance because they refuse(d) to submit to a vetting procedure. They generally put forward two main reasons: the disclosure of classified information is punishable and therefore, according to some MPs, not compatible with their freedom of speech. Others raise objections to the fact that the vetting procedure is precisely carried out by the intelligence services. Moreover, there is apparently no political consensus to amend the Classification Act. Consequently, it can be concluded that today no classified information can appear in the reports handed over by the Committee, whereas the competent ministers—who hold a security clearance—and the reviewed intelligence services are allowed to read the reports *in extenso.*

But do the MPs really need access to classified information? Their legislative work seems not to require access to such information: the Committee can substantiate its recommendations without disclosing secrets. But to be able to monitor the Committee and to control the Executive Branch, the removal of certain information can become an impediment. Several 'mechanisms', however, do exist to remedy this. On request of the Committee, the services or the Minister can declassify some information. Although they sometimes accede to this request, the Committee is totally dependent upon the services

[546] Considering that the Belgian government stuck to a strict distinction between the police and the intelligence services, the monitoring of both functions was also given to separate services.
[547] So only the Monitoring Commissions can initiate an investigation.
[548] Persons who do not hold any security clearance can only consult data that are classified as 'Restricted'.

and the Minister.[549] Standing Committee I can also be somehow more explicit about certain aspects of an investigation during meetings with the members of the Senatorial Commission.[550] This happens quite regularly. Finally, the MPs can directly ask the competent minister to declassify certain information. Any refusal can be subject to standard political control and might put the responsibility of the Minister at risk.

The members of the Senatorial Commission can thus, in practice, have access to sensitive information. But can they freely use such information within the framework of their political and parliamentary work? The answer is definitely negative. According to Parliament's internal procedures, violation of confidentiality or secrecy leads to exclusion from the Commission.[551] Only information appearing in approved reports or communications can be made public and thus used to elaborate legislative work and exert political control. The investigation reports, which have been made public by Standing Committee I itself, can of course be used as well (see 3.12).

Let's return to the different assignments of the Monitoring Commissions. Both Commissions jointly discuss and examine joint investigations of Standing Committees P and I,[552] the annual activity report of Standing Committee I (see 3.12) and its draft budget. The actual monitoring of the functioning of Standing Committee I, on observance of the provisions of the Review Act of 18 July 1991 and its internal rules, belongs exclusively to the Monitoring Commission of the Senate.[553] In theory, the Commission has to meet with Standing Committee I at least once per quarter. Finally, the plenary session of the Senate keeps a specific but important prerogative: it appoints the three members of Standing Committee I and its Secretary. It can dismiss them in case of serious shortcomings.

3. STANDING COMMITTEE I

Standing Committee I was set up by the Review Act of 18 July 1991 and has been operational since May 1993. The Committee is a permanent, independent, *sui generis* body, responsible for reviewing the activities and functioning of State Security[554], which is the civil intelligence service, and the General Intelligence and Security Service of the Armed Forces (GISS), its military counterpart. Since 2006 the Committee, together with Standing Committe P, also monitors the Coordination Unit for Threat Assessment[555] (CUTA) and, to some extent, the services that are obliged to pass on their information to this fusion centre. In principle, the review relates to the protection of the rights conferred to individuals, the effectiveness of the intelligence services, and the way they coordinate their activities.

The supervision primarily aims at detecting any structural malfunctions within the intelligence services and making recommendations to enable Parliament to perform its legislative work with knowledge of the facts. It is thus a form of indirect parliamentary control over the Executive. But this is only part of the story. The Committee also works on demand of the Executive and even of the Judiciary. Nevertheless, the Committee is not part

[549] The Committee has recommended that a system should be designed in which the classification made by the Belgian intelligence services can be rectified if it does not comply with the legal provisions.
[550] These meetings are systematically held behind closed doors.
[551] This sanction has not been used so far.
[552] Some topics (such as the coordination between the intelligence and police services and the functioning of CUTA) can or must be the subject of a joint review investigation (see Sections 3 and 3.2).
[553] Within this framework, Standing Committee I must inform the Senatorial Commission of any investigation it initiates.
[554] Van Laethem 2008b.
[555] See: Vandoren, Van Laethem and Verheyden 2010.

of any of those branches. It is an independent body that is at the service of the three branches.

The Committee is composed as follows: the Committee *stricto sensu* (i.e., two members and one Chairman appointed by the Senate), an administrative staff headed by a Secretary and finally an Investigation Service headed by a Director. The Committee performs its reviewing role through investigations that it initiates on its own initiative, on the request of the Monitoring Commissions of Parliament, the Ministerial Committee for Intelligence and Security[556], a competent minister or authority, or on the request of a citizen or a civil servant who lodges a complaint. It has been given extensive powers.

Before developing this review competence, the seven other assignments of the Committee are enumerated. It should be noted that the legal competences of the Committee differ strongly according to the assignment.

Since 2003, the Committee has been responsible for controlling interceptions of communications from abroad by the military intelligence service. Since the Special Intelligence Methods Act of 4 February 2010, the Committee has also been responsible for controlling all special intelligence collection methods used by State Security and GISS. The Committee acts here as a judicial body. If necessary, it will order to stop the method and to annihilate the illegally collected data.

Since 1 September 2010, Standing Committee I can give written advice to the judicial authorities on the legality of the way in which information added to criminal proceedings was collected by the intelligence services. Furthermore, the Committee can, on request, advise on a bill, draft Royal decree, ministerial instructions or any other document expressing the political orientations of the competent ministers regarding the functioning of the intelligence services or the CUTA.
The Committee ensures the chairmanship and the registry of the Appeal Body for Security Clearances, Certificates and Advice (see 1). The Investigation Service of Standing Committee I also plays a judicial role: when instructed by the judicial authorities, it investigates the members of the reviewed services who are suspected of having committed an offence. Finally, the Committee can be requested to carry out an investigation in the framework of a parliamentary enquiry. This competence has not been used yet.

Needless to say, these supplementary assignments can be enriching for the review role of the Committee. However, attention must be paid in this respect to possible role conflicts.
In order to explain the review assignment conferred to Standing Committee I, a series of key words will be used, which are characteristic of the manner in which the legislator has conceived the review and the way the Committee puts it into practice.

3.1 Legal basis

A first important characteristic is that the legislature has provided the Committee with a legal basis in the Act of 18 July 1991 governing the Review of the Police and Intelligence Services and the Coordination Unit for Threat Assessment. It is certainly not unimportant. So the review performed by the Committee is strongly anchored in our democracy.

[556] This Committee consists of the ministers of the federal government that have competence in security related matters. It is responsible for outlining the general intelligence policy, monitoring the priorities of the two intelligence services and coordinating their activities.

3.2 Independent

Standing Committee I is an oversight body, which on an organisational level and in its functioning is independent of Parliament, the Executive and the agencies that it oversees, and the Judiciary. In principle, none of the three branches of the State can give any instructions to the Committee on the manner in which it organises its work, carries out its review investigations, outlines its recommendations and disseminates its reports. Even when the Executive orders an investigation, the Committee acts totally independent.

This independence is, for example, emphasised as follows: the Committee is an autonomous organisation, which receives an endowment;[557] the members are appointed by the Senate and can be dismissed only in exceptional circumstances; the duration of the mandate enables them to develop their own policy[558] and the Committee can initiate investigations on its own initiative. Yet this independence does not mean that the Committee has a free hand and remains uncontrolled. As mentioned above, Parliament supervises the operation of Standing Committee I and ensures observance of the legal provisions, approves or amends the internal rules of procedure, examines the draft budget and can instruct the Committee to carry out a certain review investigation (see Section 2). Finally, there is another case where Standing Committee I does not act fully autonomously: within the framework of joint investigations together with Standing Committee P, the Committees must come up with a common report.

3.3 Impartial

The form and functioning of the Committee reveals not only independence but also impartiality. It emerges from the fact that the Committee *sensu stricto* is composed of experts in security related matters who are not parliamentarians, current members of the intelligence agencies or CUTA. Moreover, they may not hold a public elected office nor perform a public or private function or activity that could jeopardise the independence or dignity of the office. Finally, the Review Act stipulates that members of the Committee are prohibited from attending the deliberations on affairs in which they or their relatives have a direct or personal interest. All these elements contribute to the fact that the investigations can be carried out with complete objectivity without party political or personal interests filtering through in the conclusions and recommendations.

3.4 Broad mandate

Standing Committee I can supervise all activities,[559] methods, documents and directives of the two intelligence services and CUTA,[560] regardless of the fact that it is related to administration and management, resources, policies of the agencies, completed or ongoing operations, cooperation with other (foreign) services, information flows, products of intelligence work and its dissemination, etc.[561]

In principle, the review relates to 'the protection of the rights of people guaranteed by the Constitution and the law' (including the rights mentioned in human rights conventions), and

[557] The Committee autonomously decides on the spending of this budget that is granted by Parliament.
[558] The members are appointed for a renewable term of six years.
[559] The functioning, actions, conduct or failure to act.
[560] With regard to the supporting services, the review only relates to the obligation to pass on information to CUTA.
[561] All these topics have already been dealt with several times in the more than 200 investigations carried out by the Committee since its inception.

to 'the coordination and efficiency… of the intelligence and security services'. But the Committee must not confine itself to those three approaches so it can also investigate 'the effectiveness' and—as in many investigations—'the compliance with the applicable law and regulations' without the rights of people being questioned. The investigation mandate of the Committee is thus certainly 'broad'. But it does not obviously mean that everything is possible. There are three (more or less clear) limits.

The Committee has no power to review services other than the aforementioned ones, even if they sometimes engage in intelligence activities.[562] However, the Committee can ask questions to those services on their interaction (operational cooperation or exchange of information) with the intelligence services. In that respect the judiciary, the police services and other administrative authorities are often being questioned within the context of specific review investigations, not to assess their functioning but to assess the functioning of State Security, GISS or CUTA.

In addition—and this is essential to understanding the Belgian system—the review does not involve the political level. This means that the Committee is not allowed to initiate any investigation or make any judgment on a policy decision taken by the Ministerial Committee for Intelligence and Security or by the competent ministers. Standing Committee I can only assess whether the reviewed services have correctly and efficiently followed the Minister's instructions, supposing, of course, that these are not manifestly illegal. It is not always easy to observe this restriction because the actions of intelligence services are often politically directed. But if a decision by the Minister or the Ministerial Committee contravenes human rights, or the law would impede the efficiency of the services, other control mechanisms apply. In the last case, the political control exerted by Parliament (see Section 2) has to take over from the review performed by the Committee.[563] In the first two cases, the Committee could report the facts to the judicial authorities.

Finally, it was not the intention of the legislature that the Committee would investigate purely criminal or disciplinary incidents that do not indicate any structural problems. This restriction relates to the ultimate goal of Standing Committee I: advising the legislature or other branches and authorities in order to achieve better functioning and better protection of rights and freedoms. But this limit cannot always be observed either. This is certainly the case with complaints lodged by individuals that are not always based on structural problems.

3.5 Directly

The Committee performs its review directly by the services, via formal or informal contacts and written or oral consultations of staff members, irrespective of their rank or function. Conversely, all staff members of the services can contact the Committee at any time. This direct form of review differs fundamentally from the political control performed by Parliament. This control is indeed always performed indirectly, i.e., via the competent minister. This 'political filter' does not apply to the Committee.

[562] The Committee cannot perform any review on (the activities of) police services, the Financial Intelligence Processing Unit, the National Security Authority or foreign intelligence services.
[563] If the Committee had to evaluate a minister's policy, it could well be considered a political body rather than a group of experts.

3.6 Complementary

The review performed by the Committee is complementary to existing control mechanisms; it does not replace them. So the Committees' review does not rule out normal parliamentary control. The same applies for internal control within the services and hierarchic control by the competent minister. Also, the control of individual dossiers by the Commission for the Protection of Privacy and the control of expenditures by the Court of Audit (see Section 1) remain unaltered. But this does not mean that the Committee must stay on the sidelines. It can carry out similar investigations on its own. Thus the Committee often consults individual dossiers and assesses the relevance and legitimacy of the processing of personal data in its review investigations. And just like the Court of Audit, the Committee can supervise the use of financial resources[564] and initiate an investigation of the financial governance of departments. Evaluating the efficiency or effectiveness of a service is indeed impossible without consulting the financial resources and the manner in which they are spent.[565] In that sense, complementarity sometimes leads to overlapping competences.

3.7 Permanently

The Committee is not a temporary review authority, such as parliamentary inquiry commissions. In order to enable an efficient review, the legislature has opted for a permanent body of which the (staff) members have no other duties. This means that this kind of democratic control continues when Parliament is in recess, when the Chambers are dissolved or during negotiations prior to the formation of a government.

The 'permanent' character of the review was initially expressed by the fact that the Committee was conferred only one role and therefore could completely focus on the review of State Security and GISS. However, as explained above, the Committee has been entrusted with many additional assignments throughout the years (see Section 3). Considering that these new duties are related to the functioning of the intelligence services and that the Committee's staff has been beefed up accordingly, this certainly is enriching for the review role of the Committee.

3.8 Specialised

The review of intelligence services has not been conferred to an existing authority. Considering the particular nature of the matter, a specific body has been created. The legislature opted for a 'commission of wise men' with its specific Investigation Service. In order to be appointed, the three members of the Committee have to demonstrate at least seven years of relevant experience. Moreover, they must have held positions requiring a high level of responsibility. The Investigation Service, which mainly carries out the fieldwork, is multidisciplinary in its composition so as to ensure a wide range of expertise.[566] Furthermore, the Committee can always call for the cooperation of external experts. The review investigations being carried out by a specialised authority must be an

[564] The Committee already reviewed the expenses in the special funds of the intelligence services within the framework of an investigation (Standing Committee I, *Activity report 1995*, 105–109).
[565] The Committee sometimes reviews very specific expenses within the context of certain investigations; for instance, to ensure the allowance granted to an informant is proportional to the information supplied.
[566] The Committee has always opted to employ some policemen or intelligence agents in his Investigation Service. They are seconded to this service for several years.

important guarantee of the value of the conclusions and recommendations for the 'clients' of the Committee.

3.9 Powerful

The fact that the Committee is in many aspects a very 'powerful' organisation is perhaps one of the most important characteristics. Its annual budget amounts to €4 million; it employs 22 fulltime equivalents but above all it is entrusted with far-reaching legal competences in order to collect information and carry out credible investigations.

First of all, the services reviewed are obliged, on their own initiative, to provide the Committee with all documents—even classified ones—governing the conduct of the members of the service. Secondly, the judicial authorities must inform the Committee of the opening of a criminal investigation against a member of an intelligence service. Thirdly, and this is very important, the Committee may request any document[567] that is deemed necessary for the performance of its legal assignment. Information is thus gathered regardless of any specific investigation; it enables the Committee to be aware of the ins and outs of the services. The one exception is for the administrative authorities concerned (e.g., the Ministerial Committee for Intelligence and Security or the competent minister) to decide whether it is relevant to provide Standing Committee I with their policy documents.[568]

As soon as an investigation is officially opened, the Committee has many additional possibilities at his disposal. Again it may request any document in possession of the intelligence services.[569] It can thus request complete individual files on citizens and examine the way in which the services have collected, processed and analysed personal data. Information from these files originating from other authorities also has to be passed on to the Committee. These 'other authorities' include foreign (intelligence) services. According to the Law, the third party rule does not apply in relation to the Committee. But of course the Committee is extremely cautious and requests such information only if it is essential to the investigation. The Committee mostly receives photocopies of the requested information and documents. They are attached to the investigation dossier that the Committee archives. They can sometimes be useful for new investigations.

The reviewed services obviously do not always systematically follow (completely) the Committee's requests. But the Committee has more than one trick up its sleeve: it can ask other authorities what information they exchanged with the controlled services; it can check the content of the databases of the services with its own login; it can at all times enter and inspect the premises where members of the services perform their duties; it can confiscate any objects and documents useful to the investigations.[570] Nevertheless, those means of coercion are rarely used.

Besides the request of documents, the Committee can also decide to audition any person working in or outside the services reviewed. Nobody is obliged to submit to this hearing,

[567] The content, form, classification level, author or addressee of the document is irrelevant.
[568] This exception also applies, for example, to agreements with foreign governments and international organisations concluded by the political authorities; not to agreements concluded by the intelligence services themselves.
[569] Once again, this obligation does not apply to policy documents of other authorities.
[570] There are two exceptions to this rule. Documents relating to an ongoing criminal investigation cannot be confiscated. Moreover, when the confiscation of classified documents could jeopardise the missions of the intelligence services or the physical integrity of an individual, the chairman of the Committee decides what should be done with these documents.

with one important exception: members and even former members of the services reviewed may be summoned to testify under oath.[571] In this case, they are obliged to answer all questions. Any refusal is liable to punishment.[572] Furthermore, members of the intelligence services (but also citizens and civil servants of other services) can directly contact the Committee in order to make a statement. If asked, their anonymity is preserved. From every hearing, 'minutes' are drafted and added to the investigation dossier.

Finally, the Committee can demand the assistance of experts, interpreters and even the police. The Committee has already resorted to external experts especially with regard to very technical matters, but not so with interpreters and the police.

3.10 Investigator

The review performed by the Committee essentially takes the form of well-defined review investigations. These investigations can be descriptive or take the form of an audit; they can be reactive or prospective; they can be extensive or very brief. But the exercise always comes down to describing the situation 'as is' as accurately as possible. The findings, conclusions and recommendations of each investigation are drafted in a report. In principle, these reports are sent to the competent ministers and—in a declassified version—to the Senatorial Monitoring Committee.

Although it can be argued that the Committee is more an 'investigator' than a 'monitor', this is not the case in practice. The Committee closely follows the functioning of the services in order to select relevant investigation themes. It studies the documents it receives, attends working groups, organises informal hearings, maintains contact with members of the services in the field, organises periodic meetings with the management of agencies, keeps itself up-to-date with regard to specialist literature, legislation, the media etc.

However, the Committee does not decide alone what should be investigated: if the Commission within the Senate or within the House of Representatives, one of the competent ministers, the Ministerial Committee for Intelligence and Security or the director of CUTA deems it necessary, they can order the Committee to open an investigation. The Committee *must* perform this investigation. Even if a citizen or a civil servant lodges a complaint, an investigation has to be initiated, unless the complaint is manifestly unfounded. Several actors are thus interfering in the agenda of the Committee.

3.11 Advisor

The Committee has already been described as a 'powerful' organisation (see Section 3.9). But this characteristic is restricted to investigation possibilities. Indeed, within the framework of its review role, the Committee cannot take any binding decisions; it only makes recommendations or gives advice to its 'clients'.[573] The authorities—and we approve this approach—decide whether or not they take these recommendations into account. Yet

[571] It has already occurred on several occasions.
[572] Again, there are only two exceptions to this rule: if the hearing deals with the facts relating to an ongoing judicial investigation, the chairman of the Committee first consults the competent magistrate and if the physical integrity of an individual could be jeopardised as a result of the hearing, the chairman of the Committee will decide whether the questions have to be answered.
[573] If the Committee could take binding decisions concerning the efficiency of the reviewed services, it would become completely co-responsible for the elements it has to review.

the recommendations with respect to the Executive Branch are not completely free of obligations: the competent minister must inform the Committee of his or her response to these conclusions. Furthermore, the Committee can report to the Parliament when no appropriate action has been taken.

3.12 Transparency

A raison d'être of the Committee was/is to restore/keep the confidence of the citizen in the intelligence services. The Committee tries to do this in various ways. It produces very detailed annual reports that are widely disseminated and are available for consultation on the website of the Committee. Moreover, reports of high public interest are, as far as possible, fully posted on the website. What is more important is that the Committee will investigate all complaints lodged by the citizens, even if there seems to be no underlying structural problem. The complainant will be notified of the conclusions of the investigation. Only manifestly unfounded complaints are dismissed. Even then, the person concerned will be informed of this in writing.

3.13 Secrecy

There are naturally significant limits to transparency. This is obvious for all those involved in the intelligence community. In this way, all employees of the Committee hold a top-secret level security clearance, regardless of their position within the organisation. Classified documents are available only on a need to know basis. Unauthorised disclosures of classified information can lead to withdrawal of the security clearance, dismissal from the Committee and even penal sanctions.

The premises of the Committee are considered a classified area where all the security regulations required and strict procedures apply. The Secretary of the Committee is specifically responsible for the protection of the secrecy of the documentation and archives.

4. CONCLUSIONS

Many authorities (can) control one or more aspects of the functioning of the Belgian intelligence services. In this way, Belgium certainly complies with Practice 6 of Special UN Rapporteur Scheinin: intelligence services should be supervised by 'a combination of internal[574], executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law' and 'the combined remits of oversight institutions cover all aspects of the work of intelligence services'.[575] This is to be applauded. Yet the multiplicity of overlapping control modalities can indeed have negative effects, not only for the intelligence services[576] but also for the quality of the control itself[577] and for the citizen as it is unclear which authority s/he is supposed to address in a specific case. Yet it must be clear that these reasons cannot be an excuse to avoid performing

[574] In Belgium, there is obviously also internal, hierarchic control of the intelligence services. However, this aspect was not to be developed in this study.
[575] UN Special Rapporteur 2010.
[576] Considering that each control authority has its own desiderata and priorities, the intelligence services could be submerged under time-consuming investigations. Another aspect of the problem is that more persons from various bodies are informed of the functioning and of the information position of the intelligence services. It can both directly (an increasing risk of compromising confidential information) and indirectly (foreign services will perhaps pass on information more cautiously) have negative effects.
[577] For instance, the 'expertise' that is scarce given the specificity of the sector, gets disseminated to several services.

thorough external control of all aspects of the functioning of the intelligence services. Besides, practice proves that most of the control authorities do not really exploit their legal competences. There is of course one major exception: Standing Committee I. In the existence of this independent, permanent and powerful body certainly lies the strength of the democratic control of the intelligence services in Belgium.

To conclude, we could say that the good practices, procedures and standards that should be taken into account when considering effective oversight on the overall functioning of intelligence services are reflected in the abovementioned key words. However, if some significant elements would have to be picked out, they would certainly be the following:

- Set up an independent body of 'wise men'—which has as few links as possible with the reviewed services and the political class—so that its conclusions, analyses and recommendations cannot be considered unacceptable in advance by the legislature, the executive power, the reviewed services or citizens.
- Give the review body all the necessary competences and resources so that it can investigate all aspects of a case, leaving no 'blind spots' and countering all possible doubt about the results.
- Find a fair balance between 'transparency' in order to perform a meaningful investigation for the different stakeholders and 'secrecy' in order to avoid jeopardising the functioning of the intelligence services.
- Design a system in which the classification made by the intelligence services can be rectified if it does not comply with the legal provisions.
- See to it that in a parliamentary commission the opposition is represented.

REFERENCES

Delepière J.-Cl. (2005), 'Le Comité Permanent de contrôle des service de renseignement', *De Staatsveiligheid: Essays over 175 jaar Veiligheid van de Staat*, Cools M. e.o. (eds.), Politeia, Brussels, pp. 225–240.

Fijnaut C. and K. Lauwaert (1995), *Het Belgische Politiewezen*, Kluwer Rechtswetenschappen België, Diegem, pp. 195–211.

Matthijs H. (2008), 'Intelligence services in Belgium', *Intelligence and National Security*, Vol. 23, No 4, pp. 552–576.

Rapaille G. and W. Van Laethem (forthcoming), 'La nouvelle Loi sur les méthodes particulières de renseignement: une révolution pour les services de renseignement belges', *Revue de Droit Pénal et de Criminologie*.

Rapaille G. and J. Vanderborght (2010), 'L'herbe est toujours plus verte ailleurs. Sur le contrôle belge des services de renseignement et de sécurité', *Cahiers de la Sécurité*, No 13, pp. 122–133.

Schuermans F. (2000a), 'Nogmaals een wetswijziging betreffende het comité P en het comité I: de Wet van 20 juli 2000 tot wijziging van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten', *Tijdschrift voor Strafrecht*, pp. 241–251.

Schuermans F. (2000b), 'Controle op politie en inlichtingendiensten: de krachtlijnen van de wet van 1 april 1999 houdende wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten', *Tijdschrift voor Strafrecht*.

Standing Committee I, *Code des Services de Renseignements. Fonctionnement*, compétences et contrôle, Bruges, die Keure.

Standing Committee I (2010a), *Activity Report 2008 – Activity Report 2009*, Intersentia, Antwerp, available at (www.comiteri.be).

Standing Committee I (ed.) (2010b), *Fusion Centres throughout Europe - All Source Threat Assessments in the Fight against Terrorism*, Intersentia, Antwerp.

Standing Committee I (2008), *Activity Report 2006 – Activity Report 2007*, Intersentia, Antwerp, available at (www.comiteri.be).

UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Combating Terrorism (2010), *Compilation of good practice on legal and institutional and measures that ensure respect for human rights by intelligence agencies,* UN General Assembly, A/HRC/14/46.

Vandoren A., Van Laethem W. and L. Verheyden (2010), 'Belgium - The Coordination Unit for Threat Assessment', *Fusion Centres throughout Europe - All Source Threat Assessments in the Fight against Terrorism*, Standing Committee I (ed.), Intersentia, Antwerp, pp. 1–17.

Van Laethem W. (2008a), 'Remedies against an unreliable reliability-check', *Stockholm International Symposium on National Security and the European Convention on Human Rights*, The Commission on Security and Integrity Protection (ed.), *sine loco*, pp. 125–133, available at (www.comiteri.be).

Van Laethem W. (2008b), 'The Belgian civil intelligence service: roles, powers, organisation and supervision', *European Journal of Intelligence Studies*, Vol. 2, pp. 1–29.

Van Laethem W., Van Daele D. and B. Vangeebergen (eds.) (2010), *De Wet op de bijzondere inlichtingenmethoden*, Intersentia, Antwerp.

Van Outrive L. (2003), 'Intelligence Services in Belgium: A Story of Legitimation and Legislation', *Democracy, Law and Security*, Brodeur J.-P., Gill P. and D. Tollborg (eds.), Aldershot, UK, pp. 31–59.

Van Outrive L. (1991), 'La loi organique du contrôle des services de police et de renseignements: un grand défi', *Journal des Juristes Démocrates*, Vol. 80, pp. 9–11.

ANNEX A: COUNTRY CASE STUDIES

II. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN FRANCE

CHARLOTTE LEPRI

In fall 2007, the French Parliament passed a law establishing a parliamentary intelligence committee (*Délégation parlementaire au renseignement*, DPR),[578] whose purpose is to allow members of the National Assembly and senators to 'follow the general activity and the means of the specialized services',[579] thus helping the French intelligence services to gain greater recognition while preserving the confidentiality of their actions.

Passed almost unnoticed, this law is at first glance quite a revolution in France. It ends the French exception because France was one of the last democratic countries without a parliamentary committee dedicated to the monitoring and controlling of intelligence services. This law aims to facilitate the information Parliament gets on the activity of intelligence services according to the requirements of any democracy, while ensuring the safety of agents who perform an essential mission for French national security and for the defence of French interests in the world. Along with the Parliament monitoring intelligence, this text aims to legitimise these intelligence services in the eyes of French citizens and our political leaders while promoting the emergence of a genuine French culture of intelligence—a phrase that was considered an oxymoron until recently.

For a long time, intelligence has been neglected in France, both at the political and academic levels. France lags behind for mainly five reasons: the cult of secrecy, the lack of interest from political leaders, distrust of the French citizens (due to lack of knowledge about its usefulness), the lack of 'prestige' of intelligence activities that are regarded as disgraceful and despicable, and the reluctance of academic fields to go into intelligence studies. As stated in a parliamentary report, intelligence activities have only been perceived 'through the distorting prism of caricature, or even scandals'.[580] For many people in France, intelligence means lies, manipulation, deception and theft. As a result, intelligence has become a 'cultural taboo', a victim of the mistrust from both public opinion and political leaders. Due to the lack of a French culture of intelligence, French officials have always tended to keep their distance from activities related to intelligence, quickly forgetting that these services cannot act independently from the Executive Branch, which provides the orders directly. This approach is a stark contrast to the ones in other countries and accounts for the French delay in establishing a parliamentary committee in charge of intelligence related matters.

The French political system of the Fifth Republic, established in 1958, also explains the French exception. France is a semi-presidential regime.[581] The President of the Republic is popularly elected (since 1962) and is not merely a head of state without political authority:

[578] The law was discussed during the summer of 2007, adopted on 25 September 2007 and officially published on 9 October 2007.
[579] Government of France 2007, Law n°2007-1443.
[580] Paetch 1999.
[581] Duverger 1996.

he is the Commander-in-Chief of the armed forces, he can dissolve the National Assembly, but he is not responsible to the Parliament. Defence, foreign policy and intelligence matters are part of the President's so-called *domaine reservé* (reserved domain). The Prime Minister heads the cabinet and is subject to the Parliament's confidence. The Parliament is weaker than in other Western democracies[582] and, despite some oversight powers, they are hardly used by its members. Until the constitutional reform of 2000, the presidential and the parliamentary terms were disconnected, leading to 'cohabitation' periods in which the President and the Prime Minister are from opposing political parties.[583] Since 2000, the parliamentary term coincides with the presidential term (5 years) but, as chosen by the Cabinet at that time, the presidential elections are held a few weeks ahead of the parliamentary ones. As a result, the Parliament now gets its legitimacy from the President, whose election lines the path to the parliamentary majority. In such a situation, control is less effective with members of Parliament (MPs) being dependent on the President.

Despite what this new law introduced, this text is a modest first step: the DPR will not have the means to exercise real control over the services and its role will be rather symbolic.

1. THE GENESIS OF PARLIAMENTARY CONTROL OF INTELLIGENCE SERVICES IN FRANCE

The establishment of parliamentary oversight of intelligence has encountered many obstacles. It is the result of a long battle that began in the 1970s, then was further developed by Paul Quiles and Arthur Paecht in 1999. It was taken up again in late 2005 by MPs such as Alain Marsaud, which led to a promise by Nicolas Sarkozy during the presidential campaign. The reform has long been met with refractory political authorities, highlighting the complex relationship between policy makers, public opinion and intelligence matters.

In the 1970s, the idea of establishing parliamentary control of intelligence services was discussed. But bills were mainly proposed by minority parties that wanted to control the use of intelligence services by the majority party, following a drug trafficking scandal.[584] In 1971, a socialist senator[585] as well as communist senators[586] presented 'proposals of resolution' to set up a Committee of parliamentary oversight of the SDECE (*Service de documentation extérieure et de contre-espionnage*, former name of the external intelligence agency). In general, MPs were afraid of being manipulated by intelligence services and accused of connivance with them in case of a scandal – when they were not, as was usually the case, indifferent to those matters.

In September 1985, in the context of the Rainbow Warrior scandal,[587] then Prime Minister Laurent Fabius declared that the French government wanted to set up a parliamentary investigation committee regarding this scandal.[588] However, the request was not pursued. Although the Communist group twice proposed a law to set up a committee on intelligence

[582] A small number of committees, limited power to enact bills or to amend governmental bills, limited control of foreign policy and military operations abroad, etc.
[583] In such a situation, the relationship between the President and the Parliament is tense, especially because the Parliament tries to free itself from the President (primarily through more effective parliamentary oversight).
[584] Time 1971.
[585] Courrière 1971.
[586] Guyot et al. 1971.
[587] It was an operation led by the French external intelligence service, the *Direction Générale de la Sécurité Extérieure* (DGSE) in July 1985, aiming to sink the Rainbow Warrior, a Greenpeace ship, in the port of Auckland, New Zealand to prevent Greenpeace from interfering in a nuclear test in Moruroa. One person died.
[588] Fabius 1985.

(in 1985 and in 1988), the Socialist Party refused to put this proposal on the Parliament's agenda.

President François Mitterrand, as well as President Jacques Chirac, saw intelligence as a 'necessary evil' and an executive branch's prerogative. Besides, the Ministries of Defence and Interior were reluctant to share 'secret' information with MPs. Similarly, the intelligence services were afraid of widening the 'secret circle' and talking with MPs, who were considered unfamiliar with intelligence issues.

Despite those failures of direct attempts to oversee intelligence questions, some indirect efforts are worth noting:

- From 1971 to 1999, 7 out of 18 attempts to set up investigation committees on directly or indirectly intelligence-related matters succeeded.[589]
- In 1978, the CNIL (*Commission nationale de l'informatique et des libertés*) was created as an independent authority[590] to protect 'information technology, files and liberties'.[591]
- In 1991, a law regarding telephone surveillance for security reasons was passed.[592] It set up judicial monitoring on the interception of domestic communications through an independent authority, the *Commission nationale de contrôle des interceptions de sécurité* (CNCIS).[593]
- In 1998, the Parliamentary Commission on Rwanda chaired by Paul Quiles was the first parliamentary inquiry commission to examine issues related to the President's *domaine réservé* and to extend parliamentary oversight on security and defence matters.[594]
- In 1998, the law on national defence secrets created another independent authority (*Commission consultative du secret de la défense nationale* or CCSDN),[595] which was in charge of the declassification of documents.[596]
- The 2002 Finance Law[597] created a committee to oversee the allotment of secret funds (*Commission de vérification des fonds spéciaux*).
- To a great extent, there have been growing informal relations between MPs and intelligence services, as well as hearings of heads of intelligence services (in the National Defence and Armed Forces Committee and the Foreign Affairs Committee).

In 1999, two new bills were proposed: one in the Senate by Nicolas About (from the right-wing party), establishing a parliamentary delegation of intelligence responsible for assessing the 'national intelligence policy' and another one, significant to the National Assembly, by Paul Quiles (from the Socialist Party) 'for the establishment of a parliamentary delegation for intelligence matters,' to monitor the activities of intelligence services 'by examining their organization and general duties, skills and means'. This last proposal was the subject of a background report conducted by Arthur Paecht, from the centrist party.[598] However, this proposal was never put on the agenda of the Assembly: in

[589] Laurent 2010.
[590] Including MPs, judges and qualified personalities.
[591] Government of France 1978, Law n°78-17.
[592] Government of France 1991, Law n°91-646.
[593] Including MPs and judges.
[594] Quilès 1998.
[595] Including MPs and judges.
[596] Government of France 1998, Law n°98-567.
[597] Government of France 2001, Law n° 2001-1275, Article 154.
[598] Paetch 1999.

the cohabitation period, both the President (Jacques Chirac) and the Prime Minister (Lionel Jospin) were reluctant to widen parliamentary oversight on intelligence matters.

In November 2005, during the discussion in open session of the bill on the fight against terrorism, the National Assembly considered three amendments (submitted by Jacques Floch, Alain Marsaud and Pierre Lellouche) designed to create a delegation that provides oversight of intelligence. These amendments were justified by the fact that the bill was giving important powers to the intelligence services, including access to databases. They have not been adopted but the Minister of Interior at the time, Nicolas Sarkozy, promised to set up a working group to develop a text on the subject.[599] Preparatory work was carried out quickly and a bill was proposed in the National Assembly on 8 March 2006.

This bill was not included in the agenda of the XII° legislative term, which at that time was coming to an end. After the 2007 presidential and legislative elections, Law n°326—establishing a parliamentary delegation for intelligence (identical to the text of 2006)—was submitted on 5 June 2007 and passed on 25 September 2007. It was finally published on 9 October 2007. This development matched the new environment:

- Intelligence has become much more prominent since the Cold War and means of collection have increased significantly;
- French intelligence services were less reluctant to parliamentary involvement in intelligence matters. The Parliament votes on the budget, so they realise the necessity of having 'allies' in the Parliament (i.e., MPs familiar with intelligence concerns). Intelligence services also realised that too much secrecy lead to suspicion and that a parliamentary committee would help to defend them in case of misinformation (especially from foreign intelligence services);
- Parliamentary oversight of intelligence services is finally considered by policymakers as the best way to both upgrade the role and image of these services (more visibility and greater accountability to make it more effective) and to enhance the role of Parliament in monitoring intelligence activities (services having finally qualified interlocutors on these issues);[600]
- Since 2008 and the release of the French White Paper on Defense and National Security, greater emphasis has been put on intelligence. Intelligence has been recognised as a necessary tool (and no more as a 'necessary evil') to protect the homeland and to combat today's diverse, dangerous and global threats. This White Paper was followed by 'the first global reform of France's intelligence structure since World War II':[601] the merging of two traditional security services of the Ministry of Interior into a *Direction centrale du renseignement intérieur* (DCRI), the setting up of the National Intelligence Council (*Conseil National du Renseignement*) within the Defense and National Security Council (chaired by the President of the Republic), and the establishment of the National Intelligence Coordinator (advisor to the President of the Republic for intelligence-related matters, in charge of coordinating the activities of the various intelligence services); and
- The demand for the respect of democratic standards (rule of law, human rights, and civil liberties) is growing and covers intelligence matters as well.

[599] Unlike François Mitterrand and Jacques Chirac, Nicolas Sarkozy is more familiar with security issues. Moreover, his willingness to get a 'democratic image' has led him to favour the strengthening of the role of the Parliament in terms of control. The July 2008 reform of the Constitution made this project a reality by strengthening the role of the Parliament.
[600] However, during the debate of the draft text of the 2007 law, the socialist and communist parties suggested to give more powers to the DPR.
[601] Hayez 2010.

Times have changed and advancements were unavoidable. Indeed, the creation of the DPR, besides the fact that it aims to establish trusted relationships between intelligence agencies and Parliament, and therefore with citizens, also enables our country to fill a deficiency in the French democratic system. The DPR wishes to establish a link between intelligence services and the Parliament: the French parliamentary intelligence committee becomes the dedicated contact, able to better understand the challenges and needs of intelligence services (and thus pass the budget with sound knowledge of the ins and outs). However, since currently only non-operational activities are being considered—coinciding with the apparent indifference of most French MPs to make the executive more accountable—to what extent will the DPR actually be able to exert control on intelligence services?

2. THE DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT: AN INNOVATIVE BUT POWERLESS TOOL

The DPR is a semi-permanent body, composed of eight members of the Senate and the National Assembly. Among them, four are ex-officio members, as chairmen of the permanent committees of Laws and National Defence (both at the Senate and at the National Assembly).[602] Four other members are chosen by the Chairman of the Senate (one Senator from the majority party and another from the minority party) and the Chairman of the National Assembly (one member of the National Assembly from the majority party and another from the minority party), from propositions of the political groups. In practice, the chosen members are MPs familiar with intelligence issues.

At the National Assembly, Jean-Michel Boucheron of the Socialist Party and member of the Foreign Affairs Committee, as well as member of the Committee of national defence secrets (*Commission consultative du secret de la défense nationale*), and Jacques Myard of the Union for a Popular Movement (UMP) and member of the Foreign Affairs Committee, were selected to be part of the DPR.

At the Senate, Didier Boulaud, Vice-Chairman of the National Defence and Armed Forces Committee and member of the White Paper Commission on Defense and National Security in 2008, and Jean-Patrick Courtois, member of the Law Committee and board member of the National Institute of Higher Studies on Security and Justice (*Institut national des hautes études de la sécurité et de la justice*), were selected.

Members of the DPR have ex officio secret defence clearance, without undergoing a clearance process (MPs are granted access to classified information because they belong to the DPR). On the other hand, staffers must conform to the secret defence clearance process. According to the 'need to know' rule, and despite their clearance, members of the DPR can only access certain information necessary for the conduct of their mission.

2.1 The original mission of the DPR

According to the 2007 law, the DPR's mission is to 'follow the overall activity and the means of specialized services'. The law does not mention a mission of oversight or accountability of the activities and means of the services. The Executive Branch has to 'provide for the committee background information related to intelligence services' budget, overall activity

[602] Senator Jean-Jacques Hyest, Chairman of the Law Committee; Senator Josselin de Rohan, Chairman of the Foreign Affairs and National Defence Committee; Guy Teissier, Member of the National Assembly and Chairman of the Defence Committee; and Jean-Luc Warsmann, Member of the National Assembly and Chairman of the Law Committee.

and organisation'. The committee can hold hearings of 'the Prime Minister, Ministers and the General Secretary of National Defence', as well as 'current heads of the services'.[603] But it has no right to conduct investigations and is not involved in confirmation hearings of new or potential heads of services. The law states that the DPR cannot be informed of 'operational activities of those services, directives from public institutions and funding, as well as exchanges with foreign or international intelligence services'.[604] The work of the committee is classified and meetings and documents are held in a room equipped with secure communication equipment and limited access. Every year, the DPR publishes a public report regarding its activity, without releasing classified information. Even if the law does not forbid it, the DPR has not issued any thematic report so far and members of the DPR do not seem to be inclined to do so.

The 2007 Law is limited and shows modest ambitions, both because of the necessity to maintain the confidentiality of information and the lack of oversight culture in France. It bans scrutiny of past or current operations and limits the possibility of hearings to the current heads of the services. If the members of the DPR follow the book, the room for manoeuvre is quite narrow. Other practical aspects that may tend to restrain the DPR's role:

- The presence of ex-officio members (namely, chairmen of the Law and Defence committees in the Senate and the National Assembly) may rein in the activity of the DPR. Those members give legitimacy to the committee but prevent it from working effectively due to their lack of availability and their overwhelming amount of work (and perhaps a lack of interest).
- The level of knowledge of the members of the committee is quite variable, even though they are all familiar with intelligence issues.
- The lack of dedicated staff (only four part-time staffers for administrative matters) limits de facto activity of the DPR.
- The members of the DPR may show empathy, or even sympathy, towards intelligence services. By trying to gain the trust of the intelligence services, MPs may be tempted to adopt a supportive attitude and to limit their criticisms.
- The first two annual public reports[605] were not very detailed.[606] The 16-page 2009 report only mentions the legal framework and the general activity of the DPR. The 11-page 2010 report is even less informative, describing the composition of the DPR, its mission (as stated in the 2007 law) and its general activity. Those reports failed to reveal anything new and passed by unnoticed. A public report on secret intelligence is intrinsically a difficult balancing act. The members of the DPR chose not to scare intelligence services in limiting the information released in the report as much as possible (as a matter of fact, the annual public report was not initially in the law and was then added during the debate session of the law-making process). But in doing so, it prevents improving the general knowledge of their colleagues in the Parliament on intelligence matters (the classified report is only sent to the President, the Prime Minister and the two Chairmen of the two chambers of the Parliament).

[603] According to the Annual Report, in 2010 the DPR organised 14 meetings and 11 hearings (De Rohan and Warsmann 2010).
[604] Government of France 2007, Law n°2007-1443.
[605] De Rohan and Warsmann 2010 and Hyest 2009.
[606] The classified report delivered to the President of the Republic dealt with several issues involving the French intelligence services: assessment of the 2008 reform of the intelligence community (especially the coordination between intelligence services), the means of the intelligence services, the terrorist threat, cyber-defence, the recent polemic about security interceptions and abuses of the surveillance of some telephone records. This classified report presents some non-binding recommendations.

Ultimately, the DPR has not enhanced Parliament's information on intelligence issues: the overall knowledge of MPs regarding intelligence activities has not improved:[607] members of the DPR do not communicate with the rest of the Parliament and do not teach other MPs about intelligence. Because of the lack of contents in the DPR reports, the press has paid little attention to the functioning of the DPR and its work remains mainly unnoticed.

- The lack of connection with other committees dealing with intelligence questions obstructs the proper performance of the DPR. For instance, the DPR has no prerogative over budgetary accountability and is not allowed to read the annual report of the *Commission de vérification des fonds spéciaux*, which oversees the allotment of secret funds.
- The French law prohibits any legislative inquiry into facts leading to ongoing legal proceedings).[608]
- A question remains unresolved: the French penal code states that every public officer or civil servant who hears about any offense or crime while carrying out his duties must report it to the prosecuting attorney without any delay. A priori, this rule applies to the members of the DPR. But will they report to the prosecuting attorney if they hear about misdemeanours from intelligence services, thus violating the 'national defence secrets' rule? Will they prefer not to reveal what they know, thus becoming a party to intelligence services? Or will they prefer not to know about it, thus asking few and limited questions to intelligence services?

2.2 Practical evolution of the role of the DPR

During its first year, the DPR's main activity was holding hearings with the main intelligence players in order to 'get to know each other'.[609] During the two following years, the DPR went beyond its legal role: it held hearings with senior officials of the services (on behalf of the heads of the services) and other key players on intelligence-related questions (as the National Intelligence Coordinator, whose position was created after the 2007 law and is not listed in the law) and visited intelligence service compounds. It also dealt with current matters (e.g., when a French weekly satirical newspaper, the *Canard Enchaîné*, revealed in November 2010 that French journalists investigating 'sensitive' cases were wiretapped by the DCRI to identify the sources of leaks, Bernard Squarcini, head of the DCRI, and Frédéric Péchenard, head of the national police (DGPN), who were already scheduled to be heard by the DPR, were questioned about this alleged ongoing operation). A member of the DPR acknowledged that despite the restrictive mandate of the DPR, past and even ongoing operations are somehow or other discussed with respect to hot topics.

Moreover, most of the intelligence services did not really suffer from budgetary constraints. For instance, the DGSE (General Directorate for External Security or *Direction générale de la sécurité extérieure*) has even benefited from a rise in its funding since 2007 (from 450 million euros in 2007 to 543.5 million euros in 2011).

[607] Author interviews with French MPs and parliamentary staffers.
[608] Government of France 1958, Ordonnance.
[609] Author interview with a Member of the DPR, July 2009.

More generally, most people agree to say that trust between MPs (at least the members of the DPR) and the intelligence services has improved. But some other developments would be necessary to make the DPR more effective, such as:

- The end of ex-officio members;
- Merging with the Commission de vérification des fonds spéciaux, which oversees the allotment of secret funds;
- Upgrading the annual public report to improve public knowledge on intelligence issues (for instance, following up on the 2008 intelligence reform);
- Coordination between the DPR and an independent authority dealing with intelligence issues;
- Taking into account the issue of intelligence privatisation;
- Improvement of intelligence studies, to question the role of intelligence services and of the DPR;
- The possibility to look into former operations. The DPR has no investigative powers but some of its members think that in case of a scandal, the National Assembly is likely to set up an inquiry commission within the DPR; and
- The incorporation of intelligence activities within a legal framework to 'define the missions of intelligence services and the modalities for the protection of national defense'.610

3. EXTRA-PARLIAMENTARY OVERSIGHT: THE ORIGINALITY OF THE FRENCH APPROACH

As stated in a parliamentary report, 'even though the protection of top secret information has justified the French refusal to create an oversight body in the Parliament, it has not made impossible the setting up of other kinds of oversight. None of them, however, covers all the intelligence services, as they are limited to a certain aspect of intelligence activities'.[611] Generally speaking, three kinds of oversight exist:

- Hierarchical oversight;
- External oversight through independent administrative authorities; and
- Budgetary oversight.

3.1 Hierarchical scrutiny

As for every other public body, oversight and monitoring of the intelligence activities are undertaken by the supervisory ministry through internal scrutiny. However, this issue is not relevant to this study.

3.2 External oversight through independent administrative authorities

France has created an original system of independent administrative authorities (AAI, *Autorités Administratives Indépendantes*).[612] They are administrative bodies acting on behalf of the State by fulfilling a public prerogative but without coming under the government's authority. AAI are usually set up in order to depoliticise important specialised

[610] Government of France 2008.
[611] Garrec 2007.
[612] This system is close to quangos (quasi-autonomous non-governmental organisations).

functions of the State, isolating them from political influences or a potential conflict of interests. These agencies do not report to any public authority of other institutions but enjoy varying degree of independence. They prevent too much concentration of power in the hands of the Executive Branch. Whereas direct attempts to oversee French intelligence services were failing, indirect attempts were increasing through the setting up of AAI.

3.2.1 The *Commission nationale de l'informatique et des libertés* (CNIL)

CNIL was created in 1978. As stated on its website, it 'supervises the implementation of the January 6, 1978 Act, as amended by the August 6, 2004 Act relating to 'information technology, files and liberties'. CNIL's general mission consists of ensuring that the development of information technology remains at the service of citizens and does not breach human identity, human rights, privacy or personal or public liberties'.[613] It was created after a public controversy over a governmental plan called SAFARI, which 'aimed at identifying each citizen with a number and, using that unique identifier, to interconnect all government files'. It is composed of 17 members: four members of Parliament (two Senators and two members of the National Assembly), two members of the Economic and Social Council, six Supreme Court Judges (two members of the *Conseil d'Etat*, the Administrative Supreme Court, two members of the Judicial Supreme Court (*Cour de cassation*) and two members of the National Accounting Office (Cour *des comptes*)) and five qualified personalities appointed by the Cabinet (three), the Chairman of the National Assembly (one) and the Chairman of the Senate (one). According to Article 39 of the 1978 Law, CNIL can name one of its members to be granted access to classified information in order to fulfil its mission.

3.2.2 The *Commission nationale de contrôle des interceptions de sécurité* (CNCIS)

The CNCIS was created by Law n° 91-646 of July 10, 1991, after the condemnation of France on wiretapping by the European Court of Human Rights. The objective was to put administrative wiretaps by security agencies within clear guidelines,[614] allowing for administrative wiretapping with a warrant. The rule is the secret of correspondence and the only exception is related to national security purposes. This law both legalised administrative wiretaps for security reasons and set up oversight through the CNCIS. The CNCIS is composed of three judges and two MPs (one Senator and one member of the National Assembly).[615] Its Chairman is appointed for six years (to guarantee his independence). The CNCIS meets every seven weeks. Its mission is to judicially monitor the interception of domestic communications (wiretaps related to security matters), given that 12 intelligence services within three ministries (Interior, Defense, Budget) can ask for security interceptions. It is an a priori control, both on style (check who is asking for such an interception and on whether or not the application is completed) and on substance (purposes of the interception, principles of subsidiarity and proportionality, etc.). The CNCIS is granted access to classified information.

3.2.3 The *Commission consultative du secret de la défense nationale* (CCSDN)

Created in 1999, the CCSDN is in charge of expressing its opinion regarding the release of classified documents. As a result, the CCSDN is granted access to classified information. It is composed of two MPs (one member of the National Assembly and one Senator)[616] and

[613] CNIL website.
[614] The CNCIS does not deal with judicial wiretaps.
[615] The tacit rule is one MP from the majority party and one MP from the minority party.
[616] The tacit rule is one MP from the majority party and one MP from the minority party.

three Supreme Court Judges (one member of the *Conseil d'Etat*, the Administrative Supreme Court, one member of the Judicial Supreme Court (*Cour de cassation*) and one member of the National Accounting Office (*Cour des comptes*)). They are appointed for six years to guarantee their independence. Two staffers assist the CCSDN with administrative matters. The CCSDN is not a permanent committee: meetings depend on the agenda (usually, one meeting every two months). The CCSDN acts as an interface between the judiciary branch (which wants to access classified documents) and the executive branch, notably through intelligence services (which classify documents). This committee has strengthened oversight of the intelligence services, although the control remains marginal (the CCSDN mostly provides non-binding remarks and opinions to the executive branch). It is worth noting that the new Military Planning Law (2009–2014) has extended the possibility of classification to strategic places for five years. As a result, magistrates will not be allowed to enter classified places without the presence of the Chairman of the CCSDN.

3.3 Budgetary oversight

Budgetary oversight mainly relies upon:

3.3.1 The annual vote of the French Finance Law

The defence budget includes the budget of the DGSE, the DSPD and the DRM. The budget of the DCRI is included in the national police budget. The following table shows figures related to the DGSE and DPSD:

ÉVOLUTION DE L'ACTION « RENSEIGNEMENT DE SÉCURITÉ » (en millions d'euros)

	Autorisations d'engagement				
	2010	**2011**	**%**	**2010**	**2011**
DGSE DPSD	476,5 96,6	543,5 94,0	+ 14,1 - 2,7	527,4 96,6	559,0 93,1
Total	**573,1**	**637,5**	**+ 11,2**	**624,0**	**652,0**
dont personnel *fonctionnement* *investissement*	*393,1* *49,9* *130,1*	*426,2* *69,0* *142,3*	*+ 8,4* *+ 38,1* *+ 9,4*	*393,1* *49,9* *181,0*	*426,2* *68,2* *157,6*

3.3.2 The role of the *Cour des comptes* (National Accounting Office)

The *Cour des comptes* is in charge of conducting financial audits of most public institutions, including intelligence services. As stated on its website, 'the missions of the *Cour des comptes* are defined by the Constitution in paragraph 1 of article 47-2: "The *Cour des comptes* shall assist Parliament in monitoring Government action. It shall assist Parliament and the Government in monitoring the implementation of Finances Acts and of Social Security Financing Acts as well as in assessing public policies. By means of its public reports, it shall contribute to informing citizens". As an administrative jurisdiction, the *Cour des comptes* fulfils these missions in full independence'.[617] Its audits concern 'the quality and regularity of management, the efficiency and effectiveness of the actions pursued in the eyes of the objectives set by the authorities or the entity considered. This mission therefore refers to performance audit practices, i.e., auditing of the results achieved. The Cour does not only criticise but presents recommendations. The Cour releases its

[617] Cour des Comptes website.

conclusions by transmitting them to the Ministry or to the controlled entity'. Theoretically, the *Cour des comptes'* monitoring can go into the smallest details.

3.3.3 The *Commission de vérification des fonds spéciaux*

Originally created in 1947, this committee was reformed by the 2002 Finance Law (passed in 2001). Since 2001, the *Commission de vérification des fonds spéciaux* has been composed of two members of the *Cour des comptes* and four MPs (two Senators appointed by the Chairman of the Senate and two members of the National Assembly appointed by the Chairman of the National Assembly). Before 2001, secret funds were devoted to the functioning of the executive branch but were usually misused for illegal political party funding, electoral campaigns or private needs. Since 2001, most of the secret funds (80%) have been dedicated to special action of the intelligence services and are subject to the *Commission de vérification des fonds spéciaux*'s oversight. The committee oversees the use of the funds but its powers of investigation and oversight have been limited by the Constitutional Council, which banned oversight of ongoing operations.

4. CONCLUSION: LESSONS LEARNED FROM THE FRENCH EXPERIENCE

A priori, French parliamentary oversight is too recent and underdeveloped to be held up as an example. The DPR is a symbolic step ahead but cannot be considered a real oversight body yet. The lack of information sharing between the various bodies in charge of monitoring or overseeing intelligence activities remains a challenge.

However, the French experience demonstrates that it has admitted that matters of intelligence concern the Parliament. The French delay, both in terms of establishing real democratic control over intelligence, its image or even education and the publication of reference books or reflection on matters of this nature, contrast with other democratic countries. All these aspects are apparently linked to each other: better recognition of intelligence activities at the political or academic level would have a significant impact on their reputation. It is also admitted that there is a link between efficiency and legitimacy. The existence of parliamentary control on intelligence services is the norm in most democracies and seems to go hand-in-hand with better consideration (and efficiency) of the services.

The French experience shows that other ways do exist to make intelligence accountable, through hierarchical, budgetary and external oversight (through AAI, independent administrative authorities).

Finally, the French experience implicitly demonstrates the 'need to share'. Members of the DPR are inclined to imitate the secret functioning of intelligence services, jealously guarding their expertise and privileged access to intelligence services. Even though they have to preserve the confidentiality of their work, members of the DPR must also educate their colleagues about intelligence to improve the Parliament's understanding on that issue.

It would seem that French oversight of intelligence services obviously needs a doctrine to expand and improve. According to many observers, a future scandal related to intelligence services would be the test of the efficiency and the usefulness of the DPR.

REFERENCES

Commission nationale de l'informatique et des libertés website, available at (www.cnil.fr/english/the-cnil/).

Cour des Comptes website, available at (www.ccomptes.fr/en/JF/CA.html).

Courrière A. and the members of the socialist group (2 December 1971), 'Proposition de résolution n°54 instituant une Commission de contrôle parlementaire sur le fonctionnement du Service de documentation extérieure et de contre-espionnage (SDECE).'

Duverger M. (1996), *Le système politique français*, PUF, Paris, 21st edition.

Fabius L. (22 September 1985), 'Declaration', Soir 3, FR3, available at (http://www.ina.fr/politique/gouvernements/video/CAC85103391/declaration-fabius.fr.html).

Garrec R. (20 June 2007), 'Rapport n° 337 (2006–2007) sur le projet de loi portant création d'une délégation parlementaire pour le renseignement', Commission des Lois, Senat.

Government of France (2008), *White Paper on Defence and National Security*, available at (http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit__english_version.pdf).

Government of France (9 October 2007), 'Loi n°2007-1443 portant création d'une délégation parlementaire au renseignement'.

Government of France (28 December 2001), 'Loi n°2001-1275 portant loi de finances pour 2002', Article 154.

Government of France (8 July 1998), 'Loi n°98-567 instituant une Commission consultative du secret de la défense nationale'.

Government of France (10 July 1991), 'Loi n°91-646 relative au secret des correspondances émises par la voie des communications électroniques'.

Government of France (6 January 1978), 'Loi 78-17 relative à l'informatique, aux fichiers et aux libertés'.

Government of France (17 November 1958), 'Ordonnance n°58-1100 relative au fonctionnement des assemblées parlementaires', Article 6.

Guyot R., Duclos J., Boucheny S., Lefort F., Talamoni L., Bardol J., Namy L., Eberhard J. and the members of the communist group (2 December 1971), 'Proposition de résolution n°51 tendant à la création d'une Commission de contrôle parlementaire sur le fonctionnement du Service de documentation extérieure et de contre-espionnage.

Hayez P. (2010), 'Renseignement: The New French Intelligence Policy', *International Journal of Intelligence and Counterintelligence*, Vol. 23, No 3, pp. 474–486.

Hyest Jean-Jacques (17 December 2009), 'Rapport fait au nom délégation parlementaire au renseignement n° 181 (2009-2010)', Assemblée Nationale and Sénat, available at (http://www.senat.fr/rap/r09-181/r09-1811.pdf).

Laurent S. (2010), 'Les parlementaires face à l'Etat secret et au renseignement sous les IV° et V° Républiques: de l'ignorance à la politisation', *Cahiers de la Sécurité*, No 13: Les défis du renseignement, pp. 134–144.

Paecht A. (23 November 1999), 'Rapport n° 1951 au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (n° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire', Assemblée Nationale.

Quilès P., Brana P., and B. Cazeneuve (12 September 1998), 'Rapport d'information n° 1271, sur les opérations militaires menées par la France, d'autres pays et l'ONU au Rwanda entre 1990 et 1994', Commission de la Défense nationale et des forces armées and Commission des affaires étrangères, Assemblée nationale.

De Rohan J. and J.L. Warsmann (17 December 2010), 'Rapport fait au nom délégation parlementaire au renseignement n° 188 (2010-2011)', Assemblée Nationale and Sénat, available at (http://www.senat.fr/rap/r10-188/r10-1881. pdf).

Time (29 November 1971), 'Drugs: The French Connection', available at (http://www.time.com/time/magazine/article/0,9171,877429,00.html).

ANNEX A: COUNTRY CASE STUDIES

III. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN GERMANY

HANS DE WITH & ERHARD KATHMANN

1. SCRUTINY BY THE PARLIAMENTARY CONTROL PANEL

Parliamentary scrutiny of federal intelligence activities in Germany is enshrined in constitutional law by Article 45d *Grundgesetz* (GG or the Basic Law). That provision served as the legal basis for the adoption of the *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes* (PKGrG or Parliamentary Scrutiny of Federal Intelligence Activities Act), under which the federal government is subject to scrutiny by the Parliamentary Control Panel of the Bundestag with respect to the activities of the *Bundesamt für Verfassungsschutz* (BfV or the Federal Office for the Protection of the Constitution), the *Militärischer Abschirmdienst* (MAD or the Military Counterintelligence Service) and the *Bundesnachrichtendienst* (BND or the Federal Intelligence Service).

Like the G10 Commission (see section 2 below) and the Confidential Committee (see section 3), the Parliamentary Control Panel devotes itself exclusively to scrutiny of the intelligence services and is not responsible for scrutinising any other security organisations. This means that police activities are not subject to scrutiny by the Parliamentary Control Panel. There is strict separation in Germany between the intelligence services and the police authorities.

1.1 Development of the Parliamentary Control Panel

From 1956, the Parliamentary Group Chairmen's Panel was initially responsible for scrutiny of the German intelligence services. It comprised the chairs of the political groups in the Bundestag. Its activity was based entirely on an agreement between the Federal Chancellor and the parliamentary groups.

The year 1978 saw the adoption of the Parliamentary Scrutiny of Federal Intelligence Activity Act, which replaced the informal Group Chairmen's Panel with the Parliamentary Control Commission. In 1999, the Commission was renamed the Parliamentary Control Panel. In 2009, the activity of the Panel was placed on a constitutional basis by virtue of its enshrinement in Article 45d GG, and its powers were extended.

1.2 Membership of the Parliamentary Control Panel

The number of members of the Parliamentary Control Panel (hereafter the Panel), its party-political composition and its working methods are determined by the Bundestag by means of an appointment decision. Since 2009, the Panel has comprised eleven members; before then it had nine members.

The members of the Panel are elected from among the Members of the Bundestag at the start of each electoral term. The votes of a majority of the Bundestag membership—known as a *Kanzlermehrheit* or 'chancellor majority'—are required for election. This procedure emphasises the particular trustworthiness of the Panel members, for the Panel is intended to comprise only Members of Parliament who, in the firm opinion of a majority of the House, are personally trustworthy, professionally competent and discreet. At the present time, all the parliamentary groups in the Bundestag are represented on the Panel.

Membership of the Panel is relinquished when a member leaves the Bundestag, resigns from his or her parliamentary group or becomes a member of the federal government or a parliamentary state secretary. It does not expire automatically at the end of an electoral term. For the sake of continuity of parliamentary scrutiny of the intelligence services, the Panel from the term that has just ended continues to perform its duties until the newly elected Bundestag has chosen a new Panel.

1.3 Human and material resources

The Panel is assigned the requisite number of staff from the Bundestag Administration. The human and material resources to be made available to the Panel must be earmarked as a separate item in the Bundestag budget.

In addition, members of the Panel are entitled to employ staff of their parliamentary group to help them in their work after consulting the federal government and obtaining the approval of the Panel. The staff must have been cleared to handle classified material and formally sworn to secrecy.

1.4 Rules of procedure, chairmanship, meetings and confidentiality

The Panel adopts rules of procedure. Chairmanship of the Panel alternates from year-to-year between a representative of the parliamentary majority and a representative of the opposition. The Panel is bound by law to meet at least once every quarter. In practice, it meets monthly behind closed doors.

Any Panel member and the federal government may require that the Panel be convened. In principle, meetings of the Panel may be attended only by its members, staff of the secretariat with security clearance and the competent representatives of the federal government and of the intelligence services.

1.5 Disclosure obligations to the Panel

One of the main elements of the Panel's scrutiny of the intelligence services is the disclosure obligation of the federal government. In practice, this duty of disclosure places the onus on the federal government to volunteer certain information. By disclosing such information, the federal government does not absolve itself of political responsibility.

Under section 4(1) of the PKGrG, the federal government is bound to inform the Panel of:

- the general activity of the intelligence services;
- procedures of particular importance; and
- other procedures if the Panel so requests.

In addition, there are a number of special notification requirements which are prescribed by instruments such as the *Bundesverfassungsschutzgesetz* (BVerfSchG or the Federal Protection of the Constitution Act) and the *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* or G 10, also known as the Article 10 Act (Act Restricting the Privacy of Correspondence, Mail and Telecommunications). These include the disclosure of information regarding:

- Surveillance of postal and telecommunications traffic on the basis of the G 10 (half-yearly);
- Requests for information made to airlines, banks and providers of postal, telecommunication and online services and requests for information on IMSI-catcher operations (half-yearly);
- All other covert gathering of data which 'corresponds in nature and gravity to a restriction of the privacy of correspondence, mail and telecommunications',
- Alerts concerning a person or vehicle in the police information system serving as notification of arrival in the Schengen area (these are known as Schengen alerts and are reported half-yearly);
- Forwarding of personal data to foreign public authorities, such as the intelligence services of friendly states, and to supranational and intergovernmental agencies, if the data were originally transmitted to the intelligence services by the Federal Office for Migration and Refugees or the aliens authorities of the Länder or were gathered by means of strategic telecommunications surveillance (half-yearly);
- Certain service regulations, namely those governing the use of intelligence resources, the transmission of data acquired in the performance of border guard duties and assistance given to the BfV by the Federal Police in the field of radio technology; and
- Forthcoming missions abroad to be undertaken by the Military Counterintelligence Service in the framework of out-of-area Bundeswehr missions and, in that context, the mandatory agreement between MAD and the BND laying down details of their cooperation.

1.6 Right to seek information and other information sources

The Panel is empowered to require the federal government and the intelligence services to hand over files and transmit electronic data files to the Panel. The latter has access to all departments of the intelligence services. Moreover, it may interview members of the intelligence services, staff of government departments, members of the federal government and employees of other public authorities or obtain written information from them. Courts of law and public authorities are required to provide the Panel with official assistance.

This means that the Panel has far more extensive powers to procure information than the specialised committees of the Bundestag. Although the latter can invoke Article 43(1) GG to require the presence of any member of the federal government at their committee

meetings, they do not, in contrast to the Panel, have the right to seek information by means such as inspecting files, interviewing staff of government departments or visiting the seats of public authorities.

1.7 Limits to the Panel's right to obtain information

The Panel's right to obtain information does not extend to items or information over which the intelligence services of the Federal Republic have no right of disposal. This applies particularly to information transmitted to the intelligence services by foreign authorities.

The federal government may also refuse to disclose information if such refusal is necessary for compelling reasons of intelligence acquisition, such as the protection of sources, if disclosure would infringe the personal rights of third parties or if the matter in question relates to the core area of sole responsibility of the executive. If this right to withhold information is exercised, however, the reason for doing so must be communicated to the Panel by the member of the federal government with responsibility for the relevant intelligence service.

1.8 Appointment of an expert

In order to pursue particular issues systematically, the Panel may, after consulting the federal government, appoint an expert in a specific case to conduct investigations that will enable it to perform its duty of scrutiny. The appointment decision must be adopted by two-thirds of the Panel members. The expert may hear individuals or consult files on processes involving the intelligence services. The expert's rights do not extend, however, beyond those of the Panel. The expert must report to the Panel on the outcome of his or her investigations. The Panel, acting by a two-thirds majority of its members, may decide that a written report on the investigations is to be made to the Bundestag.

1.9 Submissions

Lastly, members of the intelligence services may approach the Panel directly in official matters, though not in their own interest or in the interests of other members of the services. They are not bound to use official channels for this purpose but the submission must be copied to the head of the relevant intelligence service. The Panel transmits these submissions to the federal government for its comments.

Submissions addressed to the Bundestag by members of the public regarding conduct of the intelligence services that affects them may be copied to the Panel for information.

1.10 Informing the Bundestag and the public

The Panel reports regularly to the Bundestag:

- In the middle and at the end of each electoral term on its scrutiny activities in general;
- Once a year on its telecommunication and mail surveillance under the G 10; and
- Once a year on information requests from the intelligence services to banks, airlines and providers of postal, remote and telecommunication services and on IMSI-catcher operations.

The reports are distributed as Bundestag printed papers to all Members of Parliament and are therefore publicly accessible. Confidentiality requirements are taken into consideration when reports are being prepared.

The Panel retains the right to approach the public directly for the purpose of assessing certain procedures. This divergence from the precept of strict confidentiality requires a decision to be taken by the Panel, acting by a two-thirds majority of the members in attendance. In this case, each individual member of the Panel is permitted to publish a dissenting opinion.

2. SCRUTINY BY THE G10 COMMISSION

2.1 Remit

The G10 Commission of the Bundestag (hereafter the Commission) scrutinises activities of the federal intelligence services involving the use of intelligence resources that impinge on the fundamental right to privacy of correspondence, posts and telecommunications enshrined in Article 10 GG. The main legal basis for the scrutiny effected by the Commission is the G 10.

Following a procedure that is similar to judicial proceedings, the Commission decides on the admissibility and necessity of measures taken by intelligence services which restrict the privacy of correspondence, mail and telecommunications. The powers of scrutiny of the Commission extend to the entire collection, processing and use of acquired personal data, including the decision whether or not to notify the persons concerned.

2.2 Composition, chairmanship and rules of procedure

The Commission comprises the chairman, who must be qualified as a judge, and three associate members. There are also four substitute members who can attend the meetings and have the right to speak and to ask questions. The members of the Commission—not necessarily members of Parliament—are appointed by the Panel after it has consulted the federal government. Their appointment is for one electoral term, although their period of office does not end until the appointment of their successors or three months after the end of the electoral term, whichever is earlier. The members of the Commission are independent in performing the duties of their office and are not bound by instructions. They hold their office in an honorary capacity.

From among its members, the Commission elects a chairman and a vice-chairman. The chairman convenes its meetings, unless the Commission has set its meeting dates in advance. The Commission has a quorum if four full and/or substitute members are present. The Commission adopts its own rules of procedure, subject to the approval of the Panel and prior consultation of the federal government.

The Commission meets at least once a month. Its members, like those of the Panel, are sworn to secrecy regarding matters that come to their attention in the course of their activity in the Commission. This obligation continues to apply after they leave the Commission.

The Commission must be provided with the human and material resources it needs for the performance of its tasks, and these resources are to be posted separately in the institutional budget of the German Bundestag. They include staff with technical know-how.

2.3 Scope of scrutiny and procedures

The Commission is responsible only for intelligence surveillance measures which relate to the privacy of correspondence, mail and telecommunications protected by Article 10 GG. In particular, this includes the traditional surveillance of telecommunications and of postal operations, and correspondence by the intelligence services.

2.3.1 Individual measures

Intelligence surveillance measures may take the form of what are known as individual restrictions or individual measures. The individual restriction under Section 3 of the G 10 involves ordering the surveillance of a particular telephone line or a particular postal address with the aim of discovering something about a particular person's communications. On the basis of this order, which the competent Ministry must justify in writing, the measure may be taken, but not until the Commission, which must be notified once a month of all restriction measures that have been ordered, has authorised implementation. Only in exceptional cases where there is imminent danger is it possible to commence implementation prior to notification and authorisation. Retrospective notification and authorisation must then be obtained without delay. The Commission assesses the 'admissibility and necessity' of the prescribed measure. This entails examining whether the legal conditions for the measure are satisfied as well as verifying the proportionality of the measure.

The written justification of the order is not the only decision making basis that is available to the Commission. It may also, for example, ask representatives of the intelligence services and of government ministries for information relating to any of its enquiries. Moreover, the Commission must be allowed to inspect all documentation on the restriction measure and be granted access to all official premises. The same applies to its staff who peruse the files on behalf of the Commission prior to its meetings.

If the Commission concludes that the legal conditions for a measure are not satisfied, it declares the measure to be inadmissible or unnecessary. The order must then be cancelled without delay and the measure must not be implemented. If, in a case of imminent danger, implementation has already begun, the measure is to be discontinued forthwith.

If, on the other hand, the Commission concludes that a measure is admissible and necessary, it can be implemented. No order, however, remains valid beyond a maximum period of three months. Should the intelligence service wish to prolong the measure beyond that period, it must apply for an extension, and once again it is the task of the Commission to decide on the application.

2.3.2 Strategic surveillance measures

Besides individual measures, an order may be made, on application from the Federal Intelligence Service, for the implementation of strategic restriction measures with regard to international telecommunication links (Sections 5 and 8 of G 10). In strategic restrictions, information is filtered with the aid of search terms out of numerous bundled calls and messages carried by certain transmission media, such as satellite links and fibre optic

cables. Because strategic restriction measures arouse no suspicion and have a broad spread, they are subject to tight legal restrictions.

Strategic measures for the surveillance of telecommunications or postal traffic are prescribed in the form of a two-stage procedure. In the first stage, the telecommunication or mail links to be subject to surveillance in a particular area of risk are defined. Responsibility for this lies with the Federal Ministry of the Interior, which must obtain the consent of the Panel.

Where a strategic surveillance measure is ordered in the event of a danger to life or limb of a person abroad, and where this particularly affects the interests of the Federal Republic of Germany, the consent to the definition of the target telecommunication links requires a two-thirds majority of the members of the Panel. In the event of a need for urgent action because of imminent danger, as in cases of kidnapping or abduction, provisional consent may be given by the Chairman and Vice-Chairman of the Panel and the Chairman of the Commission. The consent of the Panel and the Commission must be obtained thereafter.

If the Panel gives its consent, the Federal Ministry of the Interior may, at the request of the BND, order telecommunications surveillance within the framework authorised by the Panel with the aid of particular search terms. Before the order is executed, its legality is verified by the Commission. In other words, no strategic surveillance can take place without the consent of the Panel and of the Commission.

2.3.3 IMSI-catcher operations and information requests

The Commission also scrutinises the use by the intelligence services of an IMSI catcher to pinpoint the location of a mobile phone or to find out phone and SIM card numbers. Moreover, the Commission checks the intelligence services' acquisition of information from providers of postal, telecommunication or online services under Section 8a (2)(3) to (2)(5) of the BVerfSchG; for example, their requests for the telephone numbers of lines used in particular telecommunication links. The purpose of the latter measures is often to make appropriate preparations for telephone surveillance.

2.4 Notifications

If a measure is discontinued, because the time limit has expired, the Commission has ruled it inadmissible or unnecessary or the executive has decided not to pursue it any further, the law prescribes that the targeted person must be notified of the cessation of the measure.

The notification is not to be made 'as long as any prejudice to the purpose of the restriction cannot be ruled out or as long as the occurrence of wider detrimental effects on the well-being of the Federal Republic or any of its constituent states is foreseeable'. Notification is incumbent on the authority at whose request the order was issued. The Commission is informed once a month of notifications or of the reasons why, in the view of the intelligence service, notification should not take place. In the latter case, the Commission considers whether it shares the view of the intelligence service that notification should not occur. If the Commission, contrary to the view of the intelligence service, considers notification to be necessary, it must be effected without delay. If, on the other hand, it agrees with the assessment made by the intelligence service, no notification takes place until such time as any prejudice to the purpose of the measure can be ruled out or for as long as the occurrence of wider detrimental effects on the well-being of the Federal Republic or any of

its constituent states is foreseeable. If these conditions for the absence of notification still apply after five years, a final decision may be taken to refrain from notification, provided there is a likelihood bordering on certainty that these conditions will continue to apply in the future. A unanimous decision of the Commission is needed in this instance because the final absence of notification deprives the person concerned of any right to judicial recourse.

2.5 Scrutiny of the use of data

The powers of scrutiny of the Commission also extend to verifying whether the legal requirements have been satisfied in the processing and use of personal data collected with the aid of measures taken under the G 10, information requests under Section 8a(2)(3) to (2)(5) of the BVerfSchG and an IMSI catcher.

The first of these legal requirements is that data affecting the core areas of private life must not be utilised at all but are to be deleted immediately. Moreover, without delay following the collection of data and at six-monthly intervals thereafter, the intelligence services must check whether, in the context of their tasks, the data not affecting these core areas are essential for the purposes for which such collection is generally admissible, either on their own or together with other data that are already available. If the data are not essential, and if they are not required for transmission to other authorities, they must be deleted without delay.

If they are essential, they must, as a matter of principle, be labelled so as to ensure—particularly after transmission to another authority—that they are used only for admissible purposes. These purposes are defined exhaustively in law. The same applies to the conditions in which they may be transmitted to other authorities. Where certain data are transmitted to foreign authorities, the Commission is to be notified monthly of such transmissions.

2.6 Complaints

The Commission is empowered to decide on complaints regarding the admissibility and necessity of restriction measures under the G 10 and information requests under Section 8a(2)(3) to (2)(5) of the BVerfSchG or IMSI-catcher operations under Section 9(4) of the BVerfSchG. After the completion of the Commission's review, the complainant receives a notice setting out its findings.

3. THE CONFIDENTIAL COMMITTEE OF THE BUDGET COMMITTEE

The Confidential Committee is a body comprising members of the Bundestag Budget Committee to which the budgets of the intelligence services must be submitted for approval (see Section 10a(2) of the *Bundeshaushaltsordnung* (Federal Budget Code)).

3.1 Function of the Confidential Committee

The members of the Confidential Committee are elected by the Bundestag for the duration of an electoral term. The rules that apply to the Panel also apply, *mutatis mutandis*, to the Confidential Committee. The Confidential Committee currently comprises ten members of the Budget Committee, who are legally bound to secrecy.

The Confidential Committee discharges budgetary responsibility for the intelligence services. It deliberates on their budgets behind closed doors. The Confidential Committee communicates the final figures it has approved for the intelligence services' budgets to the Budget Committee. The latter accepts the figures without debate, incorporating them into its recommendation for a decision on the federal budget to the House, which then adopts them together with the other parts of the budget. There is no plenary debate on the budgets for the intelligence services. The final budget merely contains the total expenditure figures for the intelligence services as approved by the Confidential Committee.

As far as scrutiny of the execution of the budget and of the discharge procedure are concerned, the Confidential Committee likewise acts on behalf of the Budget Committee or Public Accounts Committee.

The Confidential Committee has similar information-seeking powers to those of the Panel. It can, for example, require the surrender of files, interview staff of the intelligence services, enter their official premises at any time and, in individual cases, commission experts to conduct investigations. In addition, at least in the middle and at the end of each electoral term, it must present a report to the Bundestag on its scrutiny activity to date.

3.2 Consultative role of the Parliamentary Control Panel

The Panel is involved in the discussion of the budgets of the intelligence services. The draft budgets must be transmitted to the Panel for its opinion, the federal government must inform it of the execution of the budgets, and the result of the audit by the Federal Court of Audit of annual accounts and of financial and economic management must be sent to it.

Members of the Panel may take part in a consultative role in the Confidential Committee's deliberations on the budgets of the intelligence services and their execution. Conversely, members of the Confidential Committee may likewise attend the corresponding meetings of the Panel in a consultative capacity. The Confidential Committee, however, still has the last word when it comes to approving the budgets of the intelligence services.

4. OTHER INSTRUMENTS OF PARLIAMENTARY SCRUTINY

Scrutiny of the intelligence services by the Parliamentary Control Committee is without prejudice to the rights of the Bundestag and its committees, which means that traditional instruments of parliamentary scrutiny remain applicable to the sphere of activity of the intelligence services. Foremost among these instruments are:

- Deliberations of the specialised committees and plenary sittings, which any government member may be summoned to attend;
- Parliamentary questions from political groups or individual Members; and
- Committees of inquiry, which must be appointed at the request of a quarter of the Members of Parliament and which can gather evidence in accordance with the provisions governing criminal proceedings.

Particularly in the cases of committees of inquiry and parliamentary questions, privacy issues are often raised in connection with intelligence matters. In this respect, the *Bundesverfassungsgericht* (Federal Constitutional Court) has acknowledged that refusal to testify to a committee of inquiry is generally something that would not occur if effective

precautions were taken against the disclosure of state secrets. Similar principles apply to parliamentary questions. In particular, it is not permissible to refuse to answer them by invoking a report that has been made or is to be made to the Panel. On the contrary, the reasons why the government believes that the question cannot be answered must be set out in detail.

5. FORMS OF EXTRAPARLIAMENTARY SCRUTINY

5.1 Federal Commissioner for Data Protection and Freedom of Information

The intelligence services' compliance with data protection legislation is monitored by the *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit* (Federal Commissioner for Data Protection and Freedom of Information), who is based at the Federal Ministry of the Interior but is independent in the discharge of his office and subject only to the law.

The Commissioner's duties include monitoring observance by the federal public authorities of the provisions of the *Bundesdatenschutzgesetz* (Federal Data Protection Act) and other data protection provisions. He/she acts of his/her own motion but can also be petitioned by any person or persons who believe that their rights have been infringed upon by federal public authorities in the collection, processing or use of their personal data. This also applies to the specific provisions on data protection contained in the BVerfSchG, the *Gesetz über den Militärischen Abschirmdienst* (MADG or the Military Counterintelligence Service Act) or the *Gesetz über den Bundesnachrichtendienst* (BNDG or the Federal Intelligence Service Act).

It is only in the area covered by the G 10—in other words, where data have been collected by the intelligence services by means of telecommunication and mail surveillance—that the Commissioner for Data Protection has no powers and sole responsibility lies with the G10 Commission. The Commission may, however, ask the Data Protection Commissioner to monitor compliance with data protection provisions in connection with specific procedures or in specific areas and to report its findings solely to the Commission. It may also give the Commissioner a general opportunity to comment on data protection matters.

The intelligence services are bound to assist the Federal Commissioner for Data Protection and Freedom of Information in the performance of his monitoring duties. When so doing, they are to be given information in answer to their questions as well as access to all documentation relating to the scrutiny of data protection, especially stored data and data processing programs.

Should infringements of data protection provisions be detected, the Federal Commissioner for Data Protection and Freedom of Information must, in principle, query them with the competent government ministry. Every two years, the Federal Commissioner for Data Protection and Freedom of Information presents an activity report to the Bundestag in which he also addresses issues of data protection law relating to the intelligence services.

5.2 Federal Court of Audit

The *Bundesrechnungshof* (Federal Court of Audit) audits the federal account and determines whether public finances have been properly and efficiently administered. Within the Court of Audit, a body known as the *Dreierkollegium* or College of Three, performs these duties with respect to the intelligence services.

The Federal Court of Audit informs the Confidential Committee and the Panel of the result of its audit. If the findings of the College of Three are liable to be relevant to the granting of discharge to the federal government, the College sums up the result of its audit in a set of observations, which it presents to the Bundestag and the Bundesrat.

6. CONCLUSION

The statutory basis for parliamentary scrutiny of the intelligence services in Germany has been regularly improved and supplemented over the past few decades. As was mentioned above, the last fundamental reform of parliamentary scrutiny of the intelligence services was made in 2009. The new provisions essentially extended the powers of the Parliamentary Control Panel as well as increasing its human and material resources. It is still too early to make a detailed assessment of the practical effects of this latest reform of parliamentary scrutiny of the intelligence services.

ANNEX A: COUNTRY CASE STUDIES

IV. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN HUNGARY

GÁBOR FÖLDVÁRY

1. INTRODUCTION

After the Second World War, the constitutional development of Hungary was forced to diverge from the mainstream of European democratic states for almost half a century. Although during this time sometimes heroic efforts were made to create democracy, these periods could last only for some years immediately after the war and only for a few weeks in the autumn of 1956. Every time, the real reason for the defeat was the international geopolitical situation, which had serious consequences for politics and society in Hungary. In the end, it was the change of these external forces which made it possible for the recovery of four-and-a-half decades of belated development to begin in 1989–90.

When laying the foundations of a democratic state, Hungarian legislation used several foreign—mainly Western European—models. In the field of legal regulation (particularly the external control) of the National Security Services' activity, however, it was difficult to find full-fledged models with a history going back decades, even in the 1990s. The Hungarian Parliament—after a provisory regulation in 1990—passed a law in 1995 on the activity of secret Services, devoting a separate chapter to the parliamentary control of the Services. The depositary of this control was the National Security Committee of the Parliament. Its activity—besides other legal counterweights (courts, ombudsman)—still constitutes an extensive, primarily political guarantee against the necessarily restrictive activity of the National Security Services, directed by the government of the day.

2. COMPOSITION (OFFICERS, MEMBERS) OF THE NATIONAL SECURITY COMMITTEE

Primarily, the same general rules apply to the creation of the National Security Committee (NSC) as to all other Parliamentary Committees. According to these rules, the interests of the larger parliamentary factions are safeguarded by their right of participation in committees in proportions similar to the composition of the Parliament of the day,[618] while the presence of all factions in all Committees must be ensured to protect the interests of smaller factions. As a consequence of the abovementioned rules, the membership of the Committee during the past two decades has been modified almost every four years, moving between 9 and 15 members.

The single regulation related to the composition of the Committee can be found in the National Security Act. According to this, 'the Chairman of the Committee may only be a member of the opposition at all times'.[619] What gives real significance to this regulation is

[618] Republic of Hungary 1994, para. 33(1).
[619] Act No 125/1995, para. 14(1).

that during the organisation of the activity of the Committee, the Chairman has a number of additional rights. Among others rights, the Chairman of the Committee proposes the agenda of the next meeting and can summon and preside over the sessions. In many other cases, it is also the Chairman who represents the Committee towards other institutions and the public.

There are no similar political or professional regulations concerning the members of the Committee. Professional expectations of the Chairman prevail without written requirements. During the past almost twenty years, there has not been any Chairman of the Committee who had not previously taken part in the control of the interior, national security or defence area either as Undersecretary of State or even as Minister.

2.1 National security clearing of candidates for membership

Regarding membership, the Hungarian National Security Act prescribes that 'only those Members of Parliament may be elected as members of the Committee who have been cleared in terms of national security as specified in this Act'.[620] In theory, it is also possible to nominate even a Member of Parliament about whom the national security clearing has found some risk factor. It depends on the decision of the concerned parliamentary faction's leader, who can maintain the candidature of this Member of Parliament to the Committee even if a risk factor has been found. In this case, however, it is the President of the Parliament or the National Security Committee as a whole that has the right to make a decision. If the Committee is not yet formed (typically at the beginning of a parliamentary cycle), the President of the Parliament decides 'on the further validity of the nomination',[621] i.e., s/he can invalidate it. In the other case, when the Committee is already functioning and it is necessary to elect a new member into a vacant position, the National Security Committee itself decides about the validity of the candidature.

3. OPERATION OF THE NATIONAL SECURITY COMMITTEE

Examining the various types of procedures of the National Security Committee, we can conclude that they can be divided into two large groups: procedures prescribed by the Act (without deliberation) and procedures whose initiation is subject to a previous decision of the Committee.

The (mandatory) procedures prescribed by the Act can be divided once again into two groups: procedures whose subject is the Committee itself and those which oblige the executive power to undertake some activity.

The most essential feature of optional procedures is that the Committee decides on their necessity on an ad hoc basis. In what follows, the above listed groups of options of parliamentary control are described in detail.

[620] Act No 125/1995, para. 19(1).
[621] Act No 125/1995, para. 19(7).

3.1 (Mandatory) procedures prescribed by the Act

3.1.1 Obligatory tasks of the Committee

In the chapter on 'parliamentary control' of the Act, we can find two points which specify tasks expressly assigned to the National Security Committee. These are:

1. reporting on the budget of the National Security Services; and
2. hearing the nominees for General Director of the National Security Services before their appointment.

3.1.2 Reporting on the budget of the National Security Services

The first obligatory task can be found in paragraph 14(4)(g) of the Act, which claims that the Committee:

> ...shall give its opinion on the detailed draft budget of the national security services, the items of the budget of other organisations entitled to gather intelligence related to such activities, and the draft of the detailed report on the execution of the Act on the Budget of the year, and shall make a proposal during the debate on the bills to Parliament to adopt the bill in question.

According to the above passage of the Act, the Committee has to receive each year the detailed plan of the Services' budget, as well as the related opinion of the State Audit Office. These documents naturally contain classified information therefore neither the whole of Parliament nor any other committees can have access to these budget figures and documents. On these occasions, the National Security Committee meets in closed session, asking the leader of the Ministry of Finance in charge of this area, the competent personnel of the Minister responsible for the National Security Services and the financial-economic leaders of the Services to answer any possible questions in connection with the budget.

During the parliamentary cycle of 2006–2010, the National Security Committee dealt with the economic activity of the Services 13 times, as defined by paragraph 14(4)(g) of the National Security Act. This average of three occasions per year cover the Committee discussion of the budget bill, the discharge bill and the amendments submitted to the bill.

3.1.3 Pre-nomination hearing of the candidates for General Directors

The other obligatory task is laid down in paragraph 14(4)(h). The regulation prescribes that the Committee, 'prior to their appointment, shall hear the persons nominated to the offices of directors general, and shall take position on their suitability therefor.' In order to understand the proper place of this act in the complete appointment process, it is necessary to quote paragraph 12(1) of the National Security Act: 'The National Security Services shall be headed by directors general, appointed and discharged by the Prime Minister upon the nomination of the Minister'.

The Hungarian legal solution—apart from the abovementioned presumption of the Prime Minister's agreement—brings another branch of power into the nomination process: the National Security Committee of the legislature. The legislative intent—five years after the democratic changes—was to enact a complex selection process. The essence of this process

is the nomination of such persons whose recognition and professional support goes beyond the circle of the political leadership.

In practice, the votes supporting the nominees come from the government representatives in the Committee, which usually has a majority from the governing party. However, it would be wrong to think that the decision on the suitability of the candidate is always a 'fixed' game. This is not true for two reasons. On the one hand, even if they have majority support, it is not indifferent for the nominator and the nominee whether the minority is completely negative or they abstain from voting with a 'well-meaning' attitude. This says a lot about the careful selection of the Director General, as well as about the quality of the future cooperation between the Committee and the Service to be directed by them. On the other hand, a Minister who takes for granted the support of the ruling party members of the Committee may easily get an unpleasant surprise. A good example was the nomination for Director General of the National Security Bureau in December 2007. From the beginning, there were serious doubts about the suitability of the candidate in political circles as well as in public opinion. The Chairman of the Committee kept postponing the placement of the hearing on the agenda for several weeks in the hope that another candidate would be named instead of the highly controversial one, but to no avail. The Minister was unswerving, with the consequence that the candidate—in a so far unprecedented manner—did not receive the support of the majority. The cooperation between the Committee and the government reached a historical low when it turned out that the Prime Minister appointed the candidate all the same.

3.1.4 Obligations of the executive

As we have seen above, in the chapter dealing with parliamentary control, the Act prescribes obligations not only for the Committee. The details of the regulation discussed below refer to an automatic obligation to provide information, to be performed without any request or special order. The bodies bound to fulfil this obligation are the institutions of the executive, mostly the Minister in charge or some of the Services. The performance must be automatic since the most important criterion for carrying out parliamentary control is a sufficient amount of detailed information provided at an appropriate time at the disposal of the Committee. The Act determines four types of this obligation.

3.1.5 'Half-yearly' report on the Services' activities

'The Minister shall inform the Committee about the general activities of the National Security Services on a regular basis, but at least twice a year'' [Paragraph 14(2)]

According to the provisions of the Act, information on the general activities of the national security services has to be provided at least every half year. The established practice is that the Minister sends a written report to the Committee every half year. The Ministers responsible for the control of the civilian and the military National Security Services will obviously send separate reports to the Committee. During the discussion of the reports, the presence of the Minister and all directors general provides Committee Members with an opportunity to ask further questions on the basis of the written material they are already familiar with, or independent of that. On these occasions, there is no time limit for the inquiry of Committee Members or for the answers given by the Minister or the directors.

3.1.6 Information about the Government's decisions relating to the National Security Services

'The Government shall inform the Committee about its decisions on the National Security Services through the Minister'. [Paragraph 14(3)]

For the efficient control of the Services, the Committee has to be aware of the framework determined by the Government for the Services to perform their tasks (competences, rules of cooperation, main directions of the activities, provision of information by other state organs, facilities to protect).[622] One copy of these mostly qualified Government decisions has to be sent to the Committee.

3.1.7 Report on intelligence gathering about Members of Parliament or their relatives

'If the National Security Services begin (pursue) intelligence gathering activities concerning a Member of Parliament or his relative living in the same household, the Minister shall immediately inform the Committee thereof. The Member of Parliament affected in the matter shall not receive information on such activities'. [Paragraph 15(3)]

The information collection of the Services concerning a Member of Parliament or their relative is worthy of attention because it may involve activities by a governmental body that restrict the rights of a Member of Parliament. In certain justified cases, the Act authorises the National Security Services to restrict fundamental rights such as personal freedom, privacy of home, personal privacy, privacy of correspondence, personal data, property, etc.[623] It is hardly necessary to emphasise what a serious violation of the fundamental democratic principles might arise if the Services—abusing their authority—could use these means against the members of political parties without proper justification. Nevertheless, since the necessity of such however delicate information gathering may arise, it seems to be justifiable to inform the Committee immediately in the event of a procedure concerning any Member of Parliament.

3.2 (Optional) tasks to carry out by the decision of the Committee

The optional tasks of the National Security Committee are the cases when there is no statutory obligation to act but the Committee—at its own discretion or majority decision—can initiate a procedure. Although these powers of the Committee are listed in the National Security Act in a different order, on the basis of their content they can be divided into two groups: entitlement for information and entitlement for inquiry.

3.2.1 Entitlement of the National Security Committee for 'requesting information'

The Hungarian National Security Act mentions that when listing the entitlements for controlling, the Committee 'may request information from the Minister, and, with the simultaneous information of the Minister, from the directors general of the National Security Services on the national security situation of the country, as well as on the operation and activities of the National Security Services'.[624] This entitlement for requesting

[622] Act No 125/1995, para. 77(2).
[623] Act No 125/1995, para. 31(3) on the measures applicable by the National Security Services.
[624] Act No 125/1995, para. 14(4)(a).

information is similar to the half-yearly reporting obligation of the Minister. However, there is a difference between the contents of the two paragraphs as the statutory obligation of the Minister refers to the (at least) half-yearly report on the general activities of the Services. The Minister, on the other hand, is compelled to give more targeted, or more in-depth and detailed information—about the national security situation of the country or about the activities and operation of the Services—only at the particular request of the Committee. Another difference is that the Committee may directly turn to the directors general as well and, with the simultaneous information of the Minister, may request information from them if they consider that in the given case the interposition of a political level is not necessary.

The National Security Committee regularly uses the opportunity to inquire about some current national security case through the Minister or the directors general. During the parliamentary cycle of 2006–2010, there were 24 occasions when the Committee, besides the regular half-yearly reports of the Services, requested detailed information from the Ministers in charge of the civilian or military services or from the directors general. With the intention to carry out its legal controlling function in its entirety, the Committee sometimes deems necessary to complement the information received from the National Security Services by the hearing of persons possessing relevant information in a given case. In such a situation, the Committee may also request the hearing of the leaders of other state institutions (e.g., Data Protection Ombudsman, Commander of the Customs and Finance Guard, Chief Commissioner of the Police, etc.)

Paragraph 14(4)(b) of the Act refers to the normal (paragraph 56) and the exceptional (paragraph 59) authorisation procedure of the intelligence gathering requiring outside authorisation. The report on the authorisation generally takes place during the half-yearly hearing of the Ministers and the Services.

3.2.2 Entitlement of the National Security Committee for inquiry

The Committee's intent to receive information is not self-serving. The parliamentary control of the Services is necessary because the secrecy—a prerequisite of efficient national security activity—does not allow for the press or the general public to fulfil its traditional controlling role. This, however, serves as even stronger justification for the creation of efficient and thorough mechanisms when controlling the Services. The above discussed entitlement of the Committee for requesting information will only find its proper place if the body may use further tools as well, if necessary. In this way, in the event of suspicion of illegal operation, these means make it possible to make actual, effective progress in a case. The National Security Committee is not an investigating authority but in order to achieve effective controlling power, it was necessary that in the event of some anomaly concerning the operation of the Services, the Committee could get at least relatively convincing evidence.

The National Security Act empowers the Committee to conduct the inquiry if it is necessary. The Committee orders such an inquiry when it receives information about the unlawful activity of the Services.

3.2.3 Investigation of complaints about the unlawful activity of the Services

Among the possible reasons for an inquiry, the Act handles separately the situation when the Committee receives a complaint in connection with the activity of the Services.

According to the Act, a complaint in connection with the national security investigation may refer to statements in the expert opinion which the person concerned considers untrue.[625] For the complainant, the National Security Act provides a two-level legal remedy process.[626] The first level is the Minister in charge of the Service which carried out the investigation, while the second level is the National Security Committee of the Parliament.

The Minister is obliged to conduct an investigation in the event of a complaint against the activities of the Services. The complainant must be informed about the findings of the inquiry and the measures taken. The requirements of the inquiry regarding form and content are not regulated by the Act.

Based on the authorisation of the Act, the Committee:

> ...*may conduct inquiries about complaints implying the illegal activities of the National Security Services, if the complainant does not accept the findings of the inquiry specified in paragraph 11(5), and the weight of the complaint, according to one third of the votes of the Committee members, justifies the inquiry; the Committee shall inform the person concerned about its findings.* [Paragraph 14(4)(c)]

In this way, the Act on the one hand binds the examination of the complaint to a condition (previous ministerial inquiry) but on the other hand makes it easier with the introduction of the one-third rule. The codification of this regulation is a guarantee to ensure that the inquiry into a complaint concerning the investigation conducted by a Service or the Minister may not be prevented by the governmental majority in itself.

The National Security Act does not give details of the procedure of the inquiry into complaints by the Committee, and neither does it describe the ministerial examination. The National Security Committee felt the urgent need to fill these deficiencies, at least concerning its own operation, only when the amount of the complaints significantly increased its workload.[627]

For the year 2009, the National Security Committee introduced a multi-stage procedure:

1. Members of the Committee may familiarise themselves with the complaint and may express a claim to familiarise themselves with the documents prepared by the Service concerned regarding the complainant.
2. If there is a demand for an inquiry into the complaint, the Chairman will propose to put it on the agenda of the next session. If the initiative earns the support of at least one-third of the members of the Committee, the examination begins.
3. The Minister as well as the complainant are invited to this session. They present their case and answer the questions of the members separately, one after the other, without hearing each other.

[625] Act No 125/1995, para. 72(3).
[626] Act No 125/1995, para. 72(3).
[627] During the parliamentary cycle of 2006–2010, the number of complaints started to increase rapidly. While in 2006 the Committee had no such case, in 2007 there were three; in 2008 already twelve complaints on its agenda. This amount caused a significant change of emphasis in the work of the Committee, which had an average of 20 sessions per year.

The Act leaves several other parts of the above process of the Committee unregulated. Contrary to the regulation of the ministerial examination, the Act does not determine a deadline for the examination.

3.2.4 Inquiry initiated by the Committee at its own discretion

The National Security Committee itself may notice a phenomenon which suggests the unlawful or inappropriate activity of a National Security Service, or on the basis of which the Committee may assume that such an activity is undertaken by a Service. Points (4)(d)(e)(f) in paragraph 14 of the Act apply to this case.

3.2.5 Ministerial inquiry initiated by the Committee

It is not necessary to deal with the inquiry defined in paragraph 14(4)(d) of the Act in detail when describing the tasks of the Committee because this type of examination is only initiated by the Committee. Conducting the examination and reporting on its findings are ministerial tasks.

3.2.6 Fact-finding inquiry

Paragraph 14(4)(e) of the Act gives a real authorisation to the Committee to conduct an inquiry. The prerequisite for this process—called a fact-finding inquiry by the Act—is that the Committee notices the unlawful operation of any of the National Security Services or that the Committee considers it necessary on the basis of a deficiency that a previous inquiry disclosed or failed to disclose. This type of former primary process may be an inquiry into a complaint by the Committee, a ministerial inquiry requested by the Committee or any unlawfulness reported to the Minister by a member of a Service which was investigated by the Minister and the Committee was informed about its findings.

Therefore if the Committee decides that it is justified to conduct a fact-finding inquiry, it means in fact that the Committee decides to conduct or repeat an examination in its own competence, although that would otherwise belong to the authority of the Minister or the Directors General. The scope of such an inquiry is, however, considerably wider than the traditional sphere of activity of the Committee. The reason why a fact-finding inquiry may be efficient is precisely the wide variety of measures, which allows the Committee to 'step over' the obligatory communication channels between the Committee and the Minister or between the Committee and the Director General. As it stands, in this procedure the Committee may make direct contact with the staff members of the Services (see 'hears the staff members of the National Security Services') and may look into the related documents of the Services.

After 12 years, the National Security Committee decided in the autumn of 2009 to initiate again a fact-finding inquiry. (We may presume that the Committee uses this measure very rarely since the fact of the initiation of such an examination already sends a message to the public that some grave anomaly has come to light in the activity of the Services). The subject of the inquiry launched in September 2009 was *Evaluation of the national security activity assisting the investigation into the serial murders of Romani persons.*

3.2.7 Example for fact-finding inquiry in connection with the serial murders of Romani persons

The circumstances and the way the inquiry was conducted shall probably serve as an example for a long time regarding the parliamentary control of the National Security Services. First of all, it is important to underline the well-organised, fast and efficient conduct of the inquiry. This may most certainly be explained by the fact that the Committee adopted a detailed plan of the examination right at the beginning. This examination plan (work plan) specified the purpose of the inquiry (matters to be examined), the deadline for the completion of the work, together with the intention that after the completion of the inquiry, the Committee would make a report about the work carried out to inform those concerned. To carry out the inquiry, the Committee set up a three-member working group, with members of different party affiliations. The group leader was authorised to act on behalf of the working group (to request documents, to call persons to hearings). Learning from negative experiences of the past[628] and to avoid controversy, the Committee specified that the working group could exercise its right to look into documents and call persons for hearings only on the location of the inquiry, i.e., in the buildings or branch offices of the National Security Services.

During the almost two months of the inquiry, the working group held formal hearings six times, which lasted for almost 18 hours, with the participation of 25 persons, ranging from the former and the acting Ministers to active and retired operational officers. During the examination, four institutions made several thousand pages of documents available to the acting representatives. Using its authority specified in paragraph 14(5) of the Act, the Committee asked a retired member of a National Security Service *to provide expert consulting*. On completion of the work, the Committee accepted the classified report of the working group which closed the inquiry and contained its main findings, as well as its short extract[629] that could be made public. Based on paragraph 14(4)(f) of the National Security Act, the report proposed some ministerial measures and further inquiry regarding responsibility.

In connection with the examination, there was a continuous fear that the whole process could result in discrediting the National Security Services in the eyes of the public. The experience, however, demonstrated that cases smelling of scandal gave considerable ammunition to the press but that on the whole, the examination of the cases had a reassuring effect on public opinion.

4. LIMITATIONS FOR THE COMMITTEE TO GAIN INFORMATION

Taking stock of the entitlements of the Committee to gain information, we must not avoid reflecting on the statutory constraints imposed on them. These limitations are necessary to understand the precise extent to which secrecy is essential for the efficient operation of the National Security Services. This secrecy is not absolute or inviolable because it is also necessary to satisfy another, somewhat contrary demand, namely the demand of the Parliamentary parties and the public, which laid its trust in them, for the external control of the Services. In an ideal situation, the national security risk caused by the insight would be counterbalanced by the legal security created by the control. As we have seen above, in order to create this balance the National Security Act places mainly obligations to provide

[628] Riba 1997.
[629] Fact-finding inquiry report 2009.

information on the side of the Services (and the Minister) who possess information, while it endows the Committee, which is 'outside the information circle', with a variety of means to request information. It is precisely these fields of obligations and entitlements whose borderlines are defined in paragraph 16 of the Act. According to this, the law protects the anonymity of persons cooperating with the Services, together with the ways the operational devices are used during the national security activity. These data are considered to be protected to such an extent that the Services cannot share them even with the controlling parliamentary Committee.

According to the Act, however, there is an exception to this restriction on data communication. It needs the agreement of two thirds of the members of the National Security Committee—i.e., a majority exceeding that of the ruling faction. In this case, the Committee has to decide with a qualified majority whether this data requirement concerning the method of internal information gathering is indispensable for the Committee to make its resolution concerning the unlawfulness.

5. SUMMARY

Act No 125/1995 on the Hungarian National Security Services deals mainly with the activities of the National Security Services but in its attitude is a step forward when compared with the former regulations that focused only on the efficiency of the Services. The main depositary of control is the National Security Committee, which possesses considerably more rights than a consultative parliamentary body. Its role as counterweight is guaranteed by such statutory provisions as the election of its Chairman from the parliamentary opposition, the extensive right of access to information, and the one-third decision about the acceptance of complaints or the possibility to carry out direct examinations. In the past one-and-a-half decades, the Committee has often proved that in its practice it is capable of finding answers to questions (expectations from the Chairman, inquiry into complaints, report on the findings of an examination) that are not regulated by the law.

Good practices in the parliamentary control of the Hungarian National Security Services are:

1. Considering that the National Security Services operate under the control of the government, the Chairman of the National Security Committee can only be a member of the opposition, to ensure tighter control.
2. The Committee may request information from the Minister and the directors general at any time, regarding any case that concerns the national security situation of the country or the operation of the Services.
3. If the Committee takes notice of the unlawful operation of the National Security Services, it can decide on initiating a fact-finding investigation, which gives it broad and direct authorisation of examination in relation to the Services.
4. In order to investigate a complaint about the unlawful activities of the Services, the Committee only requires the agreement of one-third of its members, providing that the complainant has previously filed their complaint with the Minister.
5. The Directors General of the Services are appointed by a complex process. The nomination for the position is made by the Minister in charge. The suitability of the candidate is decided by the National Security Committee. The subsequent appointment is within the competence of the Prime Minister.

Deficiencies in the Hungarian regulation are:

1. The Act does not set a deadline for the investigation or the refusal of complaints.
2. The National Security Committee is not obliged to report on its own activities or findings either to the plenary of the Parliament or to the public. Even if they do report in certain cases, e.g., following a more significant session or examination, the Committee is under no such regular obligation.

REFERENCES

Act No 125/1995 on the National Security Services

Fact-finding inquiry report ('Ténymegállapító vizsgálati jelentés') (17 November 2009), Evaluation of the Fact-finding Working Group of the National Security Committee about the national security service activity assisting the investigation of the serial murders of Romani persons, available at (http://www.parlament.hu/ internet/plsql/ogy_biz.keret_frissit?p_szerv=896).

Republic of Hungary (30 November 1994), Resolution No 46/1994 on the Standing Orders of the Parliament of the Republic of Hungary.

Riba I. (5 April 1997), 'Secret Service Scandal: Wood for a Birch Tree' ('Titkosszolgálati botrány: Nyirfától az erdőt'), *Heti Világgazdaság* No 14.

ANNEX A: COUNTRY CASE STUDIES

V. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN ITALY

FEDERICO FABBRINI & TOMMASO F. GIUPPONI*

1. INTRODUCTION: THE ITALIAN PARLIAMENTARY OVERSIGHT COMMITTEE (COPASIR)

The Italian legal framework for the oversight of intelligence agencies is provided by the recently enacted Law 124/2007.[630] This piece of legislation has overhauled the previous regime, based on Law 801/1977, reforming both the organisation of the intelligence agencies and the mandate and functions of the parliamentary oversight body. Law 124/2007 has preserved a separation between two intelligence agencies: AISI (*Agenzia Informazioni e Sicurezza Interna* or the 'Internal Information and Security Agency')—whose mandate is to gather intelligence inside the national borders (internally) and AISE (*Agenzia Informazioni e Sicurezza Esterna* or the 'External Information and Security Agency')—whose mandate is to gather intelligence outside the national borders (externally). Law 124/2007 has also explicitly provided that each intelligence agency can operate outside their sphere of functional/territorial competences only in cooperation with the other agency and pursuant to an explicit authorisation of the Executive Branch.[631]

Both AISI and AISE are coordinated by a special division set up within the executive branch—the Department of Security Intelligence (DIS). In addition, whereas under the previous legal framework the two agencies were under the control of the Ministry of Interior and the Ministry of Defence, on the basis of Law 124/2007 both AISI and AISE are now under the direct control of the Prime Minister,[632] or of the ad hoc Minister (or Secretary of State) to whom this task has been specifically delegated. Law 124/2007, therefore, has clearly centralised in the Prime Minister the power and accountability for the management of intelligence. Law 124/2007 has also replaced the Parliamentary Control Committee (COPACO) established by Law 801/1977 with a new Parliamentary Committee for the Security of the Republic (COPASIR), entrusted with more detailed and pervasive powers of oversight on the activities of intelligence agencies.

---

* The chapter follows the structure indicated in the DCAF – EUI terms of references.
Federico Fabbrini has written parts A to D and Tommaso F. Giupponi paragraphs E to H.
Federico Fabbrini is a PhD researcher in the Law Department at the European University Institute.
Tommaso F. Giupponi is Professor of Constitutional Law at the Faculty of Law, University of Bologna.

630 For a detailed assessment of the new Law 124/2007 enacted on August 3, 2007 [hereafter L.], see: Giupponi & Fabbrini 2010, p. 443.

631 L. Articles 6(4) & 7(4).

632 In the Italian constitutional system, the Prime Minister is the President of the Council since his primary task is that of coordinating the activity of the Council of Ministers. See: Barbera & Fusaro 2010, pp. 312.

2. THE GENERAL MANDATE AND FUNCTIONS OF COPASIR

The institutional task of COPASIR is to verify 'systematically and continuously that the activities of the intelligence agencies comply with the Constitution and the rule of law, in the exclusive interest of the defence of the Republic and its institutions'.[633] To this end:

1. COPASIR has a *control function*:[634] it shall review the activity of the DIS, AISI and AISE, subjecting the conduct of the Executive Branch in the field of security intelligence to parliamentary control.
2. COPASIR has an *advisory function*:[635] it needs to be consulted before the adoption by the Prime Minister of regulations concerning the organisation of the intelligence apparatus and before the appointment of the directors of the DIS, AISI and AISE.
3. COPASIR has a *warning function*:[636] it shall at all times inform the Prime Minister and the Presidents of the two chambers of Parliament if, in its oversight function, it identifies any irregularities by the intelligence agencies.
4. COPASIR has a *reporting function*:[637] it shall present a yearly report to Parliament to give information about the activities that were carried out and to formulate proposals on the issues of its competence.

In addition, in order to allow COPASIR to fully exercise its functions, Law 124/2007 makes COPASIR the addressee of several mandatory communications by the government.[638] The general budget of the DIS must also be submitted every six months to COPASIR to keep it informed of the financial management of the agencies. COPASIR, on the contrary, does not have a complaint function although nothing prevents it from activating its control powers after having received a communication or a complaint from members of the public or employees of the intelligence agencies.

3. PRACTICAL OVERSIGHT

Whereas the legal framework setting up the methods for oversight of the activities of the intelligence agencies is very detailed,[639] it is not easy to assess critically how COPASIR scrutinises a number of specific activities performed by the intelligence agencies. This is largely connected with the secrecy which characterises the internal functioning of COPASIR.[640] Also, the periodic reports that the government presents to COPASIR are undisclosed. The limited information that is available in this regard is derived only from the yearly reports that COPASIR presents to Parliament and from the short and summary minutes that COPASIR publishes on its website[641] after each meeting (reporting, e.g., what activities it has performed or who spoke).

[633] L. Article 30(2).
[634] L. Article 31.
[635] L. Article 32.
[636] L. Article 34.
[637] L. Article 35.
[638] L. Article 33.
[639] Cf. below part D.
[640] Cf. below part C.
[641] Italian Parliament website, 'Comitato parlamentare per la sicurezza della Repubblica: Competenze, composizione e funzionamento', available at (http://www.parlamento.it/bicamerali/43775/43777/43783/44438/paginabicamerali.htm).

i. *Information sharing*. Within the Italian intelligence apparatus, it is the task of the DIS to coordinate the activities of all intelligence agencies[642] and the sharing of information among them (as well as among them and the military, the regular police forces and other public administrations).[643] International information sharing, instead, is exercised by AISE. As indicated in the yearly reports, COPASIR often scheduled hearings with the Director of the DIS as well as with the Directors of AISE and AISI to ascertain the dynamics of cooperation between the agencies. However, it is impossible to assess whether during these hearings COPASIR was in the position to receive information about possible agreements concluded between the Italian and foreign intelligence agencies and to approve or reject them. From the data available on COPASIR's website,[644] it appears that from June 2008 to April 2011 COPASIR summoned the Director of the DIS 10 times, the Director of AISE 15 times and the Director of AISI 11 times. Interestingly, from the same data, it appears that COPASIR has also held meetings with the former US Secretary of State, Mr. Henry Kissinger, as well as with personnel of international bodies such as the EU Central Bank and the UN Interregional Crime and Justice Research Institute (UNICRI). The President and other member of COPASIR then participated in meetings with members of oversight bodies of other EU countries in 2009 and met with their US counterparts in 2010.

ii. *Processing and use of personal data*. In the report that the Prime Minister presents to COPASIR every six months, there must be information concerning the criteria for the processing of the personal data gathered by the intelligence agencies.[645] In addition, the data available on COPASIR's website[646] reveal that the Italian independent authority for the protection of personal data (set up in compliance with the EU Directive 95/46/EC) has been heard twice by COPASIR from June 2008 to April 2011 and that meetings have been set up in order to be briefed by the chief executive officers of the main telecom corporations operating within Italy.

iii. *Joint analysis and dissemination of information*. In the Italian legal framework, this task is also mainly exercised by the DIS, which conducts strategic analyses[647] and disseminates them among the intelligence community.[648] COPASIR often summons the Director of the DIS.[649] From the data available,[650] it appears that COPASIR periodically hears the Ministers of Interior, Foreign Affairs and Defence, which participate together with the Prime Minister and the Minister (or Secretary of State) delegated to intelligence affairs in the Inter-Ministerial Committee for the Security of the Republic (CISR)[651]—an advisory body whose purpose is to channel communication among the various intelligence and security forces. COPASIR also hears the Head of the Police, the General of the Carabinieri and the Commander of the Armed Forces, presumably to assess threats to national security and the strategic responses planned.

[642] L. Article 4(3)(a).
[643] L. Article 4(3)(c) & 4(3)(e).
[644] Cf. the data available at: (http://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/STENO_CRONO.pdf).
[645] Cf. below part D(a).
[646] See note 15 above.
[647] L. Article 4(3)(d).
[648] L. Article 4(3)(f).
[649] Cf. below part D(c).
[650] See note 15 above.
[651] L. Article 5.

iv. *Collection of open source information*. No data appears to be available on this activity.

v. *Finance of intelligence agencies.* COPASIR mainly exercises an ex post review of the financial management of the intelligence agencies. In the periodic reports of the Prime Minister, information is provided on the budget assigned to the DIS, AISE and AISI during the previous six months and on its use.[652] The Prime Minister also informs COPASIR about the allocation of resources (or variation in the allocation of resources) assigned to ordinary and secret budgets.[653] COPASIR, in addition, can always review the documentation concerning expenditures for intelligence operations archived by the DIS.[654] COPASIR, however, does not have any a priori control on the resources assigned the intelligence apparatus, which is provided by the yearly budgetary law.[655] Pursuant to an explicit constitutional provision, the budgetary bill, drafted by the Minister of the Treasury, needs to be approved yearly by Parliament first in the budget committee and then in chamber, which can reallocate the resources or set up new expenses by providing the financial means to cover them.[656] De facto, the dynamics of the parliamentary system make it extremely difficult for Parliament to modify the budgetary bill presented by the government and there is no evidence that Parliament has ever attempted to modify the intelligence budget. Moreover, the budgetary bill only specifies the resources allocated to the intelligence apparatus in their aggregate amount,[657] leaving then to the Prime Minister, after hearings with the Directors of the DIS, AISI and AISE, to decide how to reallocate the budget among the agencies and whether to allocate funds in secret budgets.[658] A judicial review of the financial management of the budget for the intelligence agencies is instead exercised by a special division of the Court of Auditors, set up within the DIS.[659]

4. COMPOSITION AND SET UP

COPASIR is composed of five Deputies (i.e., members of the lower chamber of Parliament) and five Senators (i.e., members of the higher chamber of Parliament) appointed within twenty days from each general election by the Presidents of the two chambers of Parliament.[660] Each parliamentary group is allotted a number of seats in COPASIR proportional to its size: however, 'bearing in mind its specific functions',[661] COPASIR can ensure the equal representation of both the members of the majority party or coalition parties in Parliament and of the opposition party or coalition parties. In addition, to guarantee a meaningful involvement of the minority party and an effective check on the

[652] L. Article 33(8).
[653] L. Article 29(2).
[654] L. Article 31(13).
[655] L. Article 29.
[656] Cf. Government of Italy 1947 [hereafter Const.] Article 81. For an assessment of the procedures for the approval of the budgetary law cf. also Barbera & Fusaro 2010, p. 273.
[657] L. Article 29(1).
[658] L. Article 29(2).
[659] L. Article 29(3)(c).
[660] Note that in the Italian parliamentary system, both chambers of Parliament (the House of Representatives and the Senate) are directly elected by nation-wide popular suffrage and perform exactly the same functions. The Senate, however, has higher age requirements as electors need to be above 25 years of age and candidates above 40 years of age. In addition, seats for the Senate are allocated on a regional basis. Cf. Barbera & Fusaro 2010, p. 253.
[661] L. Article 30(1).

activity of the government, Law 124/2007 requires the President of COPASIR to be chosen among the members of the opposition.[662]

The President of COPASIR is elected among the members of COPASIR by absolute majority with a secret ballot. If no candidate reaches this threshold at the first ballot, a second turn is provided between the two candidates who have obtained the majority of the votes. In case of a further tie, the elder candidate is elected President. The President of COPASIR is assisted by a Vice-President and a Secretary General, who are also elected by majority vote by the members of COPASIR. The three compose the COPASIR's Presidency Office. To perform its tasks, COPASIR uses the premises and the administrative personnel assigned to it by the Presidents of the two Chambers of Parliament. The costs and expenditures of COPASIR are entirely covered by the annual internal budget of Parliament.[663]

The functioning of COPASIR is set up by an internal regulation,[664] which integrates the provisions of Law 124/2007 and may be modified by COPASIR with an absolute majority vote.[665] The President represents COPASIR, convenes its meetings and chairs them.[666] The President decides the working days on which COPASIR meets and sets the items on the agenda.[667] For its operation, COPASIR requires the participation of six members.[668] Deliberations are adopted by simple majority vote: in case of a tie vote, the deliberation is rejected.[669] The Secretary verifies the result of the votes and drafts the minutes of the meeting.[670] Nevertheless, the meetings, the decisions and all the acts of COPASIR are secret unless COPASIR decides otherwise.[671] Only a summary report of the activities of COPASIR is published on the COPASIR website. Members of COPASIR are bound by a strict duty of secrecy, the violation of which may be liable to prosecution.[672]

Since the mandate of COPASIR tracks the mandate of Parliament (i.e., a maximum five years)[673] the members of COPASIR have only a limited period of time to acquire expertise in the field of intelligence oversight. Otherwise, the frequent turn-over among the members of COPASIR due to reasons of party politics, makes continuity of service even more difficult. As a matter of fact, this does not seem to be perceived as a problem by the relevant institutional actors. By the same token, no specific step appears to have been taken to ensure that the staff permanently assigned by the Presidents of the two Chambers of Parliament to COPASIR be adequately prepared for the task of intelligence oversight. It is not possible, however, to make an accurate assessment of the know-how and professional qualifications of the personnel of COPASIR.

[662] L. Article 30(3).
[663] L. Article 37(5).
[664] Government of Italy 22 November 2007 [hereafter Reg.].
[665] L. Art 37(1) & Reg. Art. 16
[666] Reg. Article 4(1).
[667] Reg. Article 5(1).
[668] Reg. Article 7(1).
[669] Reg. Article 7(2).
[670] Reg. Article 4(3).
[671] L. Article 37(2) & Reg. Article 8.
[672] L. Article 36.
[673] Cf. Const. Article 60.

5. METHODS OF OVERSIGHT

COPASIR exercises its oversight function through several methods, which are specifically provided by Law 124/2007:

a. *Examining reports*. Every six months, the Prime Minister must submit to COPASIR a report on the activities of the intelligence agencies, including a strategic assessment of threats to national security and the responses planned.[674] All regulations concerning the intelligence agencies adopted by the Prime Minister and the Ministers of Interior and Defence must be communicated to COPASIR. COPASIR must be informed within 30 days of any special operation by the intelligence agencies in which the authorisation to commit an unlawful act has been granted by the Chief Executive.[675] The Prime Minister must then swiftly inform COPASIR of any decision to invoke the State secret privilege in court,[676] as well as of the handling of personal data acquired in the gathering of intelligence.[677]

b. *Scrutinising the budget*. COPASIR may directly review the expenditures relating to the special operations of the intelligence agencies by accessing the archive of the DIS.[678] Every six months, the Prime Minister shall inform COPASIR about the management of the budget allocated to the intelligence apparatus during the previous six months.[679] This includes a summary, based on a homogeneous typology of expenditures, of the budget for the DIS, AISI and AISI and of its employment.[680]

c. *Holding hearings*. Periodically, COPASIR summons the Prime Minister, the Minister or Secretary of State delegated to intelligence affairs, the Ministers of Interior, Foreign Affairs, Justice and Defence and the Directors of the DIS, AISI and AISE.[681] It may also hear individuals, who are not members of the intelligence apparatus but may provide useful information for its oversight function.[682] Finally, COPASIR can exceptionally decide to summon intelligence officers: this requires, however, the prior consent of the Prime Minister, who can oppose the request for justified reasons.[683] From the data available, in any case, it appears the COPASIR has never made use of this possibility in the past. All individuals heard by the COPASIR 'shall refer, in a complete and faithful way, the information they have concerning issues of interest to the [COPASIR]'.[684]

[674] L. Article 33(1).
[675] L. Article 33(4). Note that pursuant to L. Article 17(6), the Prime Minister may specifically authorise intelligence agents to commit unlawful acts shielding them from prosecution if (and only if) the illicit acts: 'a) are committed either in the exercise of or because of the institutional tasks assigned to intelligence agencies for the purpose of ensuring the realization of a duly documented operation; b) are indispensable for the achievement of the results of an operation, proportionate to the end and if no alternative means existed; c) are the result of an appropriate balancing between the private and public interests involved; d) produce only the least possible damage to the private interests that were infringed'. For a detailed assessment of the functional guarantee set up by Law 124/2007 to shield intelligence agents from investigation in specifically tailored hypothesis cf. Giupponi & Fabbrini 2010 p. 449.
[676] L. Article 33(5).
[677] L. Article 33(9).
[678] L. Article 31(13).
[679] L. Article 33(7).
[680] L. Article 33(8).
[681] L. Article 31(1).
[682] L. Article 31(3).
[683] L. Article 31(2).
[684] L. Article 31(4).

d. *Requesting documents*. COPASIR can acquire documents from the judicial authority, even derogating from the ordinary rules of the Code of criminal procedure.[685] The judiciary, however, may postpone the disclosure of the requested documents for reasons relating to the secrecy of investigations. COPASIR, then, can acquire documents directly from the intelligence agencies.[686] Nonetheless, disclosure can be opposed when it could 'jeopardize the security of the Republic, the relationship with foreign States, the course of ongoing operation or the security of sources of information and agents of the secret services'.[687] If COPASIR insists on the disclosure of these documents by deeming the refusal unjustified, a special decision has to be taken by the Prime Minister who can resort to the State secret privilege. In any case, no refusal to disclose documents can be made to COPASIR when the latter, by unanimous decision, is investigating institutional misconduct by intelligence officers.[688] When COPASIR deems a decision of the Prime Minister unwarranted, however, it can only raise the issue before Parliament for consequential political evaluation,[689] following a 'traditional' logic of parliamentary control whose effectiveness, however, is rather uncertain.[690]

e. *Accessing premises*. COPASIR can access and make inspections of premises and buildings which belong to the intelligence apparatus.[691] The Prime Minister needs, however, to be informed beforehand and he can postpone access when this might interfere with ongoing operations.[692]

f. *Thematic studies*. COPASIR can prepare and present to Parliament thematic studies on issues of particular relevance for national security. From the data available, it appears that COPASIR has presented three such reports to Parliament:[693] the first concerning the problem of the acquisition by local offices of the public prosecutor sensitive data regarding intelligence officers and the lack of destruction thereof (delivered on February 13, 2009); the second dealing with human trafficking (delivered on April 29, 2009); and the third concerning the possible national security threat generated by cyber crime (delivered on July 15, 2010).

6. INVESTIGATIVE POWERS AND ACCESS TO INFORMATION

Law 124/2007 has created an Office of the Inspector General within the DIS to ensure the continuous internal review of the activities of the intelligence agencies and with the power to undertake, subject to the authorisation of the Prime Minister, internal investigations of possible misconduct by officers of the intelligence agencies.[694] Nevertheless, no specific data are available on this issue, since the composition, the internal organisation and the operational tasks of the Office of the Inspector General within the DIS are regulated by two decrees enacted by the Prime Minister which are currently classified.[695]

[685] L. Article 31(5).
[686] L. Article 31(7).
[687] L. Article 31(8).
[688] L. Article 31(9).
[689] L. Article 31(10).
[690] Cf. further Giupponi & Fabbrini 2010, p. 456.
[691] L. Article 31(14).
[692] L. Article 31(15).
[693] Cf. below part G.
[694] L. Article 4(3)(i).
[695] Cf. Decree of the Prime Minister of August 1, 2008 and Decree of the Prime Minister of June 12, 2009.

Besides the internal review of the Office of the Inspector General, a further external review on the activity of the intelligence agencies is exercised by COPASIR.[696] It is within the purview of COPASIR[697] to commence specific investigations to ensure that the conduct of intelligence officers conforms to the institutional tasks assigned to AISE and AISI.[698] The power of COPASIR to activate an investigation, however, is subject to the general rule that requires any decision by COPASIR to be adopted by a majority vote of the members present and no specific rule is in place to allow a minority in COPASIR to activate an investigation.[699] In addition, as mentioned,[700] when COPASIR has decided by unanimous decision to exercise its investigative powers, the Prime Minister cannot invoke the State secret privilege or assert other reasons of confidentiality to prevent COPASIR from accessing relevant documents and information.

Having said this, because of the secrecy that surrounds the internal activities of COPASIR,[701] there are no data available concerning the effective exercise by COPASIR of its investigative powers. The only data are those contained in the yearly report that COPASIR presents to Parliament,[702] which may be evaluated both by the legislature and by the public at large. Equally, it is impossible to ascertain whether COPASIR has requested access to information from the intelligence apparatus or the public administration and the judiciary more generally. From the analysis of the yearly reports presented by COPASIR in 2009 and 2010,[703] it can be understood that COPASIR has sought further clarifications from other institutional actors on specific critical issues and reported to Parliament about them: for instance in 2009, COPASIR released a report on the problems created by the acquisition by a local Office of the Public Prosecutor of sensitive data regarding intelligence officers.[704]

From the data currently available, it appears that COPASIR has never officially informed the Prime Minister or the Presidents of the two chambers of Parliament about possible misconduct committed by intelligence officers, which it might have discovered during its review.[705] Nothing excludes the possibility, however, that COPASIR has made such warnings in an informal and confidential way, either during or after its oversight functions.

7. PROTECTION OF INFORMATION BY OVERSIGHT BODIES

Since COPASIR, in the exercise of its functions, has to handle sensitive information, Law 124/2007 has codified a specific duty for all the members of COPASIR to maintain secret all information they obtain.[706] In addition, a duty of non-disclosure binds all persons who, by reason of their office or job (e.g., the administrative personnel of COPASIR), gain knowledge of information or activities about COPASIR. The prohibition to disclose information persists even after the termination of the office or of the professional collaboration. Law 124/2007 allows COPASIR to resort to collaboration with external personnel, where a specific professional and technical expertise is needed for the

[696] For a further assessment of the differences between the internal administrative review exercised on the activities of the intelligence agencies by the Office of the Inspector General within DIS and the external political review exercised by COPASIR (as well as the external review by the judiciary) cf. Giupponi & Fabbrini 2010, p. 453.
[697] Cf. above part D.
[698] L. Article 31(9).
[699] Cf. above part C.
[700] Cf. above part D(d).
[701] Cf. above part C.
[702] Cf. above part G.
[703] Ibid.
[704] Cf. COPASIR 2009.
[705] Cf. above part A(3).
[706] L. Article 36(1).

performance of its functions.[707] However, external personnel are also bound by the duty of secrecy, even after the termination of the professional collaboration.[708]

If a violation of the non-disclosure duties occurs, the President of COPASIR is legally required to denounce the fact to the judicial authorities,[709] which shall prosecute the suspected person for the crime of disclosure and use of secret information, codified in Art. 326 of the Criminal code.[710] From the data available from June 2008 to April 2011, however, it appears that the President of COPASIR has never denounced such a violation. If the violation of the non-disclosure duties is made by a member of COPASIR, not only the sentencing can be increased[711] but also a special, parallel parliamentary procedure shall be opened as an ad hoc investigation committee, composed in equal numbers by parliamentarians of the majority and of the opposition.[712] If the investigation reveals a responsibility of a parliamentarian in the disclosure of the information, the President of the chamber of Parliament to which the said parliamentarian belongs shall dismiss him/her from COPASIR and replace the individual with another parliamentarian of the same political group.[713]

To foster the confidentiality of the activities of COPASIR, Law 124/2007 requires all meetings of COPASIR to remain secret unless COPASIR decides otherwise.[714] As mentioned,[715] for each meeting COPASIR discloses only the items on the agenda but the detailed minutes remain secret.[716] The acts and documents acquired by COPASIR are archived as confidential if the administration that produced them had decided so.[717] The acts and documents produced by COPASIR itself, instead, can be disclosed if COPASIR decides this.[718] All acts and documents received, acquired or produced by COPASIR are stored in a special archive, which is organised according to the level of confidentiality of each document.[719] Members of COPASIR and, with a previous authorisation, external collaborators may access this archive;[720] but they may not pull out documents from it (except when the document is already public).[721]

8. REPORTING BY OVERSIGHT BODIES

Law 124/2007 requires COPASIR to present each year to Parliament a report on the activities that were carried out and containing specific recommendations and warnings.[722] The two yearly reports released since the establishment of COPASIR (published on July 30,

[707] L. Article 37(5) & Reg. Article 15.
[708] Reg. Article 15.
[709] L. Article 36(4) & Reg. Article 11.
[710] Cf. Criminal Code Article 326: 'The public official or the person exercising a public service, who, by violating the duties inherent to his/her function or service or otherwise abusing his/her qualification, discloses information which must remain secret or otherwise aides such disclosure shall be punished with six months to three years imprisonment. If the aid in the disclosure is not voluntary, he/she shall be punished to up to one year imprisonment. The public official or the person exercising a public service who, to obtain an economic advantage, uses information which must remain secret shall be punished with two to five years imprisonment. If the use of secret information is made to obtain a non economic advantage or to unlawfully damage others, he/she shall be punished with up to two years imprisonment'.
[711] L. Article 36(2) & Reg. Article 11.
[712] L. Article 36(6) & Reg. Article 11.
[713] L. Article 36(7).
[714] L. Article 37(2) & Reg. Article 8.
[715] Cf. above part C.
[716] Reg. Article 8(4).
[717] L. Article 37(3).
[718] Reg. Article 12.
[719] Reg. Article 14.
[720] Reg. Article 14 (3).
[721] Reg. Article 14 (4).
[722] L. Article 35(1).

2009 and July 29, 2010) contain detailed information and represent the most relevant instruments to assess the activities of COPASIR. Reports are structured thematically and include a summary of: a) the general oversight activities that were undertaken; b) the opinions that were delivered; c) the issues that were addressed through specific thematic studies; d) the status of the State secret privilege and its assertion by the government.

Besides the yearly report to Parliament, COPASIR can discretionally decide to approve and present to Parliament other reports on specific thematic issues that COPASIR considers of compelling relevance for national security.[723] From the data available, it appears that COPASIR has presented three such reports to Parliament:[724] the first concerns the acquisition of sensitive data regarding intelligence officers and the lack of destruction thereof by local Offices of the Public Prosecutor (delivered on February 13, 2009);[725] the second dealing with human trafficking (delivered on April 29, 2009);[726] and the third concerning the possible national security threat generated by cybercrime (delivered on July 15, 2010).[727]

The public reports that COPASIR presents to Parliament highlight the direct and privileged relationship between the two institutions. As already mentioned, however, COPASIR has many exchanges of information with the government and the intelligence apparatus (DIS, AISE, AISI) in the exercise of its institutional functions.[728] As the law now stands, it does not seem that COPASIR has any involvement in the governmental decisions concerning the declassification of secret information. As indicated,[729] however, COPASIR can decide the disclosure or classification of the documents that it has itself generated.

9. GOOD PRACTICES

The analysis of the role of COPASIR as the parliamentary body which oversees the activities of Italian security and intelligence agencies highlights several positive features, although a major (and perhaps largely unavoidable) hurdle is represented by the difficulties in accessing data and information which is often classified or secret. These limitations notwithstanding, the assessment of the two yearly reports presented so far underlines a positive trend. The choices of legislative drafting made by Law 124/2007 look particularly significant in this regard. This Law, contrary to Law 801/1977, provides a detailed and precise regulation of the powers, activities and functions of COPASIR. As the data available in the yearly reports reveal, this carefully drafted regulatory framework has allowed COPASIR to effectively review the activity of the intelligence agencies.

Nevertheless, as the new legislative regulation has only recently entered into force, it seems necessary to acknowledge that the role of COPASIR is still a work in progress: as such, it is too early to identify in the Italian system of parliamentary oversight consolidated and precise good practices which can be taken as a model in comparative perspective. From this point of view, perhaps, the best practice that can be identified in the Italian legal regime for the oversight of intelligence agencies is the definition of a clear and precise regulatory framework for the exercise of power by COPASIR.

[723] L. Article 35(2).
[724] Cf. above part E.
[725] See note 75.
[726] Cf. COPASIR 2009.
[727] Cf. COPASIR 2010.
[728] Cf. above parts B & D.
[729] Cf. above paragraph F.

REFERENCES

Barbera A. And C. Fusaro (2010), *Corso di diritto pubblico*, Il Mulino, Bologna.

Campanelli G. (2007), 'Commento agli Artt. 30–38 della L. 3.8.2007 n. 124', *Legislazione penale*, No 4.

COPASIR (2010), Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico, available at (http://www. parlamento.it/service/PDF/PDFServer/DF/234494.pdf).

COPASIR (2009), RELAZIONE SUI RISCHI PER L'EFFICIENZA DEI SERVIZI DI INFORMAZIONE PER LA SICUREZZA DERIVANTI DALL'ACQUISIZIONE E MANCATA DISTRUZIONE DI DATI SENSIBILI PER LA SICUREZZA DELLA REPUBBLICA, available at (http://www.parlamento.it/documenti/repository/commissioni/ bicamerali/COMITATO%20SICUREZZA/34-1.pdf).

Gambacurta S. (2008), 'Il sistema dei controlli—Il controllo parlamentare' in Mosca C., Gambacurta S., Scandone G. And M. Valentini (eds.), *I servizi di informazione e il segreto di Stato*, Giuffrè, Milan.

Giupponi T.F. (2010), 'La riforma del sistema di informazione per la sicurezza della Repubblica e la nuova disciplina del segreto di Stato' in Illuminati G. (ed.), *Nuovi profili del segreto di Stato e dell'attività di intelligence*, Giappichelli, Turin.

Giupponi T.F. and F. Fabbrini (2010), 'Intelligence Agencies and the State Secret Privilege: the Italian Experience', *International Constitutional Law Journal*, No 3.

Government of Italy (22 November 2007), *Regulations of the Parliamentary Committee for the Security of the Republic (COPASIR)*, available at (http://www. sicurezzanazionale.gov.it/web.nsf/documenti/Regolamento_Copasir.pdf).

Government of Italy (3 August 2007), *Law No 124/2007*, available at (http:// www.sicurezzanazionale.gov.it/web.nsf/documenti/law_124_2007.pdf).

Government of Italy (27 December 1947), *La Costituzione della Repubblica Italiana*, available at (http://www.sicurezzanazionale.gov.it/web.nsf/documenti/ Costituzione.pdf).

Italian Parliament website, 'Comitato parlamentare per la sicurezza della Repubblica: Competenze, composizione e funzionamento', available at (http://www.parlamento.it/bicamerali/43775/43777/43783/44438/paginabicamerali.htm).

Nardone C. (2008), 'Il controllo parlamentare sui servizi di informazione e sicurezza e sul segreto di Stato' in Dickmann R. Ans S. Staiano (eds.), *Funzioni parlamentari non legislative e forma di governo. L'esperienza dell'Italia*, Giuffrè, Milan.

ANNEX A: COUNTRY CASE STUDIES

VI. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE NETHERLANDS

NICK VERHOEVEN[730]

1. INTRODUCTION

Pursuant to the Dutch Intelligence and Security Services Act 2002, the Netherlands has two intelligence and security services: the General Intelligence and Security Service (GISS) and the Defence Intelligence and Security Service (MISS).[731] The core business of both services consists of processing information— for example, collecting and disseminating information. This sets them apart from other more executory or coordinating services, such as the police or the National Coordinator for Counterterrorism (NCTb). Another important characteristic of the intelligence and security services is the use of surreptitious powers that invade personal privacy. The services use such powers to collect information. In the Netherlands, a distinction is made between intelligence collection and criminal investigation. When the police use special powers in the course of an investigation, this leads to criminal proceedings and is subject to review by the courts; this is not the case for intelligence collection. Consequently, oversight of the activities of intelligence and security services is necessary.

Since the terms of reference for this chapter include an express request to leave out the military component, I will only deal with the oversight of GISS, the Dutch civil intelligence and security service.

2. THE OVERSIGHT BODIES

Oversight in the Netherlands is exercised by parliament as well as specialised bodies. One of these specialised bodies, the Intelligence and Security Services Review Committee (CTIVD), has even been established specifically to exercise oversight over the intelligence and security services.

2.1 Parliamentary oversight

The Dutch Parliament is composed of a First Chamber and a Second Chamber.[732] The First Chamber (the Senate) does not exercise (direct) oversight over the activities of GISS.

Two committees in the Second Chamber are concerned with the oversight of GISS: the Committee on the Intelligence and Security Services (ISS Committee) and the Committee on Home Affairs and Kingdom Relations (Home Affairs/KR Committee).[733]

[730] Nick Verhoeven is the Secretary of the Intelligence and Security Services Review Committee (Dutch abbreviation: CTIVD) in the Netherlands.
[731] Intelligence and Security Services Act 2002, Sections 1a, 6 and 7.
[732] Act on the constitution of the Kingdom of the Netherlands 1815, paragraph 3.
[733] *Rules of Procedure of the Second Chamber 1994*, Sections 16 and 22.

The ISS Committee is constituted of the chairpersons of all the political parties represented in the Second Chamber.[734] This is the only standing parliamentary committee which is authorised to discuss matters involving state secrets. Yet the members of this committee are not screened. This is an exception to the statutory rule on the handling of state secret information: normally speaking, access to state secret information is restricted to persons having security clearance, which is given to persons who have successfully passed security screening.[735] In the Netherlands, however, it is considered incompatible with the principle of the separation of powers to screen members of the ISS Committee, and so they are not screened. Members of the ISS Committee affirm that they will observe confidentiality; this is the (sole) guarantee that the matters discussed in the committee will not be shared with non-members. The meetings of the ISS Committee are closed. The Committee does, however, render account for its activities in a public annual report.

The Home Affairs/KR Committee is constituted of the subject experts of all the political parties represented in the Second Chamber. This Committee does not discuss matters involving state secrets. Its meetings with the Minister are public. The Home Affairs/KR Committee addresses matters falling under the responsibility of the Minister of Home Affairs and Kingdom Relations: these include GISS but also matters such as the integrity of public administration and democracy. The Committee has the same powers.

Both Committees derive their mandate from the Constitution and more specifically from the Rules of Procedure of the Second Chamber. Both have authority to exercise parliamentary oversight of GISS, in principle over all aspects: efficiency, effectiveness, lawfulness and budget. In practice, the oversight primarily handles general issues.

Both committees can ask the Minister concerned to provide all documents it deems necessary to examine in order to discharge its duties. It may also consult with a Minister either orally or in writing, or convene a round-table meeting. In addition, the Committees may hold hearings, make working visits, obtain information from advisory bodies, engage external experts or propose to the full Lower House to designate a large project.[736]

The abovementioned means that the Home Affairs/KR Committee takes the lead in the parliamentary oversight of GISS. The guiding principle, and a gentlemen's agreement between government and Parliament, is that as far as possible all matters are dealt with by the subject experts of the parliamentary groups. The ISS Committee is only brought in for matters unsuitable for being discussed in public. Consequently, the public annual report of GISS and its public reports are considered in the Home Affairs/KR Committee. The same applies to matters concerning GISS that have attracted media attention. And lastly, the public reports of the specialised oversight body CTIVD (see the next section) are discussed in the first place by the ISS Committee.

In 2004, the Committee for the Administrative Evaluation of GISS, established by order of the Minister of the Interior and composed of specialists, issued a study report which not only dealt with the functioning of GISS but also how it was directed and supervised.[737] The report concluded that even though the ISS Committee was a useful, confidential link between GISS and the Second Chamber, it hardly got around to an in-depth debate on the functioning of the service. It is generally recognised that this is partly due to the busy

[734] *Rules of Procedure of the Second Chamber 1994*, Section 16 (2).
[735] Security Screening Act 1996.
[736] *Rules of Procedure of the Second Chamber 1994*, chapter 7, paragraph 5.
[737] Havermans 2004.

agendas of the chairpersons of the political groups in parliament and the fact that they are not specialists in the field of intelligence and security services.

The two parliamentary committees in practice do not carry out investigations of their own and do not issue reports.

2.2 Other oversight bodies

2.2.1 The CTIVD

The Intelligence and Security Services Review Committee (CTIVD) is the main specialised oversight body of GISS. It was established by statute (ISS Act 2002). The CTIVD is an independent government body whose main task is to review whether the ISS Act 2002, the law pertaining to the activities of GISS (and DISS), is implemented lawfully.[738] The scope of this task not only covers the activities of GISS but also those of officers of other services who perform tasks for GISS pursuant to Article 60, ISS Act 2002. These are the Regional Intelligence Services which form part of the police force, the Tax and Customs Administration, the Fiscal Information and Investigation Service, the Customs, and the Royal Netherlands Military Constabulary.

The CTIVD has three members, working part-time, one of whom acts as chairperson. Members are appointed after an extensive procedure, laid down in Article 65, ISS Act 2002. A group of three individuals selected from the highest spheres of the judiciary and the public service announce a vacancy and prepare a list containing at least three candidates. This serves as a list of recommendation to the Second Chamber, which may take it into account insofar as it deems it useful to do so. The Second Chamber may adopt the list, change the order of recommendation or reject the list and take the procedure in hand itself. The Second Chamber prepares a list of three persons and sends it to the ministers concerned, namely the Prime Minister, the Minister of Home Affairs and Kingdom Relations and the Minister of Defence. After the ministers have agreed on a candidate, he or she is referred to GISS for a security screening. When the result of the security screening is positive, the person can be appointed. So the judiciary, the legislature and the executive are all represented in the procedure. This arrangement was chosen in an attempt to embed the independent nature of the committee in the appointment procedure.

The CTIVD has a secretariat (Section 69, ISS Act 2002), which provides substantive support to the Committee. At present the secretariat is composed of a secretary and four investigators. They, too, have all been security screened. Since the CTIVD concentrates on lawfulness, it is not surprising that the Committee is made up predominantly of qualified lawyers. Article 65(4), ISS Act 2002, even requires that two of the members be qualified lawyers. In practice, all investigators have been qualified lawyers so far.

The CTIVD has an annual budget of around a million euro.

The CTIVD has several tasks. Its main task is that of reviewing whether the ISS Act 2002 and the Security Screening Act are implemented lawfully, in other words: oversight of the activities of GISS and DISS. So its oversight does not cover the efficiency and effectiveness of the services' activities. In practice, the CTIVD performs its oversight task in two ways: it conducts in-depth investigations resulting in review reports that are made public, and it monitors a number of activities of the services. In addition to its main task, the CTIVD also has an advisory task: it can give advice to the ministers concerned, both on request and on

[738] Intelligence and Security Services Act 2002, Section 64 (2).

its own initiative. This task is not limited to lawfulness alone. Finally, the CTIVD has the task of advising the ministers on complaints relating to the conduct of GISS or DISS. In this case, it acts as an internal complaints advisory committee within the meaning of Article 9:15(4) of the General Administrative Law Act and assumes the task of dealing with the substance of the complaint. The advice of the CTIVD is sent to the Minister, but ultimately the Minister gives an independent decision on the complaint. If the Minister does not adopt the advice of the CTIVD, s/he must enclose the advice when sending his/her decision to the complainant. If the complainant disagrees with the decision given by the Minister, he or she may lodge the complaint once again, this time with the National Ombudsman (see section 2.2.2). The CTIVD handles about 10–15 complaints each year, of which the lot are manifestly ill-founded.

The CTIVD has been given far-reaching statutory powers for the purposes of performing its main review task (Sections 74 through 77, ISS Act 2002). For example, the CTIVD has access to all relevant (state secret) information of the services and it may hear all employees of the services, who are then required to give the CTIVD all the relevant information. There are no restrictions in this area. Furthermore the CTIVD has power to hear witnesses under oath and to summon expert witnesses. Finally, it has the authority to enter any and all places when it deems it necessary, except dwellings.

Whenever the CTIVD has conducted an in-depth investigation, it prepares a review report based on this investigation (Section 79, ISS Act 2002). The report must in any case comprise a public part and sometimes it also has a secret part. Both parts are drawn up by the CTIVD and sent to the minister concerned, the Minister of Home Affairs/KR in the case of GISS. The minister may then send his comments on the report to the CTIVD, stating among other things whether the public part of the report contains passages that ought not to be made public. The CTIVD incorporates the minister's comments at its discretion and subsequently adopts the report, which is then again sent to the minister. The minister must forward the report, with an accompanying note, to both chambers of parliament within six weeks. The minister sends the secret part to the aforementioned Parliamentary ISS Committee, under strict confidentiality. The CTIVD publishes the public parts of the reports on its website. The CTIVD also issues a public annual report, in which it reports on its activities. Generally the reports are of a juridical nature and cover the theoretical framework involved, the facts and conclusions and recommendations. The CTIVD tries to say as much as possible in the reports, and has set its own rule that irregularities will always be mentioned, however brief or abstract, in the report itself and not only in the secret part. The CTIVD publishes 2–4 reports each year.

The CTIVD also conducts (systematic) monitoring activities. These include official messages, telephone taps, signals intelligence, security screenings, applications for inspection of files and the obligation to notify. The monitoring is done by random inspections. In this way the CTIVD obtains a picture of the key activities of the services. The monitoring findings do not result in a report to parliament, but they can lead to the CTIVD writing a letter to the GISS or starting an in-depth investigation.

Since the CTIVD both receives and produces state secret information, it has an office of its own at its disposal which fully satisfies the highest security standards. The CTIVD, among other things, makes use of fingerprint access, a secure internal network and a vault. It also has a secured connection with GISS and has its own workspace and computers at the service. There, the CTIVD has direct access to the digital system of GISS.

2.2.2 To complete the picture: non-specialised oversight bodies

A number of organisations exercise some form of oversight of GISS with regard to specific aspects. These organisations do not focus on GISS only but on public bodies in general.

Oversight of the financial aspect of the activities of GISS in a broad sense is exercised by the Netherlands Court of Audit and the National Audit Service. The Court of Audit has the power to check whether revenue and expenditure are balanced and in addition has the duty of reviewing whether policies are implemented as intended. In doing so, it may also scrutinise state secret information. The duties and powers of the Court of Audit are laid down in the Government Accounts Act 2001. The National Audit Service is part of the national government and can do audits of a more financial nature. Both agencies have a number of employees who have been screened specifically for doing this work. Both the Court of Audit and the National Audit Service may issue public reports. The audits are done yearly. The last specific report about the GISS however dates from before the ISS Act of 2002.

The National Ombudsman deals with complaints from citizens and can make non-binding recommendations based on its investigation. A person having a complaint about GISS must first lodge the complaint with the Minister of Home Affairs/Kingdom Relations, who will call in the CTIVD in its capacity as complaints advisory committee. If the complainant disagrees with the Minister's decision on the complaint, he or she can lodge the complaint once again, this time with the National Ombudsman. The latter has the power to inspect state secret documents in the possession of the service. A number of employees of the National Ombudsman have been screened for this purpose. The activities of the National Ombudsman are based on the National Ombudsman Act.

3. OVERSIGHT ON THE PROCESSING OF INFORMATION

3.1 Information processing

3.1.1 General

As was stated in the introduction, processing information is the core business of any intelligence and security service. The ISS Act 2002 does in fact acknowledge this. Pursuant to Article 1.f of the Act, processing information covers just about everything that can be done with information: 'any action or any set of actions regarding information, including in any case collecting, recording, arranging, storing, updating, altering, retrieving, consulting or using information, providing information by forwarding it, disseminating or making information available in any other way, assembling, interrelating, protecting, exchanging or destroying information'. Division 3 of the Act sets a number of requirements for information processing. Processing information may take place exclusively for a specific purpose and only in so far as necessary for the proper implementation of the law. It must also be done with due and proper care. In addition, the information processed must be accompanied by an indication of the degree of reliability or a reference to the document or source from which the information has been derived. In the case of the processing of personal data, additional provisions apply regarding the categories of data that may be processed and restrictions are imposed—for example, with respect to data processing solely based on religion or sexual orientation. These requirements apply to any form of information processing, including therefore the internal analysis or circulation of information. Some forms of information processing are subject to additional requirements. These will be discussed below. Thanks to the existence of all these provisions, there is a manageable

legal review framework available to the persons exercising oversight of this aspect of the activities of GISS.

There is no real parliamentary oversight of information processing, since parliamentary oversight is restricted to general issues, while information processing is predominantly a matter of detail. Since the CTIVD is a specialised oversight body with a staff of its own, while its main task is reviewing the lawfulness of activities, it is pre-eminently equipped to exercise oversight over the conduct of GISS in this area. The findings of the CTIVD can then serve as the basis for a debate between government and parliament.

The fact that the oversight of GISS is exercised by the CTIVD and not by another oversight body is decisive for the form the oversight takes. This is due to the fact that the CTIVD reviews for lawfulness. This implies that the law is the guiding principle for the selection of matters to be investigated and also for the assessment of actual cases. So, where the law does not provide a (clear) review framework for a specific matter, review of this matter will necessarily be minimal or even absent.

The CTIVD has not explicitly designated information processing as one of its focus areas. It is indeed not necessary to do so. In many of the review reports issued so far by the CTIVD, the information processing that took place in the specific case under review was tested against the aforementioned review framework. The guiding questions in all reviews are: did the retrieving and sharing of information satisfy the requirements of, inter alia, purpose, necessity and proper and due care? Naturally, the CTIVD always restricts itself to testing for reasonableness: it is not the intention for the CTIVD to repeat the work of GISS but to review whether the service could reasonably have made the decisions it made and made the decisions with proper and due care.

Two arrangements are included in the law that give citizens a possibility to take note or become aware of the attention GISS has given them: they concern the application for inspection of files and the obligation to notify. Both are monitored by the CTIVD. A citizen may file an application for inspection of his own data file or of the data file concerning an administrative matter (for example in the context of journalistic or historic research). The CTIVD conducts random inspections of such applications and assesses whether GISS interpreted the application correctly and has actually released the data qualifying for release. The obligation to notify means that five years after an investigation into a person is terminated, GISS must inform this person that certain special powers have been used if this does not conflict with the interest of keeping it secret. The CTIVD also conducts sample inspections with respect to this obligation and has published a report on an in-depth investigation concerning the obligation.[739]

3.1.2 National sharing of information

For the purposes of the ISS Act 2002, information sharing is understood as a form of information processing. Consequently, whenever GISS requests or receives information from other agencies or shares information with others this falls under the provisions pertaining to information processing, as set out in part 3.1.1 above. Some additional requirements apply, moreover, to the external sharing of (personal) data by GISS with other agencies.

[739] CTIVD 2010.

As was discussed above, the CTIVD has selected a number of the services' activities for structural monitoring. One of these activities is that of issuing official messages. It is a statutory requirement that when personal data are provided to other agencies, while these agencies may take action based on such data, the provision of the data must be effected in writing. This happens in the form of official messages. Every six months the CTIVD examines whether the official messages issued in the preceding six months are—briefly stated—covered by the underlying documentation. In fact, the CTIVD thus monitors every piece of information disclosed by the services which may have consequences for a citizen; for example, in an asylum or deportation procedure or in criminal proceedings. The CTIVD has also issued a report on an in-depth investigation into the official messages issued by GISS, which presents a clear picture of the review framework.[740] When the CTIVD, in the process of monitoring the official messages, comes across things which it holds to be incorrect, it can inform the head of GISS, the Minister of Home Affairs/Kingdom Relations or, as a last resort, the Second Chamber. It can also decide to start an in-depth investigation.

3.1.3 International sharing of information

Traditionally, the international sharing of information between intelligence and security services has always been a sensitive subject. Parliament has shown a certain amount of interest in the subject, particularly because of the controversy entailed in the cooperation with countries that are not very particular about human rights. Parliament is confronted, however, with the fact that the services will not say publicly with whom and how they cooperate. The subject can be raised in the ISS Committee, but this happens only occasionally and not in-depth because of the committee's set-up.

So in regard to this aspect as well, the oversight exercised by the CTIVD plays an important role. The official rules laid down in the ISS Act 2002 give some guidance but certainly not complete clarity. Here, too, the general framework for information processing applies but in practice the additional provisions are the most important. These are stated in general terms, however. Considered in connection with the exchanges between government and Parliament while the bill was being debated, it can be deduced, for example, that cooperation may not be contrary to the interests to be protected by GISS; for example, the protection of human rights. In 2009, the CTIVD issued a report on the cooperation between GISS and foreign services.[741] Obviously, the report assessed only the actions of GISS, that is: only one side of the cooperation. The CTIVD examined—among other things—the agreements with foreign services, whether GISS' sharing of information with foreign partners, requesting and rendering assistance and carrying out joint operations fit within the parameters set by law, parliamentary history and its internal policy (which is based on the former). It was no obstacle to the proper conduct of the investigation that for its examination only the information present at GISS was available to the CTIVD, and not the information at the foreign services. The CTIVD was concerned with the actions of GISS, as documented by GISS. It should be noted that the investigation resulted in critical findings, causing GISS to tighten its procedures. The CTIVD has the impression that both the assessment framework (with whom may GISS cooperate?) and the procedures (what form is the cooperation to take?) have gained in quality as a result.

The investigation also covered the cooperative groups formed with international and European organisations. The cooperation in these groups is, however, always cooperation

[740] CTIVD 2006.
[741] CTIVD 2009.

at a more abstract level; not the level of personal data but of analytical, strategic products. This makes it straightaway a less interesting form of cooperation from the perspective of lawfulness. The CTIVD has little to review in regard to these forms of cooperation.

Due to the limited resources of the CTIVD, sharing information with foreign services is not part of the structural monitoring. The subject, however, deserves attention since it plays a major role in the work of GISS and can potentially have grave consequences for individuals.

3.1.4 Joint analysis

Since 2005, the Netherlands has had the Counter-Terrorism Infobox (CT Infobox), a cooperative group comprising GISS and a number of other bodies (police, INS, Royal Netherlands Military Constabulary etc.) and set up for the purposes of sharing information to combat terrorism and radicalisation. Since very strict secrecy requirements and a closed system for providing such information apply to the information in the possession of GISS, it was decided to locate the CT Infobox at GISS while furthermore the ISS Act 2002 must be applied to the activities of the cooperative group. This means that the CTIVD has the authority to exercise oversight over the activities of the CT Infobox. In 2007, the CTIVD issued a report on the CT Infobox in which all sorts of aspects of the cooperative group were considered after in-depth review: including persons in the box, removing persons from the box, access to systems of the participating organisations, the legal basis for the phenomenon and the status of the recommendations issued by the box.[742]

In the case of the CT Infobox, there is again no direct oversight by Parliament. But the CTIVD report has been very useful in providing Parliament with information, enabling it to have an informed discussion with the Minister.

For some time now we have had the National Coordinator for Counterterrorism in the Netherlands. It does not fall under the ISS Act 2002 and does not have a separate oversight body. This is not considered necessary because, as far as information processing is concerned, the service merely acts as a coordinator and an intermediary. It does not itself collect information nor disseminate information of its own, and it does not make use of special powers.

3.1.5 Collection of open source information

The collection of open source information is governed by the same provisions as were set out above with regard to the processing of information, on the understanding that the ISS Act 2002 considers the collection of open source information to be the lightest form (as regards privacy infringement) of collecting information. In this perspective, it is in fact worthy of praise when the service can manage solely by collecting open source information. For this reason, the CTIVD subjects the collection of open source information to very minimal review.

[742] CTIVD 2007.

3.2 Finances

As was already stated above in part 2.2.2, budgetary oversight has not been vested in the regular oversight body, the CTIVD, but in the authorities that audit the expenditure of the central government in general: the Netherlands Court of Audit and the National Audit Service. These bodies conduct an annual audit of the financial picture of GISS.

If the occasion arises, however, the CTIVD may take financial aspects into account. For example, when the CTIVD examines whether an operation was carried out within the parameters of the service's internal guidelines, it may also examine whether the internal control of expenditure was performed correctly. This is a very infrequent examination which the CTIVD—because the CTIVD is no expert on these issues—necessarily performs with restraint.

4. GOOD/BAD PRACTICES

It is important to have a clear grasp of the objective of oversight and what is therefore the task of an oversight body. Does the oversight serve the purpose of establishing whether the service performs its numerous activities in compliance with the law, for example because the service has far-reaching powers which are used secretly? In 2002, this latter circumstance was the reason for establishing the CTIVD: it was expressly linked to the case law of the ECHR requiring that in case of secret privacy intrusions, citizens must in certain circumstances have an opportunity to address the intrusions: this called for an oversight body which could exercise in-depth oversight of the lawfulness of the activities of the services.

Or does the oversight serve to enable Parliament to monitor whether the service does what government and Parliament have agreed? In this case, oversight of lawfulness is too limited a tool and Parliament might itself have to assume greater responsibility for the oversight. In the Netherlands, the limited scope of the CTIVD (the accent on legality) has been criticised. It has been argued though that this limited scope enables the CTIVD to look at all important issues while still maintaining a sound distance from purely operational matters.

It is of overriding importance that the committee charged with the oversight, whether parliamentary or specialised, is supported by staff members working fulltime at exercising oversight. In the Dutch system, the choice has been to establish a specialised committee that is supported by a secretariat. Parliamentary committees do not have a supporting secretariat. Thus a system has developed in which the CTIVD rather quietly conducts in-depth investigations that result in public reports, which provide Parliament with a basis for questioning the government about the activities of its intelligence and security services. This appears to work well: experience has taught that members of parliament—and certainly the chairpersons of parliamentary groups constituting the ISS Committee—have little time, capacity for, or interest in conducting detailed investigations. Partly because of the elaborate appointment procedure of its members and the emphasis in its tasks on lawfulness, the CTIVD does not have a political profile. This means that the government, the services and Parliament can be confident that its investigations are conducted objectively and with great care. In this way, the system provides for well-balanced public information in a domain which, because of its secrecy, can be a playing field for unverifiable rumours and political fireworks. Since the CTIVD cannot issue binding decisions, it is the responsibility of parliament to induce the government to act on the basis of the information provided by the CTIVD. In this sense, the decision of how to weigh conclusions regarding

the actions of the intelligence and security services remains with the elected parliament and not with the CTIVD: the primacy lies with politics. The consequences of the findings of the specialised oversight body are determined in the debate between government and Parliament.

This system of a division of tasks between Parliament and the specialised oversight body will only function well if Parliament can make effective use of the information provided by the CTIVD. Dutch law does not say anything about the contacts between the CTIVD and Parliament, so these contacts have been given an informal shape. Perhaps it would do no harm to safeguard the process in some way or other (by law), so as to ensure cooperation between Parliament and the specialised oversight body.

Some other good practices appear to be rather self-evident: in any case, there must be an oversight body which 'can dive into' the services on its own initiative to investigate. This body must have access to all information. Some oversight systems make an exception for, e.g., operational information or information concerning cooperation with foreign services. Such restrictions may sound reasonable to some but they are disastrous for the credibility of an oversight body. Operations or cooperation with foreign services make up a large and complex part of the activities of intelligence and security services. Passing over these activities practically turns the oversight into mere window dressing. Following on from this, the oversight body must be able to determine itself which information it does or does not consider relevant: in this sense, the oversight body determines its own procedure. Of course the oversight body may pay heed to (legitimate) wishes of the service being investigated, like how the information should be handled, but in the end the oversight body must be able to determine itself how it performs its tasks—within the parameters of legislation and regulations. This will prevent the need for repeated discussions or negotiations between the oversight body and service. Finally, the oversight body must be able to issue reports that are public and this must also be the basic principle. Secret information cannot be debated and it would then be impossible to make a contribution to the public reporting on the activities of the services.

REFERENCES

Act on the constitution of the Kingdom of the Netherlands 1815, *Stb.* 2008, 348.

CTIVD (2010), *Review report on the performance of the GISS on the obligation to notify*, *Kamerstukken II* 2009/10, 29 924, No 49 (attachment), available at (www.ctivd.nl).

CTIVD (2009), *Review report on the cooperation of GISS with foreign intelligence and/or security services*, *Kamerstukken II* 2009/10, 29 924, No 39 (attachment), available at (www.ctivd.nl).

CTIVD (2007), *Review report on the Counter-Terrorism Infobox*, *Kamerstukken II* 2006/07, 29 924, No 16 (attachment), available at (www.ctivd.nl).

CTIVD (2006), *Review report on the official reports issued by GISS in the period from January 2004–January 2006*, *Kamerstukken II* 2005/06, 29 924, No 13 (attachment), available at (www.ctivd.nl).

Havermans Commissie (2004), *De AIVD in verandering*, Van Langen Drukwerk, Rijswijk.

Intelligence and Security Services Act 2002, *Stb.* 2002, 148.

Rules of Procedure of the Second Chamber 1994. *Kamerstukken II* 1991/92 and 1992/93, 22 590, *handelingen II* 1992/93, Nos 31 and 33.

Security Screening Act 1996. *Stb.* 1996, 525.

ANNEX A: COUNTRY CASE STUDIES

VII. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN SPAIN

SUSANA SANCHEZ FERRO

1. INTRODUCTION

The Spanish oversight system of its security[743] and intelligence services[744] has improved in recent years—mainly as a reaction to various scandals revealed by the Spanish press—but there is still a long way to go. When it comes to the fight against terrorism, there is a tacit pact (broken from time-to-time) among the main Spanish political parties to let the government lead this fight and show the country's unity on its anti-terrorism policy, preferring to keep any disaccord over the policy under wraps. Regarding the oversight of the intelligence agency, since 2002 there has been a specialised committee in place to oversee its activities, which is a clear improvement. A culture of oversight is emerging but there are still some flaws in the mechanisms of oversight that will need significant effort to remedy.

2. VALUABLE TOOLS FOR PARLIAMENTARY OVERSIGHT OF THE SECURITY SERVICES: A STRICT DEFINITION OF THE LEGAL MANDATE OF THE INTELLIGENCE AGENCIES AND A REDUCTION OF THE SCOPE OF SECRECY

2.1 The National Intelligence Centre (CNI) legal mandate

The first way to diminish the danger posed to democracy by intelligence and security services is for Parliament to limit their powers through detailed legal provisions.[745] The absence of a clear and explicit legal basis for intelligence agencies 'may bring a state into conflict with constitutional or human rights norms, especially in the case of powers affecting individuals'[746] and will hinder the oversight of intelligence agencies as there will be no set limit to their activities. A mandate for the intelligence agencies that is strictly compatible with the jurisprudence of the European Court of Human Rights would be an essential tool to allow the Parliamentary Committees in charge of oversight to carry out their functions.[747]

[743] 1.1.1.1 The National Police and the Guardia Civil are the national law enforcement agencies whose main function is the prevention of crime. In order to fulfil its mandate, both agencies are allowed to gather, collect and analyse any information relevant to prevent crimes and preserve the legal order (Art. 11 of the Security Forces Organic Act, Act 2/1986, of 13th March). There are also police forces at the different Autonomous Communities.
[744] The Spanish National Intelligence Agency is called Centro Nacional de Inteligencia.
[745] Scheinin 2009, p. 7; Revenga Sánchez 2001a, p. 63.
[746] Ibid., 5.
[747] See, inter alia, *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, Reports 1998-V, p. 1925, Section 46 (iii); Case of *Liberty and Others v. The United Kingdom*, (Application 58243/00), Judgment of 1 July 2008, Section 93; Case of *the Association for European Integration* (supra), Section 75.

In 2002, the Spanish Parliament passed two acts applicable to the CNI: the National Intelligence Centre Act (2002)[748] and the Act on Ex Ante Judicial Oversight of the National Intelligence Centre (2002).[749] The new legal regime implied a new legitimacy for the activities of the CNI.[750] Unfortunately, however, Parliament did not take this opportunity to improve the legal framework: the definition of the functions and activities of the Centre is too broad.

Though the law in this field is usually quite vague, the National Intelligence Centre Act of 2002 is too vague. Article 1(a) of the Act, for example, reads that the Centre shall gather, analyse and interpret information, and disseminate the intelligence needed to promote the political, economic, industrial, commercial and strategic interests of Spain. Intelligence services can exercise their functions in order to enhance the economic well-being of the population. But to allow them to gather, analyse and interpret the information, as well as disseminate the intelligence needed to promote commercial and industrial strategic or economic interests goes beyond just protecting the economic well-being of the country. On the other hand, the law provides that the Centre will act in accordance with the goals fixed by the government in the Intelligence Directive—but this Intelligence Directive is secret (see Articles 2 and 3 in the National Intelligence Centre Act).

2.2 The scope of secrecy in Spain as an obstacle to the parliamentary oversight of the Intelligence Agency

The scope of secrecy in Spain is too broad. The government can classify any object, information or document whose publicity could pose a risk to defence or national security as secret (see Articles 2 and 4 of the Official Secrets Act).[751] The information can be classified in two different categories, 'secret' or 'confidential', depending on the degree of protection required. The government passed two resolutions classifying different categories of information so that any information that falls within these categories must be considered classified.[752] There is no proper system of declassification for the documents, no automatic declassification of the documents after a certain number of years, nor any systematic review of the documents.[753] The competent classifying authorities have to mark the document, when possible, with a date for declassification but there are no time limits for a document to be declassified.[754]

The government is the only competent authority to declassify official secrets. Of course, it does not have the time to review every document classified as secret. There is too much classified information and this can have a negative impact on the control of the security services by Parliament. Even if Parliament has access to secret information, Parliament can get lost in the countless secret documents.

[748] *Ley 11/2002, de 6 de mayo, del Centro Nacional de Inteligencia.*
[749] *Ley Orgánica 2/2002 del Control Judicial Previo del Centro Nacional de Inteligencia*.
[750] Revenga Sánchez 2001b, pp. 30–31.
[751] Official Secrets Act of 5th April 1968, amended by Act 48/1978 of 7th October, whose dispositions are developed by Decree 242/1969 of 20th February. The Official Secrets Act says that the Joint Committee of the Heads of the Military could also classify information as secret following the Official Secrets Act, but we considered that this provision has been overruled by our Constitution (see Sanchez Ferro, S. (2006), *El Secreto de Estado,* Centro de Estudios Políticos y Constitucionales, Madrid, pp. 286–289).
[752] Government Resolution of 28th November 1986 and Government Resolution of 16th February 1996.
[753] *See* Sanchez Ferro 2006, pp. 295–301.
[754] Article 3.III of Order 242/1969, of 20th February, of the Official Secrets Act.

3. ACCESS TO (SECRET) GOVERNMENT INFORMATION BY PARLIAMENT

Article 109 of the Spanish Constitution gives Parliamentary Committees a right to request, through their respective Speaker, any kind of information or help they may need from the government, government departments and any authorities of the state. This right is not given to individual members of Parliament (MPs).[755] The Committees may request, through the Speaker:

i) Such information and documentation as they may require from the government and administrative bodies;
ii) The attendance of members of the government to report on matters relating to their respective department;
iii) The attendance of authorities and civil servants competent in the subject matter of the debate so that they report to the committee; and
iv) The attendance of persons competent in the subject matter of the debate for the purposes of reporting to and advising the committee.[756]

Article 10.2 of the Official Secrets Act determines that Parliament will have access to classified information in the way established by the Parliament Standing Orders and in secret sessions. The Standing Orders did not say anything about access to classified information. This omission was solved by the President of Congress through the Resolution of 18 December 1986, amended by the Resolution of 2 June 1992[757] and the Resolution of 11 May 2004. Therefore, only Congress has ruled on access to secret information by members of Congress.

According to the 1986 Resolution, one or more political groups amounting to at least three-quarters of the Members of the House (263 MPs from a total of 350) were empowered to request access to classified information via the House President. Secret information would then be given to three MPs belonging to different political groups, elected by a three-fifths majority (210 MPs) for the whole term. When the information was classified as confidential, it would be given to the Spokespersons of the different parliamentary groups (Article 2 of the Resolution). The government, exceptionally and only by justifying it, could ask the House's Bureau to share the information with the President of Congress alone. The Bureau would have to decide on this. He could then ask to share the information with the Committee involved in the matter under discussion, in secret session and with attendance only of the members of the Committee (see Article 2, Section 3 of the 1986 Resolution).

On the other hand, Parliamentary Committees, through the President of the House, could also ask for access to classified information. When the information was classified as secret, the government would share the information with the three MPs as stated in Article 2. If the information was classified as confidential, the government would share the information with the MPs that act as spokesmen for their political groups in the Committee. The government, exceptionally and only by justifying it, could also ask the House's Bureau to share the information with the President of the Committee alone or to share the

[755] See Article 7 of the Standing Orders of Congress and, for a discussion on this, Ruiz Miguel 2002, pp. 248–249 and Bueso 1997, available at (http://www.icps.es/archivos/WorkingPapers/WP_I_133.pdf).
[756] Article 44 of the Standing Orders of Congress.
[757] Resolución de la Presidencia sobre acceso por el Congreso de los Diputados a materias clasificadas, 18 December 1986 (B.O.C.G., series E of 19 December 1986, No 14) and Resolución de la Presidencia del Congreso de los Diputados, 2 June 1992 (B.O.C.G., Series E, of 3 June 1992, No 208).

information with the Committee, in secret session, and with attendance only of the members of the Committee (see Article 3 of the 1986 Resolution).

With this regulation, no member of Herri Batasuna (HB)—later illegalised for being the political branch of the ETA (*Euskadi Ta Askatasuna)*—would ever have access to secret information as they would never get the necessary votes to be elected to have access to that information.

The 1992 Resolution changed the majority needed to request classified information to 'only' one-fourth (88) of the MPs in Congress (see Article 2). On the other hand, instead of sharing the information with three MPs, the government would share the information classified as secret with one MP from each political group in Congress as established under Article 23.1 of the Standing Orders of the House (elected by a three-fifths majority for the whole term).[758] HB could not form its own political group in the House and had to join the non-attached political group. The non-attached group is not constituted following Article 23 so the non-attached group (with HB) would be excluded from the access to secret information.

HB was declared illegal in 2003 by the Supreme Court[759] in accordance with the Spanish Political Parties Act of 2002.[760] Probably because of this, in 2004 the President of Congress made a new resolution by which any reference to Article 23.1 of the Standing Orders disappeared. Now, when information is classified as secret, the government will share the information with one MP for every political group of the House. The MPs will be elected for this by a three-fifths majority in the House. When the information is classified as confidential, the government will share the information with the Chairmen of the political groups or their representatives at the Committee when the request came from it (Articles 3 and 4 of the Congress Resolution). Thus there is a representative of each political group in the House that has access to secret information.

4. HANDLING OF CLASSIFIED INFORMATION BY MPs

When the information concerns a particular document, MPs with access to classified information can ask the relevant authority to show them the document (the original or a photocopy) if they believe their knowledge of the information would be incomplete without seeing it (see the Resolutions mentioned above). The MPs are allowed to see the documents for themselves and take notes under the supervision of the authority that shows them the document but they cannot copy or reproduce them. The MPs examine the document in the House, unless the House President thinks that it will be better to improve access to particular information to see documents in the place where they are kept (see, in this regard, Articles 7 and 8 of the 2004 Resolution). Secret documents cannot be reproduced or kept by the MPs (see Article 11.3 of the CNI Act). Access by parliamentary staff to these documents is not envisaged by the law. In a case where some MPs from the Catalonian Parliament wanted to be accompanied by their parliamentary staff in the analysis of some bank statements of the Government of Catalonia, the Spanish Constitutional Court said that although the right of access to the documents belonged to the MPs they could be accompanied by experts from their parliamentary group—staff of

[758] Article 23.1 of the Standing Orders of Congress: 15 MPs can set up a political group. 5 MPs could also form a political group if the votes they obtained in the elections amounted to 15 per cent of the total amount of votes in the circumscription in which they presented their candidates or 5 per cent of the total amount of votes of the whole nation.
[759] Supreme Court Resolution of 27th March 2003.
[760] Organic Law 6/2002, of 27th June, of Political Parties [BOE No 154, of 28th June].

their group in Parliament (registered as such in the House)—as otherwise they would not be able to exercise their functions as MPs and carry out real oversight of the Government of Catalonia (right to representation of Article 23.1 of the Spanish Constitution).[761] It does not seem that this doctrine could also be extended to access to classified documents by MPs as even individual MPs cannot access secret information themselves.

All those MPs with access to secret information must refrain from disclosing any proceedings which may be of a secret nature (Article 16 of the Standing Orders of Congress). The sanction for breaching this obligation is disciplinary. A Member may be deprived, by resolution of the Bureau, of some or all of the rights granted to him/her under Sections 6 to 9 of these Standing Orders (Articles 99.1 and 101 of the Standing Orders of Congress), which include the right to vote, the right to sit in at least in one committee, to request information or to be paid a financial allowance; the MP can even be suspended for a time.[762] If the cause behind the penalty may, in the opinion of the Bureau, constitute a criminal offence, the Speaker shall convey the incriminating facts to the judicial authority with jurisdiction (Article 101.3 of the Standing Orders of Congress).

This being said, is the disclosure by an MP of information that he or she has received in secret session to the press or citizens a criminal offence?

Articles 584 and 598 to 603 of the Spanish Criminal Code dealing with crimes related to revealing classified information seem to apply to MPs that have access to official secrets. Article 598 provides that he who reveals or renders useless information classified as secret or confidential, related to national security, will be sanctioned with imprisonment from one to four years. Article 584 provides that the Spanish national who reveals secret or confidential information that may harm national security with the intention to benefit a foreign nation will be considered a traitor and sanctioned with six to twelve years imprisonment. Despite this, we could argue that the Resolution of the Supreme Court No 921/2006 of 26 September opens a window to reinterpret these norms. In its sentence of 4 April 1997, the Supreme Court held that classified information does not lose its classified character, not even in a case when it is made public by the press: this information is protected until the government decides to declassify it (although the Supreme Court could review the secret documents in private and tell the government to declassify them if there is no harm for national security).

In its Resolution of 2006, the Supreme Court affirms that the activities of the Centre that clearly exceed the aims to which the declaration of secrecy is made, cannot automatically be covered by secrecy. Information about illegal interception of communications could not be considered classified because the classification was made in broad categories, that is, in abstract, without referring to particular facts (e.g., methods and operations of the Intelligence Service), and its revelation, as it covered criminal offences, did not affect the national security of the nation. We could think, then, that an MP revealing criminal offences covered by the veil of secrecy would not being condemned by the judges as they could consider that this information would not be really classified. Despite this, it would be better for the legislature to foresee a mechanism to allow MPs to reveal this kind of information, minimising the dangers of leaving MPs to be judges of the secret nature of information.

[761] Ruling 181/1989, of 3rd November 1989.
[762] Standing Orders of Congress of 10th February 1982 (an English version is available here: (http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/standing_orders_02.pdf).

5. THE OVERSIGHT OF THE SECURITY AND INTELLIGENCE SERVICES BY PARLIAMENTARY COMMITTEES

5.1 Introduction

Undoubtedly, access to secret information by Parliament is essential to carry out effective oversight of the information services and departments[763] but it is not enough. Different abuses uncovered by the Spanish press committed by the Intelligence Agency were clear proof that a specialised body was needed to oversee the Intelligence Agency.[764] Because of this, the CNI Act of 2002 gave a committee, the so-called Secret Funds Committee, the special task of controlling the activities of the CNI (but not those of the Police and the *Guardia Civil*). The Committee was created as a consequence of a case of embezzlement of secret funds by the Director of the *Guardia Civil*.[765]

When it comes to the oversight of the Security Forces, the Standing Orders of Congress and the Senate contemplate a Permanent Home Affairs Committee to control internal affairs so that any questions related to the subject are supposed to be dealt with by these two Committees.[766] The Parliament Home Affairs Committees are in charge of the oversight of the Security Forces and have access to secret information through the channels established by the Standing Orders of Congress. These Committees are in charge of a mixture of tasks, including those of a legislative nature.

5.2 Oversight of the use of secret funds by the Security Forces and the CNI and oversight of the budget of the CNI

The law provides that secret funds of the Security Forces and the CNI must only be used to cover expenses necessary to protect national security (Article 1, 11/1995 Act). The power to authorise expenditures of these funds and the special means by which these expenditures have to be justified is vested in the Ministers of Defense, Home Affairs, Foreign Affairs and Justice. Secret expenditures must be included in the budget. The departments that handle secret funds must report to the Secret Funds Committee on the use of the money every six months (Articles 2 and 7.2 of the Secret Funds Act) and on the internal rules that these departments approved to make sure that credits are handled by the authorities of their department in accordance with the legal ends established by the 1995 Act (Article 6 of the Secret Funds Act). The Parliamentary Oversight Committee must send a report to Congress whenever the Ministers ask for an increase in the amount of secret funds.

[763] Government Resolution of 28th November 1986 on classified information declared, for example, that the structure, organisation, methods and operational means of the information services (and this now includes the CNI, and the Information Departments of the police and the *Guardia Civil*) are classified in the category of Secret and so is the information, analysis and assessment of actual or potential threats to national security. In Spain there are only two categories of classified information, Secret and Confidential, and they do not match with the four ordinary categories in which other legal systems classify information, following for example, NATO's system of classification.

[764] See: Constitutional Court Resolution No 39/2004 of 22nd March and Supreme Court Resolution No 367/2001 of 22nd of March in the case of the CESID illegal interception of communications of persons of public relevance, including the King, during the years 1983 to 1991, and Supreme Court Resolution No 224/2004 of 31st March on the case of illegal interception of communications of the Herri Batasuna Political Party (afterward consider illegal because of its links with ETA by a decision of the Supreme Court of 2003, from the years 1994 to 1998).

[765] Secret Funds Act of 11th May 1995 (Act 11/1995).

[766] Articles 31 and 46.1 of the Standing Orders of Congress of 10th February 1982, and Articles 54 and 49.3 of the Standing Orders of the Senate of 3rd May 1994.

Since 2002, the Secret Funds Committee must also oversee the use of the budget by the CNI and every aspect of the activities of the Intelligence Agency (Article 11.1 of the CNI Act).

When it comes to the budget of the CNI, the CNI has the power to make a preliminary draft of it (Article 8.2, Act 11/2002) and the government will incorporate this into the total budget. Parliament has the power to approve the final budget. The use made of the budget by the CNI is overseen by the Court of Exchequer, whose components are appointed by Parliament (Article 30 of the Exchequer Court Act 2/1982, of 12 May).

5.3 The oversight of CNI activities

The Secret Funds Committee, in charge of oversight of the CNI, is made up of the President of Congress and the Congressmen that have access to official secrets in accordance with the rules of the House (Article 7.1 of the Secret Funds Act). The spokesmen of every political group in the House have been elected to be part of this Committee. On the one hand, this is positive as it reflects that Parliament gives the utmost importance to this matter but, on the other hand, these MPs are involved in everyday business of Parliament and do not have much time to focus on the CNI, aside from the fact that they do not seem to have parliamentary support staff to carry out their job in this Committee.

The Committee will not have access to any classified information from a foreign secret service (Article 11.2 of the CNI Act). This is an important exception in an interconnected world. The CNI Act also excludes access by the Committee to information on the methods and sources of the intelligence service. Under Article 1.2 of the Spanish Constitution, citizens are the source of legitimacy of all powers and the MPs are their representatives. They must know what the executive does and judge for themselves whether these activities merit the secrecy with which they are surrounded. Why must we trust our security services and government but not our MPs to keep secret the sources and methods of the CNI and the information coming from other foreign intelligence agencies?

The Government is obliged by law to send information to the Committee annually about intelligence aims. The Committee will also receive the annual report evaluating the activities of the Centre and the degree of accomplishment of the aims fixed by the government (Article 11.2 of the CNI Act). Of course, the sessions of the Committee are secret (Article 11.1 of the CNI *Act*). Until 2002, Spanish law did not envisage an obligation by the Intelligence Agency of reporting to Parliament on its activities. Because of this, and because of the breadth of secrecy, Parliament was half blinded when it wanted to ask for information that could be relevant to control the Intelligence Agency. Fortunately, the CNI Act established the obligation by the CNI to inform the Parliamentary Committee about its activities annually and, despite the vague character of the information, it can always give clues to Parliament on what to ask for (Article 11.4 of the CNI Act, 11/2002, of 6 May). Obviously, the Director will have the means to hide what he does not want Parliament to know and an annual report can be too general or vague. The Committee usually develops more *ex post* oversight than *ex ante* control. The avoidance of possible abuses demands an active Committee with time to devote to its task, which uses all available means, and a law that obliges the security services to report more often.

Until now, the Committee seems to have acted only after the press raised the alarm rather than at its own initiative. The population already knew about wrongdoings by the CNI before the Committee acted upon them. We ignore whether the activity of the Committee has produced any change in the way these services operate, as the activities of the

Committee are too secretive. There has been no real discussion about the value of these ad hoc investigations by parliamentary committees on security matters.

6. OMBUDSMAN CONTROL

The Spanish Ombudsman is appointed by Parliament and his task is to protect the fundamental rights of the people. To accomplish its tasks, the Ombudsman has the power to supervise any activity of the Spanish Administration (Article 54 of the Spanish Constitution and Articles 1, 2, 9 and 10.2 of the Ombudsman Act of 6 April 1981 [Act 3/1981]). Article 22 of the Ombudsman Act provides that the Ombudsman can request public authorities to send him any document that he considers necessary for his/her work, even those classified according to the Official Secrets Act. Only the Ombudsman and his deputy will have access to official secrets.[767] The Ombudsman must ask the government for authorisation to access the classified documents and establish the mechanisms to protect the secret documents. The government can decide that the documents should not be sent to the Ombudsman, in a written agreement. The Ombudsman and his Deputy do not have to go through a vetting process or a security clearance; the key element here is whether the government grants them access to the documents. If they are granted access, no reference can be made in the Ombudsman's annual report to the content of secret documents or in response to the complainant. The Ombudsman considers whether to give information about the classified documents to Congress and the Senate or not.

When the Ombudsman thinks that the denial of access can seriously affect the development of his investigations, he must notify the Congress-Senate Committee of relations with the Ombudsman, and then Parliament can act. The investigation by the Ombudsman, if the complaint is upheld, concludes with a recommendation for putting matters right (Articles 23, 28.2 and 30.1 of the Ombudsman Act).[768] The Ombudsman can, if s/he thinks that the abuse committed by the administrative authorities or personnel amounts to a criminal offence, inform the Public Prosecutor.

The activity of the ombudsman in the field of intelligence and the security forces has not been great (see his Annual Reports of 1993, 1995, 1999 and 2002).[769] There are some recommendations about police files and their handling by the police, mainly about how to keep secret the personal data of the citizens discussed in police files. The Ombudsman, at least, has the tools to initiate investigations when he receives complaints about the Intelligence Services and departments of law enforcement agencies, but has not made much use of them.

[767] Article 26, Decree on the Organization and Functioning of the Ombudsman (BOE No 92 of 18th April 1983).
[768] Escobar Roca 2010, pp. 229–257, pp. 238–239.
[769] The reports can be found on the webpage of the Ombudsman, (http://www.defensordelpueblo.es/).

1. GOOD PRACTICES

- There is an MP for every political group of the House represented in the Committee that controls the CNI.
- The Special Rules establish control over secret funds. Money can many times tell better than any general annual report what exactly the intelligence services are doing.
- Control of the use of secret funds extends not only to the CNI but also to the Police and the Guardia Civil.
- The Committee that controls secret funds is the same that controls the CNI.
- There is continuity of the members of the Committee for the whole term and the way they are elected, which requires a high consensus in Parliament.
- The Ombudsman can access secret documents to help carry out his/her investigations. The people have direct access to the Ombudsman and can complain of any activity infringing their fundamental rights carried out by the Administration and the Executive Power. The Ombudsman has better access than Parliament to particular cases of violation of rights.
- Even if the Ombudsman cannot access secret information when the government refuses access, it can notify parliament, which has complete access to the classified information and can follow up the investigations begun by the Ombudsman.

REFERENCES

Aba Catoira A. (2002), 'El secreto de Estado y los servicios de inteligencia', *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, Nos 38/39, pp. 133–168.

Bajo Fernández M. (1982), 'Protección del honor y de la intimidad' in *Comentarios a la legislación penal*, Vol. I, EDERSA, Madrid.

Barata I Mir J. (1997), 'Secretos oficiales y jurisdicción: crónica y análisis de un largo recorrido. De la sentencia del Tribunal de Conflictos de Jurisdicción de 14 de diciembre de 1995 a las sentencias del Tribunal Supremo de 4 de abril de 1997 (1)', *Revista Vasca de Administración Pública*, No 48, pp. 207–249.

Barcelona Llop J. (1998), 'El secreto policial. Acceso a archivos y registros de la policía. Los ficheros automatizados de las fuerzas y cuerpos de seguridad' in *Acceso judicial a la obtención de datos*, Consejo General del Poder Judicial, Madrid, pp. 157–222.

Blay Villasante F. (1989), 'El delito de traición mediante espionaje' in *Comentarios a la legislación penal*, TX ('La reforma de los delitos contra la defensa nacional'), M. Cobo del Rosal (dir.) and M. Bajo Fernández (coord.), EDERSA, Madrid, pp. 1–41.

Born H., Johnson L. and I. Leigh (eds.) (2005), *Who is Watching the Spies? Establishing Intelligence Service Accountability*, Potomac Books, Washington, D.C.

Bueso J. (1997), 'Información parlamentaria y secretos oficiales', Working Paper No 133, Barcelona.

Casas Nombella J.J. (1989), 'Breve consideración sobre la protección penal de materias clasificadas', *Boletín de información del Ministerio de Justicia e Interior*, Vol. II, pp. 974–980.

Cousido González P. (1995), *Comentarios a la Ley de Secretos Oficiales y su Reglamento*, Bosch, Barcelona.

Defensor del Pueblo (26 June 1996), *Informe del Defensor del Pueblo correspondiente a la gestión realizada durante el año 1995*, Boletín oficial de las Cortes Generales, Series A, No 7.

Díez-Picazo L.M. (1998), 'Publicidad y secreto en la Constitución' in *Acceso Judicial a la obtención de datos*, *Cuadernos de Derecho Judicial*, Consejo General del Poder Judicial, Madrid, pp. 43–62; (also available in *Sobre secretos oficiales* (1998), Civitas, Madrid).

Escobar Roca G. (2010), 'Interpretación y garantía de los derechos fundamentales por el defensor del pueblo', *Teoría y Realidad Constitucional*, No 26, pp. 229–257.

Fernández Alles J.J. (25 March 1999), *Los secretos de Estado en España: jurisprudencia y teoría constitucional (I)* in *Diario La Ley*, No 4762, Vol. II, D-82.

Fernández Alles J.J. (26 March 1999), *Los secretos de Estado en España: jurisprudencia y teoría constitucional (II)* in *Diario La Ley*, No 4763, Vol. II, D-83.

García-Trevijano Garnica E. (1996), 'Materias clasificadas y control parlamentario', *REDC*, No 48, pp. 145–178.

Gómez Orfanel G. (1996), 'Secretos de Estado: algo más de lo mismo', *Jueces para la democracia*, No 27, pp. 7–9.

Gómez-Reino Y Carnota E. (1976), 'El principio de publicidad de la acción del Estado y la técnica de los secretos oficiales', *REDA*, No 8, pp. 115–133.

Leigh I. and L. Lustgarten (1994), *In From the Cold: National Security and Parliamentary Democracy*, Clarendon Press, Oxford.

Luna Abella C. (2002), 'Artículo 22' in *Comentarios a la Ley Orgánica del Defensor del Pueblo*, A. Rovira (dir.), Aranzadi (ed.), pp. 561–585.

Massó Garrote M.F. (2001), *Poderes y Límites de la investigación parlamentaria en el Derecho Constitucional español*, Monografías Congreso de los Diputados, Madrid.

Perez Villalobos M.C. (2002), *Derechos Fundamentales y Servicios de Inteligencia* (*un estudio a la luz de la nueva legislación*), Grupo Editorial Universitario.

Revenga Sánchez M. (2001a), 'Servicios de Inteligencia y Derecho a la intimidad', *Revista Española de Derecho Constitucional*, No 61.

Revenga Sánchez M. (2001b), 'Servicios de Inteligencia. La Ley imprescindible', *Claves de Razón Práctica*, No 110.

Revenga Sánchez M. (1998), 'Razonamiento judicial, seguridad nacional y secreto de Estado', *REDC*, No 53, pp. 57–74.

Rodríguez-Villasante Y Prieto J.L. (1989), 'Protección penal de la información relativa a la defensa nacional (Comentario a los artículos 135 bis, a), b), c) y d) del Código penal)' in Manuel Cobo del Rosal (dir.) and Miguel Bajo Fernández (coord.), *Comentarios a la legislación penal*, TX ('La reforma de los delitos contra la defensa nacional'), EDERSA, Madrid, pp. 43–372.

Ruiz Miguel C. (2002), *Servicios de Inteligencia y Seguridad del Estado Constitucional*, tecnos.

Sáinz Moreno F. (1991), 'Secreto e información en el Derecho Público' in *Estudios sobre la Constitución española. Homenaje al Profesor Eduardo García de Enterría*, Vol. III, Civitas, Madrid, pp. 2863–2981.

Sanchez Ferro, S. (2006), *El Secreto de Estado,* Centro de Estudios Políticos y Constitucionales, Madrid.

Santamaría Pastor J.A. (1995), 'Secreto oficial' in *Enciclopedia Jurídica Básica*, Civitas, Madrid, Vol. IV, pp. 6088–6090.

Santaolalla López F. (2002), 'Actos políticos, inteligencia nacional y Estado de Derecho', *REDC*, No 65.

Santolaya Machetti P. (1995), 'El control de los secretos de Estado. La experiencia en Derecho comparado', *Poder Judicial*, No 40, pp. 57–83.

Scheinin M. (4 February 2009), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* Human Rights Council, Tenth session, A/HRC/10/3.

Segrelles de Arenaza I. (1994), *Protección penal del secreto de Estado (artículo 135 bis a) al 135 bis d)) del Código penal*, EDERSA, Madrid.

Vila Ramos B. (2004), *Los sistemas de comisiones parlamentarias,* Centro de Estudios Políticos y Constitucionales, Madrid.

ANNEX A: COUNTRY CASE STUDIES

VIII. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN SWEDEN

IAIN CAMERON

1. THE GENERAL MANDATE AND FUNCTIONS OF RELEVANT OVERSIGHT BODIES

This chapter gives an overview of the relevant bodies involved in oversight in Sweden and a very brief contextual and historical background. Sweden does not have a separate internal civilian security agency. Internal security is instead exclusively a matter for the Security Police, which is organised as an autonomous part of the National Police Board (NPB). The NPB is under the leadership of a National Police Commissioner appointed by the government, with the head of the Security Police as Vice Chairman and a Board of Directors representing the political parties in the Parliament (*Riksdag*).

Neither the NPB nor the government is allowed to make decisions in operational police work. Sweden is unusual in having a constitutional provision (Instrument of Government, Chapter 12, Section 2) which prohibits the government from interfering in administrative agencies' decision making in individual cases. It is still possible, however, to steer decision making more generally in a number of ways, for example by means of rules set out in government ordinances and policies and priorities in the annual budget instruction to the agency. Sweden does not have a system of ministerial responsibility so formally speaking the police are not accountable to the Minister of Justice as such but to the government as a whole.

The Security Police has full police powers.[770] The major mechanism of control over the Security Police has been until relatively recently prosecutorial involving judicial control over Security Police operations involving certain particularly serious infringements of privacy, namely surveillance, arrest and search and seizure. The chief government law officer, the Chancellor of Justice, exercises general control over government departments and administrative agencies. The Chancellor of Justice can be tasked by the government to investigate an agency and may prosecute civil servants for misuse of office. Although an 'internal' mechanism of control, the Chancellor of Justice tends to operate with a high degree of independence. S/he has on occasion investigated the Security Police.

There are two standing parliamentary committees that have the competence to investigate the police, including the Security Police—the Committee on the Administration of Justice (JuU) and the Committee on the Constitution (KU). These committees can hear witnesses *in camera* but this is very unusual. They do not take evidence under oath. Both committees have on occasion investigated the Security Police. KU in particular is a useful mechanism for discovering and highlighting alleged governmental abuse of power. Another method of

* Thanks to Dennis Töllborg for helpful comments.

[770] The agency employs about 800 people in total, including a relatively large number of civilian analysts. Only the members who have been trained as police may employ police powers.

providing a degree of parliamentary insight into the work of the Security Police that has occasionally been used is consultations with leaders of political parties represented in the *Riksdag*. This, in my opinion, is not satisfactory: it can work instead as cooption rather than meaningful oversight. Besides, as explained further below, historically the problems in this area have been not so much governmental abuse of power but a relative lack of effective governmental (and parliamentary) insight into the work of the Security Police.

Another form of scrutiny is the Parliamentary Ombudsman. The jurisdiction of the Ombudsman extends to the police, including the Security Police. The Ombudsman has in fact criticised the Security Police on occasion. However, the Ombudsman will usually refrain from investigating what can loosely be called 'operational decisions'.

The Swedish system of oversight of the Security Police data files was the subject of the scrutiny of the European Court of Human Rights (ECtHR) in the Leander case.[771] The majority of the ECtHR, wrongly as it transpired, accepted that the forms of oversight sketched out above were adequate. However, none of them in practice examined the important issues: the reliability of the intelligence gathered, the adequacy of the routines for filing and the proportionality of a decision to release it in vetting cases. None of these bodies consisted (or today consist) of experts in security matters, their staff resources are limited and they have limited time to devote to investigations of security matters.[772]

In 1996, a new oversight body, the Register Board (*Registernämnden*) was established. The main impetus behind this was the Swedish ratification of the Europol treaty, which resulted in the enactment of the Police Data Act (PDA).[773] However, revelations regarding the inadequacy of the oversight functions, an aftermath of the Leander case, was also a factor in its establishment. The Register Board was given the task, which was previously performed by the NPB, of deciding whether or not to release intelligence from the Security Police files to employers in vetting cases.[774] It thereby also exercised an indirect supervisory role over intelligence filing routines. The Register Board had judges as Chair and Vice Chair and Representatives from the two major Parties in parliament. It took seriously its mandate to weigh possible gains to security against losses to personal integrity involved in releasing speculative or otherwise unreliable intelligence. At around about the same time, the Security Police itself—largely to increase efficiency—weeded out a large number of unnecessary or unreliable personal files and improved its routines for starting, and adding to, files. Senior staff changes following the errors made and illegal activities during the investigation of the murder of PM Olof Palme can also be assumed to have had some significance here. In any event, the combined number of occasions in which security intelligence was released in vetting cases dropped dramatically, from around 70% to between 1.5 per cent to 10 per cent.[775] Moreover, cases in which the vetted person was communicated part of, or the essence of, the allegations against him/her increased considerably.

In the later case of Segerstedt-Wiberg and others v. Sweden,[776] a violation was found of Article 13 of the European Convention on Human Rights (ECHR) because the applicant did

[771] *Leander v. Sweden,* 27 March 1987, A/116. See, generally: Töllborg 1986 and 1999.
[772] See further: Cameron 2000, pp. 225–241 and Cameron and Töllborg 2002.
[773] 1998:622. A new PDA was enacted in 2010 and will enter into force in 2012.
[774] Security Protection Act 1996:627 and Security Protection Ordinance 1996:633.
[775] See: Cameron and Töllborg 2002, p. 197 and SIN Annual Reports 2009 and 2010. The way the vetting system is constructed means that, as the Security Police or SIN take no formal decision regarding employment, the usual basic right of appeal under Swedish administrative law is not applicable. It is the employer who takes the employment decision.
[776] No. 62322/00, 6 June 2006.

not have access to a legal remedy which was capable, in law and practice, of erasing or rectifying data.[777]

In 2007, the Register Board was replaced by the Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden* or SIN).[778] There were several reasons for this. Increased investigative powers had been, or were in the process of being, granted to the police and the Security Police.[779] There was also a realisation that prosecutorial and judicial control only checked if there was reasonable cause to initiate surveillance, and there was no post hoc monitoring. SIN was thus given a follow-up oversight function over surveillance.

SIN consists of, first, two self-contained delegations (Security Screening and Secret Identities), which have authorising functions over, respectively, the release of intelligence in vetting cases and over the use of secret (assumed) identities by the police, and second, a monitoring/complaints body. This construction was chosen because SIN acts as both a control and a remedies body. However, the components are not totally sealed off from each other: the delegations can inform the monitoring/complaints body of information of interest and vice versa.

SIN's mandate is 1) to ensure that surveillance activities by the police, including the Security Police, are conducted in accordance with laws and other regulations and 2) that the Security Police filing of personal data is 'conducted in accordance with laws and other regulations'. These laws etc. include the limits set out on the filing of sensitive data in the constitution (Instrument of Government Chapter 2, Section 6; ECHR Article 8) and in the Police Data Act,[780] as well as the Security Police's own regulations on initiating, adding to, correcting and terminating personal files. Although the mandate is only framed in terms of ensuring compliance with the law, a proportionality test is a fundamental part of this. Proposals have recently been made to extend SIN's mandate to follow-up supervision of police/Security Police access to teledata and police/Security Police use of infiltration methods.[781]

While much of the sensitive work of the Security Police falls within SIN's supervision, not all of it does. SIN has no overall mandate to supervise the work of the Security Police generally, to scrutinise its budget, or to be involved in its management or efficiency (except insofar as these matters overlap its specific mandate). Nor does SIN, as an agency answerable to the government, have oversight over government instructions or security priorities to the Security Police. This is a matter for the parliamentary select committees, KU and JuU.

[777] Following ratification of the Schengen and Europol conventions, the Data Inspection Board (DIB) was given the formal role in monitoring compliance with the requirements of these conventions relating to accuracy, relevance etc. of stored information. It could order rectification/erasure, however, the ECtHR found that it had never done so, and it was, in practice, not competent in matters of security intelligence. Even though it since appears to be developing such competence, it is likely (and sensible to avoid fragmentation of oversight) that it leaves the main task of 'quality control' to SIN.

[778] Act on Supervision of Certain Crime-Fighting Activities 2007:980 ('Supervision Act').

[779] These were, in particular, surveillance powers to prevent crime under certain circumstances (Measures to Prevent Certain Serious Crimes Act 2007:979), bugging (Measures to investigate certain dangerous crimes Act 2008:854) and use of police agents (Act on Qualified Assumed Identities 2006:939).

[780] According to Section 5 of this Act (based on Article 10 of the Europol Convention), a file may not be opened on a person solely on the grounds of what is known about a person's 'ethnic background, political opinion, religious or philosophical conviction, membership in a trade union, health or sexual character'. Such information may, however, be attached to a file, created because of other reasons, if this is absolutely necessary.

[781] See: SOU (Statens offentliga utredningar, Public commission of inquiry) 2009:1 and SOU 2010:103 respectively.

The final issue to be mentioned in this introductory section is oversight of the civilian strategic surveillance (or signals intelligence) agency, the Defence Radio Establishment (*Försvarets Radio Anstalt* or FRA).[782] I will deal only briefly with this, as it is not a focus of the present report. However, occasional comparisons are instructive and will be made between this and the system for oversight of the Security Police.

The proposal in 2008—prepared by the Ministry of Defence, not the Ministry of Justice—to extend the power of FRA from monitoring only ether-borne communications to also monitoring international telecommunications borne by cable caused a major political controversy in Sweden. Although a statute providing for this Act was passed,[783] the government conceded the protections for integrity were inadequate and later added a complicated battery of safeguards.[784] A Defence Intelligence Court was established (*Försvarsunderrättelsedomstolen* or FUD) together with a control and monitoring body, the Defence Intelligence Inspection (*Statens inspektion för försvarsunderrättelseverksamheten* or SIUN).[785] Basically, the system is that the government, the Cabinet office and the defence forces may task FRA to produce foreign intelligence on a particular issue. FRA then requests a warrant from FUD, which sets out what search streams can be used and which signal bearers (i.e., which cables, going to which destinations) can be monitored. The raw intelligence is then delivered by telecom operators to a location physically under the control of SIUN, which monitors whether the conditions set by FUD have been complied with. Communications originating, transiting or terminating in Sweden can be monitored, as well as communications having no connection with Sweden (e.g., satellites passing overhead). The raw intelligence is then transferred for analysis to FRA, which then delivers the product to the body that requested it.

The system is thus a control rather than oversight system, although SIUN also has oversight functions in that it is to monitor whether FRA complies with requirements on handling personal data.[786]

2. ANALYSIS OF OVERSIGHT OF PARTICULAR ACTIVITIES PERFORMED BY SECURITY AND INTELLIGENCE AGENCIES

2.1 Information sharing

The Security Police, being part of the NPB, have automatic access to the other centrally kept police data files. The Swedish Police is organised into 21 separate county authorities and, at the present time, county data registers are kept organisationally separate. If for some reason the Security Police wish intelligence kept by county police forces, it must formally request access to these files, which is likely to be granted without any problems. The same applies to information held by other administrative authorities: the Security Police must prove to the satisfaction of the agency in question that the information is necessary for its investigations.

[782] The Military Intelligence Agency (*Militära underrättelsetjänsten*, MUST) is not permitted to gather intelligence on internal security threats.
[783] Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
[784] Prop. 2008/09:201, Förstärkt integritetsskydd vid signalspaning, 20 May 2009.
[785] See: Security Protection Act 2009:966 and Security Protection Ordinance 2009:969. SIUN oversees also MUST. See: Defence Intelligence Activity Act 2000:130 and Defence Intelligence Activity Ordinance 2000:131 as amended.
[786] Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. DIB has also investigated FRA's practices under this law. The very limited practice so far under the law itself has also been (somewhat prematurely) investigated by a parliamentary commission of inquiry, SOU 2011:13.

As regards exchanges of data between the Security Police and FRA, a major part of the political compromise on improved safeguards for strategic surveillance (above section A) was that the Security Police would no longer have the power to task FRA to collect specific intelligence. However, as is well known, internal and external threats can be inextricably linked in a number of ways. Nonetheless, giving the Security Police direct power to task FRA will involve a paradigm shift in surveillance, which in the long run may risk making law enforcement/security telecommunications surveillance less important or even obsolete (and, incidentally, sidelining the elaborate safeguards applying to this).

The first head of SIN was requested by the government to investigate the issue and propose some sort of compromise solution. His proposal—permitting the Security Police itself to engage in strategic surveillance—was regarded by all political parties (and the Ministries of Defence and Justice) as unacceptable. He, his Deputy and the Staff Director of SIN later resigned. The issue has, however, emerged again after the failed suicide bombing in Stockholm in December 2010 and discussions are ongoing between the government and opposition on how to solve it.

As regards transfers to and from foreign and EU agencies, the Public Access to Information and Secrecy Act 2009:400 permits the revealing of security intelligence to a foreign police or intelligence service or an international organisation.[787] It would appear that the absence of an adequate level of protection for this data in the receiving state does not constitute an insurmountable obligation to transfer of personal data, though it would be a factor to take into account in determining whether it is in Sweden's interest to do so.[788] The government has delegated powers to the NPB to enter into treaties with foreign authorities governing transfer of data.[789] This is an important area which has hitherto been neglected in Sweden (as in many other countries).[790] SIN has, however, recently begun a thematic study on these data transfers and the general arrangements made to protect personal integrity, etc. Other statutes require that conditions set by foreign and EU agencies on the use of data transferred to Sweden be respected.[791]

2.2 Processing and use of personal data

This issue has already been largely examined in sections A and B.i. One point can be added here. The normal rule, designed both to promote efficiency and protect integrity, is that personal data files should normally be terminated (weeded out) ten years after the information came to light that justified registration.[792] However, it is the Security Police that determines whether an incident has occurred, or circumstances exist, which justify continued retention of a personal file. Some security threats (particularly espionage) are of a long-term nature and so the security agencies have a natural tendency to retain older

[787] See: Chapter 8, Section 3, p. 1 in combination with the PDA, Sections 7 and 8 and the Police Data Ordinance (1999:81) (PDO), Section 18. In addition, under Chapter 10, Section 2, an agency may transfer secret information where this is regarded as necessary to fulfil its own functions, even to foreign authorities (Chapter 8, Section 3, p. 2), it is clearly in Sweden's interest to do so. Thus, p. 2 can justify the Security Police transferring data to a foreign authority e.g., if this will facilitate its own ongoing investigations.
[788] The rules in the PDA and PDO are lex specialis, and the 'third country' rule is only to be found in Section 33 of the general *Personal Data Protection Act* 1998:204.
[789] Ordinance 2009:1277, amending Ordinance 1989:773.
[790] See the recommendations in Venice Commission 2007, paras. 177–189.
[791] See: lagen (2000:343) om internationellt polisiärt samarbete, lagen (2000:344) om Schengens informationssystem, lagen (2000:562) om internationell rättslig hjälp i brottmål, lagen (2000:1219) om internationellt tullsamarbete, and lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar.
[792] See: Security Protection Act 1996, Section 35. See now: PDA 2010, Chapter 5, Section 12.

material on the off-chance that this will later turn out to be relevant. SIN has recently initiated a thematic study of the routines of the Security Police in this regard.

2.3 Joint analysis / fusion and dissemination of information

There is a standing working group on threat assessment consisting of representatives from the Security Police, the Military Intelligence Agency (MUST) and FRA. In 2004, the Security Police also established a Counter Terrorism Cooperation Council consisting of representatives from other agencies in law enforcement, etc. The Council's tasks include producing common threat assessments, identifying areas of responsibility and producing a national strategic plan for combating terrorism. There is no body charged with oversight of this Council. However, it is an advisory, not an operative body.

2.4 Collection of open source information

As is well known, a large amount of security intelligence comes from open sources. As mentioned, the Swedish Security Police has greatly expanded its civilian analytical capability since 1990. No special oversight arrangements are provided for Security Police that use open source information. Open source material can admittedly cause problems for individuals, e.g., where it is uncritically used to justify opening, or adding to, personal files. But thresholds for file opening, etc. are within SIN oversight.

2.5 Finances of security and intelligence agencies

Control of the budget of the Security Police and FRA falls formally within the competence of the parliamentary committees on justice and defence. However, the lack of expertise of these bodies and their lack of access to secret information or any operational detail mean that this control is minimal.

3. COMPOSITION

Under Section 5 of the Act on Supervision of Certain Crime-Fighting Activities, SIN shall have a maximum of ten members. These are appointed by the government for a (renewable) fixed period of no more than four years. The members are to be 'suitable for the assignment in terms of judgment, independence, obedience to the law and other circumstances'.

The Chair and Vice Chair shall be, or have been, a tenured judge or have other equivalent legal experience. Experience from the Register Board showed that the integrity and competence of the Chair and Vice Chair were vital to the success of oversight. Appointment of the Chair is preceded by consultations with the heads of the other parties represented in the *Riksdag*.

Unlike the case with the Register Board, all the parties in the *Riksdag* can propose a member of the Commission. Most of the parties have appointed experienced politicians who are nonetheless not active MPs. The main problem is that most of these lack experience in security issues. In these circumstances, a steep learning curve is likely during the first two years.

Decisions are taken by majority vote: there is a quorum when the Chair and half of the other members are present. Any member may request that a meeting should be held but the Chair decides.[793] SIN as a monitoring/complaints body meets around once a month, as do its delegations.

Experience from Canada, inter alia, has shown that the staff of a part-time oversight body can be very important. They get to know the right questions to ask and how to ask them. The staff is also crucial to building a cooperative as opposed to confrontational relationship with the agency. Finally, the staff plays an important role in maintaining continuity of expertise when the membership of the oversight body changes. SIN is assisted by a legally qualified director (appointed by the government) and four to five legally qualified desk officers, as well as administrative staff.

The members of the two delegations are appointed by the government for a fixed period. The Chair and Vice Chair shall be, or have been, a tenured judge or have other equivalent legal experience.[794] The same point about learning curves applies here. As regards the Security Screening Delegation, information may normally be released only if all members of the Delegation are agreed on the decision.

4. METHODS

Section 2 of the Supervision Act provides that SIN exercises its supervision through inspections and other investigations. It takes up a number of cases of its own motion every year. It has adopted a practice of investigating themes or patterns of activity, which can involve scrutinising a large number of individual cases.[795] In this it has been influenced by the positive experiences of the Norwegian oversight committee (which, in turn, has been influenced by the experience of the Canadian body, SIRC). SIN has no role in confirming the appointment of the head of the Security Police. This official has the status of 'General Director' and is, like other heads of administrative agencies, appointed directly by the government after consultations with political parties in the *Riksdag*.[796]

5. INVESTIGATIVE POWERS

Section 3 of the Supervision Act provides that, at the request of an individual, the Commission is obliged to check whether he or she has been the subject of secret surveillance or subject to processing of personal data and whether the use of secret surveillance and associated activities or the processing of personal data was in accordance with laws and other regulations. The Commission has received a large number of complaints from individuals alleging that the Security Police improperly have files on them, all of which require investigation.[797] So far, only one case has been referred to the Chancellor of Justice for a decision as to whether to pay damages. In the long-run, the low level of upheld complaints can naturally create a legitimacy problem for the Commission, even if the vast majority of these complaints are groundless.

[793] Ordinance containing instructions for SIN 2007:1141, Section 19..
[794] Ordinance 2007:1141, Section 15.
[795] Eight were initiated during 2010, of which three concerned the Security Police data files. See: Annual Report 2010, p. 8.
[796] A General Director cannot usually be fired by the government during the period of his or her employment contract (usually four or six years) but a special provision in the Employment Act allows the government to transfer to other duties persons engaged in work of significance to national security.

Regarding the standing oversight work of SIN, Section 4 of the Supervision Act provides that it is entitled to obtain the information and assistance it requests from agencies subject to SIN's supervision. Even courts and agencies that are not subject to its supervision are also obliged to supply it with the information it requests. While SIN cannot compel witnesses to appear before it, failure to cooperate with SIN can, ultimately, be seen as misuse of office and reported as a criminal offence (Criminal Code, Chapter 20, Section 1).[798] However, SIN members must know the right questions to ask. In practice, the main problem is not likely to be outright refusal to cooperate but rather unwillingness on the part of the Security Police to go out of its way to volunteer all the relevant information. Having said this, the Security Police are likely to inform SIN of anything that is seriously wrong, even without a positive statutory duty to do so, on the basis that SIN will probably, and eventually, find out anyway. It can be noted here that SIN is entitled to employ an expert when it considers that specialist knowledge is necessary, and may also invite a person who can provide information in a case to attend a meeting.[799]

The present leadership of the Security Police appears to take a cooperative approach to SIN's investigations. This is sensible as SIN can provide it with both a relatively informed sounding board and extra legitimacy.

In some states, access to security data of foreign origin has been problematic. Where such data enters into personal files, this falls clearly under SIN's mandate. Having said this, as already mentioned, a transferring state may impose restrictions on access to data—even for an oversight body—and, under Swedish law, these restrictions are to be respected. It has not (yet) been put to the test whether this provision can justify refusing SIN access to foreign origin data.
Another restriction is that SIN's mandate in relation to monitoring surveillance applies to the law enforcement agencies (i.e., the police, including the Security Police and the prosecutors). It does not, as such, extend to the courts which authorise the use of such measures. Scrutiny of the adequacy of the reasoning of a court thus is not within SIN's mandate. This restriction is to preserve judicial independence. However, satisfactory oversight here really involves matching the initial suspicions justifying the surveillance against the product of the surveillance. Where a pattern emerges of weighing losses to integrity too lightly against alleged gains to an investigation, SIN should criticise this and demand improvements in routines. This must, reasonably, involve implicit criticism of the body which has authorised the surveillance—the courts.

6. PROTECTION OF OFFICIAL INFORMATION

SIN members and staff are bound by secrecy. The Public Access to Information and Secrecy Act, Chapter 15, Sections 1 and 2, deals with maintaining secrecy for purposes of protection of national security and foreign relations. Chapter 18, Sections 1 and 2 deals with secrecy in the prevention and investigation of crime and in intelligence gathering.

As SIN is an administrative agency, its members (even if they are serving MPs) can be and are security vetted. The same applies to SIUN and FUD (which is regarded as a court). Criminal sanctions for breach of the Act are to be found in the Criminal Code, Chapter 20,

[797] In 2009, there were 65 complaints; in 2010, 720 (Annual Reports 2009, 2010). The latter figure can largely be explained by a newspaper article urging readers to complain to SIN.
[798] A special commission of inquiry, *Säkerhetstjänstkommissionen*, was given such powers as part of its investigation into Security Police activities during the 1970s–1990s, SOU 2002:87. However, it produced little new material: most of the work had already been done by academics and the Register Board.
[799] Ordinance 2007:1141, Sections 20 and 21.

Section 3. Other security crimes in Chapter 19 of the Code (espionage, unlawful revealing of secret information, reckless revealing of secret information) may also be applicable.

To protect the physical security of data files, the Security Screening Delegation tends to meet in the premises of the Security Police. The case-officers who present cases to the Delegation are Security Police staff, who are appointed by SIN for a fixed period. SIN, SIUN and FUD have secure meeting rooms.

7. REPORTING

Section 2 of the Supervision Act provides that SIN 'may make statements on established circumstances and express its opinion'. It can decide to publish special reports, something which is an important feature of oversight. So far, what has been published on its website is mainly information about how it works, in particular its thematic investigations. Parliament may not formally task SIN to look at a particular issue but the fact that the composition of SIN consists mainly of politicians means that the same thing can be achieved informally: where there is a majority for investigating a particular issue, SIN will do so.

SIN reports annually to the government.[800] The report is published. SIN itself decides what information to reveal (albeit applying its duty to keep confidential secret information). If SIN considers that laws or regulations are deficient, it may express its opinion on this, if need be confidentially. Again, both these powers are important features of oversight.[801]

If SIN considers that a criminal offence has been committed, it is to refer the case to the Prosecutor-General. If it considers that errors have been committed in handling of personal data which should be rectified, or which might entitle an individual to damages, it is to refer the case to the Data Inspection Board or the Chancellor of Justice (or both). These bodies make an independent assessment of the need for rectification/damages, so SIN's decision in this regard should be seen as only the first stage in the obtaining of an effective remedy. As mentioned, so far, only one referral has been made to the Chancellor of Justice.

SIN's annual reports tend to be relatively short (12–15 pages of substantive text). They are relatively informative as far as vetting is concerned. Its thematic reporting practices have only just begun and these have, so far, not been presented in any detail as SIN, like any other oversight/complaints body, can always be subject to attack on the basis that it never (or seldom) upholds complaints. One method of countering this difficulty in the future and maintaining public confidence is to reveal as much as it can of its standing oversight activities.

8. CONCLUDING REMARKS

Comments have already been made on good practices. Only four remarks will be made here. The first is that the Swedish oversight system is focused on special investigative powers and data protection. As such, the system is of limited direct relevance for the European Parliament in devising its oversight arrangements. Second, having said this, the Swedish experience is interesting because it supports the view that a pure parliamentary system of oversight is of limited value. To engage in meaningful oversight requires the oversight body to be within the 'ring' of secrecy, to be able to scrutinise operations, not

[800] Ordinance 2007:1141, Section 29.
[801] See, in this regard: Venice Commission 2007, para. 171.

simply policy, and to be sufficiently expert to pose the right questions. Politicians have the democratic legitimacy to question executive action but neither the time, the patience nor the expertise to penetrate adequately the arcane world of security. The solution then, is either a purely expert oversight body, if need be with some form of special briefing/consultation relationship to a parliamentary body, or like the Swedish system, some form of hybrid body. The fact that the political parties choose the members of SIN gives it political legitimacy. The fact that the Director, Chair and Vice Chair are lawyers trained for judicial office is important for the integrity of SIN.

Thirdly, the *proprio motu* investigative, reporting and publication powers of SIN are important: a yearly report to the government is not adequate to allay public fears of misuse. Finally, SIN is both a control body and a remedies body. The latter function is necessary to fulfil the requirements of the ECHR.

REFERENCES

Act on Supervision of Certain Crime-Fighting Activities (22 November 2007), SFS 2007:980 ('Supervision Act'), available at (http://www.sweden.gov.se/sb/d/ 5806/a/95172).

Cameron I. (2000), *National Security and the European Convention on Human Rights*, Iustus/Kluwer, Uppsala/Dordrecht.

Cameron I. and D. Töllborg (2002), 'Internal Security in Sweden' in Brodeur J.P., Gill P. and D. Töllborg (eds.*), Democracy, Law and Security: Internal Security Services in Contemporary Europe*, Ashgate, Farnham.

Defence Intelligence Activity Act (2000), SFS 2000:130.

Defence Intelligence Activity Ordinance (2000), SFS 2000:131.

Police Data Act (1998), SFS 1998:622.

Public Access to Information and Secrecy Act (2009), SFS 2009:400.

Säkerhets- och integritetsskyddsnämnden, Årsredovisning (annual report) 2009, available at (www.sakint.se).

Säkerhets- och integritetsskyddsnämnden, Årsredovisning (annual report) 2010, available at (www.sakint.se).

Security Protection Act (1996), SFS 1996:627.

Security Protection Ordinance (1996), SFS 1996:633.

Ordinance containing instructions for SIN, (2007) SFS 2007:1141

Segerstedt-Wiberg and others v. Sweden (6 June 2006), No. 62322/00.

Töllborg D. (1986), *Personalkontroll*, Symposium, Gothenburg.

Töllborg D. (1999), *Medborgerligt pålitlig?, Norstedts juridik*, Stockholm.

Venice Commission (2007), *Report on the democratic oversight of the security services*, Study No 388/2006.

ANNEX A: COUNTRY CASE STUDIES

IX. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE UNITED KINGDOM

IAN LEIGH

1. INTRODUCTION

Since the 1970s, the United Kingdom has, in common with many other countries, exchanged the tradition of exclusive executive control over the security and intelligence agencies for a measure of parliamentary and judicial scrutiny.[802]

A series of legal challenges in the 1980s under the European Convention on Human Rights (ECHR) forced a modernisation of the legal regime governing the agencies because at that time, interferences with privacy by the agencies were not 'authorised by law' (i.e., in legislation) in the sense required by Article 8 of the ECHR. Moreover, the Convention system required there to be some legal mechanisms for dealing with complaints about abuses and violations of rights. The Security Service Act 1989 established a legal basis for the Security Service and for supervision of the ministerial powers to authorise interference with property by a commissioner, together with a tribunal, to which complaints could be brought. The government estimated correctly that these mechanisms would satisfy the Convention system in the then outstanding cases involving alleged surveillance and recording of personal details by the Security Service.[803] This statutory model was followed in the Intelligence Services Act 1994—extending it to the Secret Intelligence Service (MI6) and the Government Communications Headquarters (or GCHQ, the UK's signals intelligence agency).

Legal reform did not initially result in greater parliamentary oversight. It was not until 1994 that legislation was enacted for scrutiny by a committee representing a cross-section of parliamentary opinion. The Intelligence and Security Committee, established under Section 10 of the Intelligence Services 1994 Act (ISA), comprises nine members drawn from both the House of Commons and the House of Lords. Its task is to examine the expenditure, policy and administration of the three main security and intelligence agencies (the Security Service, the Secret Intelligence Service and the GCHQ).

[802] Lustgarten and Leigh 1994; Born and Leigh 2007; Born, Johnson and Leigh 2005; European Commission for Democracy through Law 2007.
[803] Resolution DH(90) 36 of 13 December 1990.

2. THE GENERAL MANDATE AND FUNCTIONS OF THE RELEVANT OVERSIGHT BODIES

2.1The Intelligence and Security Committee[804]

Oversight of the intelligence and security agencies outside the executive branch now takes place through review by a committee of parliamentarians (the Intelligence and Security Committee) and, in relation to specific surveillance techniques, by judicial commissioners. Neither have a role in advance approval of the agencies' actions nor, in the case of the Committee, is there any legal duty on the services to inform them of major operations or programmes in a timely fashion.

The role of the Intelligence and Security Committee (ISC) is 'to examine the expenditure, administration and policy' of the three services that fall under its jurisdiction.[805] These terms mirror the usual remit given to a departmental parliamentary select committee, despite the fact that the ISC has a different constitutional status. What they apparently omit is the jurisdiction to review security and intelligence operations.

Nor does the legislation specify the standard according to which expenditure, administration and policy are to be examined; for example, whether to a standard of propriety, efficiency or legality. As regards expenditure of the services, although the ISA does not explicitly mention efficiency or value for money, the ISC has in practice regularly criticised expenditure by the services (notably construction and information technology projects) with reference to these measures.

From time-to-time, parliamentary select committees also examine matters related to specific areas of work of the intelligence and security agencies. In 2008–09, for example, the Parliamentary Joint Committee on Human Rights (a Select Committee comprised of members from both Houses) examined the question of alleged complicity of the agencies in torture.[806]

2.2 Jurisdiction of the Commissioners and Tribunal

Ministers are responsible for issuing warrants to the security and intelligence agencies for interception of communications and authorisations for interference with property. The use of these powers is reviewed by judicial commissioners. This arrangement began in the 1980s with the appointment of successive senior judges as judicial monitors for the interception of communications and was then, in effect, put on a statutory basis under the Security Service Act 1989 and the Intelligence Services Act 1994. The current legislation covering the Commissioners is the Regulation of Investigatory Powers Act 2000 (RIPA). The Intelligence Services' Commissioner is responsible for reviewing and reporting upon the issue and authorisation by the relevant minister of warrants for operations involving interference with property (for example, covert searches and placing of surveillance devices) by the agencies.[807] The Interception of Communications Commissioner (established under Section 57 of RIPA) reviews the issue and authorisation of warrants to intercept mail and telecommunications by the intelligence and security agencies and law

[804] For more detailed critical evaluations of the ISC see: Leigh 2007; Phythian 2007; Defty 2008; Gill 2007; Glees, Davies and Morrison 2006.
[805] Intelligence Services Act 1994 (hereafter, 'ISA'), Section 10(1).
[806] Joint Committee on Human Rights, 2009.
[807] Regulation of Investigatory Powers Act 2000 (hereafter 'RIPA'), Section 59.

enforcement organisations. The Commissioners report annually to the Prime Minister on their work and their reports are in turn laid before Parliament, subject to deletions on grounds of national security.

There is also a tribunal, the Investigatory Powers Tribunal (IPT), which is established to investigate public complaints against the agencies or allegations of illegal interception by them.[808] Members of the Tribunal must hold or have held high judicial office or be qualified lawyers of at least ten years' standing. Any person may bring a claim and the IPT must determine all claims brought before it, except those it considers to be vexatious or frivolous.[809]

The IPT is specified as the only appropriate forum for proceedings against any of the intelligence services concerning alleged incompatibility with European Convention rights and for complaints by persons who allege to have been subject to the investigatory powers of the Regulation of Investigatory Powers Act.[810] It has, for example, been held to be the appropriate forum for a challenge to a refusal by the intelligence services to authorise publication of the memoirs of a former officer[811] and for challenges to the decision by any of the agencies to issue a 'Neither Confirm Nor Deny' response to an information or access request.[812] The IPT has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. The IPT is required to follow the principles applicable by a court on an application for judicial review.[813]

The IPT can require anyone involved in the authorisation and execution of an interception warrant to disclose or provide documents and information[814] and to require a relevant Commissioner to provide it with all such assistance as it thinks fit.[815]

At the conclusion of proceedings, the IPT is required to give a simple statement either that they have found in favour of the complainant (i.e., that there has been unlawful action against him or her) or that 'no determination has been made in his favour'.[816] In this way, the Tribunal safeguards information about interception of communications and about the agencies so that its proceedings cannot be used to discover whether or not a person is lawfully under surveillance. The Tribunal has, however, determined that this provision and procedural rules requiring oral hearings to be in private[817] do not prevent it from giving public reasons on preliminary matters of pure legal principle in a way necessary to comply with Article 6 of the ECHR.[818] In the event of a successful claim, the IPT is also required to submit a report to the Prime Minister.[819] The IPT has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling interception warrants and requiring the destruction of any records so obtained.[820] There is no appeal from a decision of the IPT.[821]

[808] RIPA, Section 65.
[809] RIPA, Sections 67(1), (4) and (5).
[810] RIPA, Section 65(2).
[811] *A v. B (Investigatory Powers Tribunal: Jurisdiction)* (2009) UK SC 12.
[812] *Hilton v. Secretary of State for Foreign and Commonwealth Affairs* (2005) UKIT NSA1*; Gosling v. SSHD* (2003) UKIT NSA4*; Hitchens v. SSHD* (2003) UKIT NSA5.
[813] RIPA, Sections 67(2) and 67(3)(c).
[814] RIPA, Section 68(6) and (7).
[815] RIPA, Section 68(2).
[816] RIPA, Section 68(4).
[817] Investigatory Powers Tribunal Rules 2000 (SI 2000/2665).
[818] *Applications Nos. IPT/01/62* and *IPT/01/77* (23 January 2003).
[819] RIPA, Section 68(5).
[820] RIPA, Section 67(7).
[821] RIPA, Section 67(8).

The system of Commissioners and tribunal has been found to satisfy Articles 6, 8 and 13 of the European Convention on Human Rights. In a challenge where the act's complaints machinery had been used unsuccessfully by an applicant, the Commission of Human Rights found that the scheme struck a reasonable compromise between the requirements of defending democracy and the rights of the individual. Accordingly, it held that the complaint was manifestly ill-founded.[822] There are reasons, however, to doubt their overall effectiveness as instruments of accountability or for instilling public confidence due to the tightly prescribed legal jurisdiction within which each operates. There are only four reported examples of findings in favour of complainants by the IPT[823] and it is unclear (since they are unpublished) if these were made against the security and intelligence services (against whom several hundred cases have been brought over nearly two decades).[824] The Commissioners have never found that a warrant or authorisation has ever been improperly issued, although in several dozen instances the agencies have admitted to minor breaches such as entering the wrong phone number or address.

2.3 Deficiencies of the Oversight Regime

There are several gaps in this general oversight scheme. Firstly, some bodies handling intelligence are not included in the legal mandate of the Intelligence and Security Committee, although in practice the ISC has examined their work: the Joint Intelligence Committee, the Assessments Staff and the Defence Intelligence Staff are outside the statutory remit. (It should be noted, however that in practice the ISC has had free access to these bodies on the basis that they are the principal consumers of intelligence produced by the agencies that it oversees without any hindrance or resistance on the part of the government).[825] Secondly, there is no formal link between the Commissioners who review warrants and authorisations issued to the agencies and the ISC. In particular, the ISC has no access to the confidential unpublished parts of the Commissioners' reports to the Prime Minister. In this respect they are outside the barrier of secrecy as regards the oversight of these powers. Thirdly, non-statutory processes have been established by which staff from the agencies can raise ethical concerns arising from their work with the Staff Counsellors for the Security and Intelligence Services (currently a retired Ministry of Defence official).[826] Again, there is no link between these administrative procedures and the legal jurisdiction of the Committee. Even where such ethical points may touch on 'policy', the ISC has shown no interest in its public reports in concerns raised by staff or by whistle-blowers. Fourthly, as discussed further below, the Committee is ill-equipped to oversee international cooperation by UK agencies.

2.4 Oversight of Information Sharing by the Security and Intelligence Agencies

Under the current legal framework, only partial and inadequate oversight of information sharing exists. Cooperation between the police and the Security Service is partially addressed by the Security Service Act 1996, which gives the Service a subsidiary role in investigating serious crime. A domestic fusion centre for counterterrorism work (the Joint

[822] *Esbester v. UK*, App. No. 18601/91 (2 April 1993); *G, H, and I v. UK* (1993), 15 EHRR CD 4; *Kennedy v. UK* Application no. *26839/05*, E CtHR (18 May 2010).
[823] Interception of Communications Commissioner 2010, para. 6.4.
[824] For a detailed breakdown by year until 2005: see *House of Commons Debates*, vol. 436, cols 435-6 w, 12 September 2005.
[825] See Intelligence and Security Committee 1999, paras. 8 ff.
[826] House of Commons, Written Ministerial Statements, 19 June 2009.

Terrorism Analysis Centre or JTAC) was created in June 2003 as the UK's centre for the analysis and assessment of international terrorism. It is housed within the Security Service (since this is the lead agency for counterterrorism in the UK) and is responsible to the Director-General of the Service.[827] Its role is to analyse and assess all intelligence relating to international terrorism, whether domestic or abroad, and to produce threat assessments for other government departments and agencies. Although originally created to improve cooperation between MI5 and the police, following September 11 JTAC membership has broadened to include representatives from 11 government departments. JTAC operates with departmental representation under the wing of the Security Service and without affecting the responsibilities of other departments and agencies. Officers from the police and security and intelligence agencies work within it cooperatively with each bound by their respective mandates. Oversight of the JTAC as an entity in its own right does not fall clearly under legislation governing either the security and intelligence agencies or the police. Bearing in mind, however, the limited nature of its functions, the case for oversight of JTAC is less pressing than for agencies with operational capacity.
Where international cooperation is concerned, the oversight position is even less satisfactory.[828] At a general level, the procedure for political approval of international cooperation agreements between the UK and overseas agencies is opaque at best. Unlike legislation in some of its partner countries, UK law does not stipulate that ministerial approval is necessary or that it require agreements to be shown to an outside review body. It also does not expressly protect the interests of UK citizens under such arrangements. The legislation does not contain clear safeguards against the avoidance of the controls that apply in domestic law through cooperation with foreign agencies or concerning the types of information that may be shared or the purpose of doing so (beyond the statements of the broad statutory aims of the services).

The Intelligence and Security Committee's 2007 investigation into extraordinary renditions has highlighted the limits of existing oversight in this field. In its report, the UK Intelligence and Security Committee concluded, inter alia, that conditions imposed on information given by the Security Service (MI5) and the Secret Intelligence Service (MI6) to the CIA concerning two businessmen resident in the UK subsequently rendered to Guantanamo Bay had been ignored by the CIA.[829] The Committee's published findings were based upon information from UK agencies only.

2.5 Oversight of the Use of Specific Forms of Data

Section 2(2) of the Security Service Act 1989 requires the Director-General to ensure that there are arrangements limiting the collection of information by that Service to that necessary for the proper discharge of the Service's role or for preventing or detecting serious crime. There are equivalent provisions for MI6 and the GCHQ.[830] The Intelligence Services Commissioner has general oversight of these arrangements.

There is no oversight of the use by the agencies of personal data by the Information Commissioner since the security and intelligence agencies are effectively exempted from the Data Protection Act 1998 by a ministerial certificate relating to national security.[831] It is possible, however, to challenge such certificates in the Information Tribunal which, applying

[827] *National Intelligence Machine* 2006, p. 16.
[828] Gill 2009; Leigh 2009.
[829] Intelligence and Security Committee 2007, paras. 111–147.
[830] ISA, Sections 2(2)(a) and 4(2)(a).
[831] Data Protection Act 1998, Section 28(2).

the principles of judicial review, may allow the appeal and quash the certificate.[832] The Information Tribunal did exactly this in 2001 in a challenge brought by Norman Baker MP concerning an alleged file held by the Security Service.[833]

The agencies' expenditure is audited under arrangements with the Comptroller and Auditor General.[834] Review of expenditure of the Services is also explicitly within the jurisdiction of the Intelligence and Security Committee.[835] The Committee and the government have in the past had a long-running disagreement concerning publication of the budgets for the individual agencies (rather that a total 'Single Intelligence Vote'). The Committee has consistently argued that publication of the information is not sensitive, at least provided it is not done every year.[836]

2.6 Composition and Setup of Oversight Bodies

At present, the ISC remains a committee of nine parliamentarians (but not a Select Committee) whose members are appointed from both Houses of Parliament by the Prime Minister after consulting the Leader of the Opposition.[837] Current Minsters of the Crown are legally debarred from being members of the Committee.[838] Certain additional practices have supplemented the statutory provisions, however. The composition has usually been eight members of the House of Commons and one member of the House of Lords. Members have frequently included past holders of ministerial office with experience of responsibility for security and intelligence (including past Foreign, Defence and Home Secretaries) and retired senior civil servants. Unlike a Select Committee, the ISC is governed by legislation, rather than the standing orders of Parliament. This affects the appointment of its members, the procedure it adopts, its powers over witnesses and hearings, and the publication of its reports. Since 2008, however, Parliament has been consulted over the choice of members, although the final decision remains the Prime Minister's.

The ISC appears to work by consensus, perhaps because it meets in private. The Intelligence Services Act 1994 does not prescribe the process for the ISC to reach decisions. The published reports do not record formal disagreement or voting among members of the Committee and nor have there been any published minority reports.

Although the existence of the ISC has done much to redress the democratic deficit concerning security and intelligence in the UK, the Committee is arguably hampered in its work by being too closely associated with the executive—particularly when it tackles controversial topics such as intelligence before the Iraq war, the 7 July 2005 bombings in London and allegations of complicity in torture. The result has been a series of ad hoc inquiries into topics that the ISC has already investigated and published reports on; for example, the Butler review, the special inquest into the 7/7 bombings and the Gibson torture inquiry. The inability of the ISC to produce definitive reports that allay public concern and mistrust surrounding these topics shows that the current oversight regime is now failing in one of its core objectives—providing public assurance that the agencies are acting efficiently and with propriety.

[832] Data Protection Act 1998, Section 28(4) and (5).
[833] *Norman Baker MP v. Secretary of State for the Home Office,* Information Tribunal (National Security Appeals). Additional information available at (http://www.informationtribunal.gov.uk/Documents/ nsap/baker.pdf).
[834] Security Service Act 1989, Section 2(3A)(b); ISA, Sections 2(3)(b) and 4(3)(b).
[835] ISA, Section 10.
[836] Intelligence and Security Committee 2000, paras. 43 ff.
[837] Intelligence Services Act 1994, sections 10(2)(a) and 10(3).
[838] Intelligence Services Act 1994, section 10(2)(b).

The future of the ISC is under review, with a Green Paper on security expected to be published by the government in summer 2011. Other parliamentarians have continued to call for it to be replaced with a Parliamentary Select Committee (Joint Committee on Human Rights 2009). Members of the current ISC are known to favour the same option. It is noteworthy that the last act of the ISC before the 2010 election was to make a series of suggestions for strengthening its own independence by visibly separating itself from the Cabinet Office (it has since moved to separate premises), staffing and ensuring budgetary independence (Intelligence and Security Committee 2010, Appendix A).

2.7 Methods of Oversight

The Committee is proactive in seeking information. In an early report it warned that it expected to be 'properly and promptly informed' by the agencies of their activities, rather than merely responding to requests for information. In this, the Committee was consciously following the congressional oversight model, rather than the more responsive mode contemplated in the legislation.[839]
The Committee conducts both incident-based and thematic studies. The ISC publishes an annual programme of work which it follows from year-to-year, as well as considering topics that may emerge between annual reports in ad hoc reports. It has also on several occasions conducted investigations at government invitation. The ISC does not, however, receive or investigate complaints from individuals.

The ISC has tended to meet frequently (often weekly during the parliamentary session). Typically, it interviews several dozen witnesses each year, visits intelligence establishments and engages in liaison and exchange, both by visiting oversight agencies abroad and receiving such visits. The ISC sees the budgets of the services but does not publish them, except in general terms intermittently. The ISC does not conduct confirmation hearings of senior officials.

2.8 Investigative Powers and Access to Information

The agency heads may refuse to disclose to the ISC 'sensitive information'.[840] This is defined in the 1994 Act to include information that might lead to the identification of sources, other forms of assistance given to the agencies, or operational methods. A second category of 'sensitive information' concerns past, present or future specific operations. Within these categories, refusal of information is discretionary. The head of one of the three agencies may disclose the information if satisfied that it is safe to do so.[841] Moreover, the responsible Minister may order disclosure to the Committee the public interest notwithstanding,[842] overruling the agency head concerned. From a certain point of view, however, the status of the Committee's requests for information is greater than a conventional parliamentary committee since its demands have statutory backing.

There are other limits to the Committee's information gathering powers. It may request 'information' but does not have the power to demand particular documents, even those referring to the policy, administration or expenditure of the agencies. Moreover, the ISC

[839] Intelligence and Security Committee 1996, para. 37.
[840] ISA, schedule 3, paragraph 4. In addition, Ministers have power to withhold 'non-sensitive' materials on grounds similar to those that apply to select committees: ISA, schedule 3, para. 3(4).
[841] ISA, schedule 3, paragraph 3(2).
[842] ISA, schedule 3, paragraph 3(3).

has no right to examine as witnesses officials from the security and intelligence agencies at a level lower than the Director or Director-General.

For the most part, the weak legal entitlements to information are not a major obstacle in the Committee's work because the government and the agencies also have a considerable stake in the public credibility of oversight. All actors are aware that the withholding of information or undermining the ISC would be counterproductive and would likely result in public and parliamentary calls for increased investigative powers.

A key issue in the development of the Committee's work was the acquisition of a proactive investigative capacity. Without this facility, the Committee would be able to hear evidence from witnesses but have no way in which to dig deeper into the performance of the agencies. The 1994 Act made no provision for investigations of this kind, whether by the Committee or any independent official, such as an Inspector-General. It might be argued that in view of the Committee's limited remit, investigation as such was unnecessary since it would venture into operational matters. Nevertheless, the Committee took the view that investigative capacity was necessary since a power of independent verification would give added authority to its findings and so strengthen public confidence in the oversight system.[843] The government agreed to cooperate but without formally changing the powers of the Committee.[844] A retired Deputy Chief of Defence Intelligence was appointed to this role part-time.[845] The Investigator was 'tasked' by the Committee as part of its annual programme of work to investigate and report to it on certain topics. The use of the Investigator ended, however, in July 2004 when the incumbent, John Morrison, gave an extended interview to the BBC's *Panorama* television programme relating to his previous responsibilities as Deputy Chief of the Defence Intelligence Staff. Following this, the ISC decided not to renew the contract because the agencies had indicated they could no longer have trust in their dealings with him.[846] A spokeswoman announced that the ISC did not intend to appoint another investigator.

2.9 The Protection of Information

The ISC has (until now at any event) met only in private session, although this is not a legal requirement and the current Chairman has indicated there may be a place for occasional public hearings in future.[847] In practice, however, most of the evidence and briefings it receives are from the agencies and the other officials and ministers who work with them. An exception was the evidence taken from newspapers over their liaison with the agencies.[848]

As parliamentarians, the members of the Committee do not undergo formal security clearance before appointment, although (in view of the Prime Minister's power to appoint) presumably any imputation of a security risk against a prospective member would act as an informal bar to appointment. The ISC staff, however, are security-cleared. Moreover, members of the Committee and the staff are 'notified' persons under Section 1(1)(b) of the Official Secrets Act 1989 in the same way as officials working with the agencies, so that strict criminal liability for unauthorised disclosure of security intelligence information applies

[843] Intelligence and Security Committee, 1998, paras. 67–9.
[844] Prime Minister, 1998, para. 21.
[845] Intelligence and Security Committee 1999, para. 84.
[846] *BBC News*, 29 October 2004.
[847] Rifkind 2010.
[848] Intelligence and Security Committee, 2005, paras. 80–88.

to them. The Committee meets in secure premises. Incidents of leaking by the ISC have been almost non-existent and relatively minor in any event.

2.10 Reporting

The ISC is legally required to produce an annual report. From time-to-time it also publishes ad hoc reports. Nothing prevents it from also conducting unpublished investigations and there is good reason to believe that it has done so occasionally. The ISC's reports are delivered to the Prime Minister and, thereafter, published with any deletions agreed to on security grounds.[849]

The Prime Minister is able to exclude material from a report, after consulting the ISC, if its publication 'would be prejudicial to the continued discharge of the functions of the agencies'.[850] In the event of disagreement between the Committee and the Prime Minister over material to be deleted from the report, the Prime Minister can insist on excluding material, although to do so would probably be counterproductive if it led to public dissent from the members of the Committee or their resignation en masse. The ISC has stated that in practice, consultation over redactions is extensive and that there has never been an instance in which agreement could not be reached.[851] Despite this, the published reports are regularly criticised in parliament and by commentators for the extent to which material is redacted on security grounds.

The timing of publication is in the hands of the Prime Minister rather than the Committee. The practice has been to publish the government's response at the same time as ISC reports. The reports are debated in Parliament. Nevertheless, the Prime Minister retains control over the timing of publication and the Committee has on occasion criticised delays by the government in publishing its report, in particular the delay before the 2010 general election in publishing its findings on the controversial question of guidance over possible complicity by officers of the agencies into mistreatment of detainees in the hands of foreign agencies.

3. CONCLUSION

Broadly speaking, the UK arrangements conform to the pattern for oversight advocated by the UN Special Rapporteur in that they involve a combination of different institutions with legally-based mandates and include 'civilian' elements independent of the executive.[852] There are, however, some gaps in oversight of compliance with the law because of the focus of the Commissioners and Tribunals on narrow questions concerning specifically approved activities. The ISC fares reasonably well in practice against the standards for implementation of its mandate in terms of freedom of action, access to information and cooperation from the agencies, despite formal limits to its information gathering powers and the lack of an Inspector-General within the UK system.[853]

Concerning redress for complaints against the services by individuals,[854] the Investigatory Powers Tribunal has a wide jurisdiction to hear complaints and to grant remedies. The

[849] ISA, Sections 10(6) and (7).
[850] ISA, Section 10(7).
[851] Intelligence and Security Committee 2010, Appendix A.
[852] UN Special Rapporteur 2010, Practice 6.
[853] UN Special Rapporteur 2010, Practice 7.
[854] UN Special Rapporteur 2010, Practice 9.

deficiencies are more in the vagueness of the powers granted to the agencies (which make a finding of illegality unlikely in the first place) and in the secrecy restrictions placed on the process, which mean it is impossible for a complainant to distinguish between a Tribunal finding based on justifiable use of legal powers and lack of evidence of the services' involvement.

In the case of oversight of information sharing, it is doubtful if the current UK arrangements satisfy the standards proposed by the UN Special Rapporteur.[855] Domestic legislation fails to outline 'clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence'.[856] Nor does it explicitly prohibit the use of foreign intelligence services to circumvent national legal or institutional controls.[857]

The history of the ISC, which has now operated for some 15 years, contains both positive and negative lessons. Positively speaking, working behind closed doors may help to strengthen the bipartisanship and trust that are essential to oversight. The ISC was well ahead of its time in oversight not only of security but also intelligence and signals intelligence. There is a clear need for a holistic approach—reflected in the ISC's practice—that all the relevant agencies and components of the intelligence cycle should fall under oversight. The practice of the committee (contradicting the strict legal position) also shows that trust and cooperation may allow an oversight body to investigate sensitive operational details without damaging leaks. Negatively, however, the UK experience underlines the need for critical distance from the executive to be woven into oversight arrangements (especially in such procedural questions as appointment of overseers and reporting) if public confidence is to be retained. Moreover, in the current climate such is the importance of intelligence sharing that any effective oversight scheme must be designed from the start with this firmly in view.

REFERENCES

A v. B (Investigatory Powers Tribunal: Jurisdiction) (2009), UK SC 12.

Born H., Johnson L. and I. Leigh, eds. (2005), *Who's Watching the Spies: Establishing Intelligence Service Accountability*, Potomac Books, Dulles, Virginia.

Born H. and I. Leigh (2007), 'Democratic Accountability of Intelligence Services' in *Armaments, Disarmament and International Security: Yearbook of the Stockholm International Peace Research Institute 2007*, Oxford University Press, Oxford.

Data Protection Act 1998 (1998), available at (http://www.legislation.gov.uk/ukpga/1998/29/contents).

Defty A. (2008), 'Educating parliamentarians about intelligence: The role of the British Intelligence and Security Committee', *Parliamentary Affairs*, Vol. 61, No 4, pp. 621–641.

Esbester v. UK (2 April 1993), App. No. 18601/91.

[855] UN Special Rapporteur 2010.
[856] UN Special Rapporteur 2010, Practice 31.
[857] UN Special Rapporteur 2010, Practice 35.

European Commission for Democracy through Law (2007), *Report on Democratic Oversight of the Security Services in Council of Europe States, Study 388/2006* (CDL_DEM 2007-001), Strasbourg.
G, H, and I v. UK (1993), 15 EHRR CD 4.
Gill P. (2007), 'Evaluating Intelligence Oversight Committees: The Case of the UK Intelligence Security Committee and the "War on Terror"', *Intelligence and National Security*, Vol. 22, No 1, pp. 14–37.

Gill P. (2009), 'The ISC and the challenge of international security networks', *Review of International Studies*, Vol. 35, pp. 929–941.

Glees A., Davies P. and J. Morrison (2006), *The Open Side of Secrecy: Britain's Intelligence and Security Committee*, Social Affairs Unit, London.

Gosling v. SSHD (2003), UKIT NSA4.

Hilton v. Secretary of State for Foreign and Commonwealth Affairs (2005), UKIT NSA1.

Hitchens v. SSHD (2003), UKIT NSA5.

Intelligence and Security Committee (1996), *Annual Report for 1995,* Cm. 3198.

Intelligence and Security Committee (1998), *Annual Report for 1997–1998,* Cm. 4073.

Intelligence and Security Committee (1999), *Annual Report for 1998–1999,* Cm. 4532.

Intelligence and Security Committee (2000), *Annual Report for 1999–2000*, Cm. 4897.

Intelligence and Security Committee (2005), *Annual Report for 2004–2005,* Cm. 6510.

Intelligence and Security Committee (2007), *Rendition*, Cm. 7171.

Intelligence and Security Committee (2010), Annual Report for 2009–10, Cm. 7844.

Intelligence Services Act 1994 (1994), available at (http://www.legislation.gov.uk/ukpga/1994/13/contents).

Interception of Communications Commissioner (2010), *Annual Report for 2009,* HC 341.

Investigatory Powers Tribunal Rules 2000 (2000), SI 2000/2665, available at (http://www.legislation.gov.uk/uksi/2000/2665/contents/made).

Joint Committee on Human Rights (2009), *23rd Report for 2008–9*, HL 152/HC 230.

Kennedy v. UK (18 May 2010), Application no. *26839/05*, E CtHR.

Leigh I. (2009), 'Changing the Rules of the Game: Some Necessary Legal Reforms to UK Intelligence', *Review of International Studies*, Vol. 35, pp. 1–12.

Leigh I. (2007), 'Parliamentary Oversight of Intelligence in the UK: A Critical Evaluation' in H. Born and M. Caparini (eds.), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Ashgate, Aldershot.

Lustgarten L. and I. Leigh (1994), *In From the Cold: National Security and Parliamentary Democracy*, Oxford University Press, Oxford.

National Intelligence Machinery (2006), HMSO, London.

Phythian M. (2007), 'The British Experience with Intelligence Accountability', *Intelligence and National Security,* Vol. 22, No 1, p. 81.

Prime Minister (1998), *Government Response to the Intelligence and Security Committee Annual Report for 1997–1998*, Cm. 4089.

Regulation of Investigatory Powers Act 2000 (2000), available at (http://www.legislation.gov.uk/ukpga/2000/23/contents).

Rifkind Sir Malcolm (2010), 'Intelligence Oversight in the UK: the Intelligence and Security Committee', Royal United Services Institute.

UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Combating Terrorism (2010), *Compilation of good practice on legal and institutional and measures that ensure respect for human rights by intelligence agencies,* UN General Assembly, A/HRC/14/46.

ANNEX A: COUNTRY CASE STUDIES

X. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN AUSTRALIA

NICOLA MCGARRITY

1. INTRODUCTION

The oversight framework for the Australian Intelligence Community (AIC) is extensive and substantially effective in scrutinising the activities of the AIC. However, one of the main criticisms that could be levelled against this framework is that it is *too* extensive. There are six members of the AIC (see Appendix 1):

- Office of National Assessments (ONA);
- Australian Security Intelligence Organisation (ASIO);
- Australian Secret Intelligence Service (ASIS);
- Defence Signals Directorate (DSD);
- Defence Imagery and Geospatial Organisation (DIGO); and,
- Defence Intelligence Organisation (DIO).

The functions of overseeing the members of the AIC are shared across a large number of governmental, parliamentary, judicial and independent bodies and this is further complicated by the fact that, in addition to the formal statutory arrangements, there are also informal arrangements between these bodies as to which should exercise what functions.

2. MINISTERIAL OVERSIGHT

While this is outside the terms of reference for this case study, it is nevertheless important to note that:

> ...the key accountability mechanism applying to intelligence agencies is their relationship to ministers.... Ministers, individually and collectively, oversee agencies' activities, approve their budgets and, in many cases, ministerial approval is required for individual operations. The sense of accountability to ministers is deeply embedded in the culture of the intelligence agencies. There is no hint in Australia of the semi-detachment from governmental structures and lines of authority that is a feature of some intelligence systems.[858]

There are a number of government committees that oversee and coordinate the activities of the AIC. The National Security Committee of the Department of Prime Minister and Cabinet (NSC) is the focal point of decision making on national security and sets broad policy and priorities for Australia's intelligence agencies. The NSC is chaired by the Prime

[858] Flood 2004, p. 53.

Minister and consists of a number of other relevant Ministers. The other key government committee is the National Intelligence Coordination Committee (NICC). The NICC was established in 2009 and ensures that Australia's national intelligence efforts are fully and effectively integrated and accord with Australia's national security priorities.

3. PARLIAMENTARY OVERSIGHT

3.1 Responsible Government

The principle of 'responsible government' means that the minister overseeing each of the members of the AIC is accountable to Parliament for his or her agency on a day-to-day basis. For example, the Attorney-General (who is a member of both the executive and legislative branches of government) may at any time be asked questions in Parliament regarding the budget or activities of ASIO. In *Church of Scientology v Woodward*,[859] Murphy J of the High Court of Australia stated:

> As part of the executive government, ASIO and its members are subject to the administrative control of the Executive Council and Ministers envisaged by the Constitution: ss 61, 64. The Constitution vests the executive power in the Governor-General and Minister who (except for a three months' period of grace) must be members of the Senate or the House of Representatives. This is the mechanism by which responsible government is secured.[860]

3.2 Annual Reports

ASIO is the only member of the AIC to directly make an annual report to the Parliament. ASIO produces an unclassified annual report for tabling in Parliament, as well as providing a classified annual report to the Attorney-General, the Prime Minister and the Leader of the Opposition on its activities.[861]

The annual unclassified report of the Department of Defence and the annual report of the Inspector-General of Intelligence and Security (IGIS) make broad references to the activities of the DIGO, DSD and the DIO.[862]

The heads of ASIS and the Office of National Assessments (ONA) provide the responsible minister with an annual report on their operations.[863] These reports are not made public. However, both ASIS and the ONA also produce unclassified budget documents.[864]

3.3 Opposition Briefing

Section 21 of the Australian Security Intelligence Organisation Act 1979 (Cth) requires that the Director-General of Security brief the Leader of the Opposition for the purpose of keeping him or her informed on matters relating to security. Similarly, the Director-General of ASIS must consult regularly with the Leader of the Opposition in the House of

[859] *Church of Scientology v Woodward* (1982) 154 CLR 25.
[860] Ibid., p. 64.
[861] Australian Security Intelligence Organisation Act 1979 (Cth), Section 94.
[862] Office of National Assessments 2006, p. 15.
[863] Intelligence Services Act 2001 (Cth), Section 42; Office of National Assessments Act 1977 (Cth), Section 19.
[864] Office of National Assessments 2006, p. 15.

Representatives for the purpose of keeping him or her informed on matters relating to ASIS.[865]

3.4 Parliamentary Joint Committee on Intelligence and Security (PJCIS)

3.4.1 Oversight Responsibilities

Section 29 of the Intelligence Services Act 2001 (Cth) sets out the oversight responsibilities of the PJCIS. The key ongoing responsibility of the PJCIS is to review the administration and expenditure of the AIC on an annual basis. This avoids any significant overlap with the functions of the IGIS (discussed below), which are chiefly to review operational matters and investigate complaints. However, the PJCIS may review any matter in relation to the AIC referred to it by the responsible minister or a resolution of either House of Parliament. This may include scrutinising Bills, such as those subject to a sunset clause, or, more rarely, reviewing substantive operational matters, such as the 2003–4 Parliamentary Inquiry into Intelligence on Iraq's Weapons of Mass Destruction.

3.4.2 Composition

Part 3 of Schedule 1 to the Intelligence Services Act 2001 (Cth) sets out the procedures for the appointment of members of the PJCIS. The PJCIS is made up of five members from the lower house of Parliament (House of Representatives) and four members from the upper house of Parliament (Senate). These members are nominated by the governing party, after consultation with the leaders of any other recognised political party represented in the Parliament. The governing party 'must have regard to the desirability of ensuring that the composition of the Committee reflects the representation of recognised political parties in the Parliament'.[866]

3.4.3 Investigatory Powers

The PJCIS may require a person to give evidence before it or to produce documents.[867] This includes the heads of the AIC and the IGIS. It may not, however, require a person to disclose operationally sensitive information or information that would or might prejudice Australia's national security or the conduct of Australia's foreign relations.[868] The Minister relevant for a particular agency may certify that a person is not to give evidence or produce documents to the PJCIS if he or she is of the opinion that it is necessary to prevent the disclosure of operationally sensitive information. Such a certificate is binding on the PJCIS and may not be challenged in any court or tribunal.[869]

In a report of June 2010, the PJCIS said that it had been provided with 'significant and meaningful information' by the members of the AIC. It did, however, suggest that it would be useful to create a statutory requirement for the members of the AIC to provide the PJCIS with broad information about 'their activities, operations, skills, methods and the product they create'. The availability of this information 'is critical to the capacity of the

[865] Intelligence Services Act 2001 (Cth), Section 19.
[866] Ibid., Section 14.
[867] Ibid., Sections 2, 3.
[868] Ibid., Section 1.
[869] Ibid., Section 4.

Committee to fulfil its obligations and to meet the expectations of the Parliament and the wide community'.[870]

3.4.4 Security of Information

By convention, members of Parliament are not required to have security clearances. They should, however, handle security classified resources (such as those which may be revealed in evidence before the PJCIS) in accordance with the requirements of the Australian Government's Protective Security Policy Framework (January 2011). The ordinary staff of the PJCIS must have security clearances to the same level and at the same frequency as staff members of ASIS (Top Secret Positive Vet).[871]

Part 2 of Schedule 1 to the Intelligence Services Act 2001 sets out a number of offences relating to the unauthorised disclosure of information. For example, it is an offence for a current or former staff member of the PJCIS to make a record, disclose or communicate information acquired as a result of holding the employment, except where the action is carried out for the purposes of enabling the PJCIS to perform its functions.[872]

The PJCIS must make arrangements acceptable to all the heads of the AIC for the security of information held and any records made by PJCIS. It must also ensure that any documents having a national security classification are returned as soon as possible after the members of the PJCIS have examined them.[873]

3.4.5 Reporting

Section 31 requires the PJCIS to prepare and table an Annual Report as soon as practicable after each year ending 30 June. The PJCIS may not, however, disclose to Parliament the identity of a person who is or has been a member of the AIC, any information from which the identity of such a person could reasonably be inferred, or operationally sensitive information or information that would or might prejudice Australia's national security, the conduct of Australia's foreign relations or the performance by an agency of its functions. The PJCIS must comply with the advice of the responsible Minister as to whether the report or part of the report would or might disclose such a matter.[874]

3.5 Senate Estimates

In addition to the oversight of the AIC's finances and administration by the PJCIS, there is an additional budget estimates process. This process involves the twice-yearly referral of estimates of government expenditure to Senate committees as part of the annual budget cycle.[875] This opportunity to examine the operations of government plays a key role in the parliamentary scrutiny of the executive. Senate Standing Order 26(5) provides that the estimates committees 'may ask for explanations from ministers in the Senate, or officers, relating to the items of proposed expenditure'. This may include the heads of the members of the AIC.[876]

[870] Australian Parliament 2010 [1.48]-[1.53].
[871] Ibid., Section 21.
[872] Ibid., Section 12.
[873] Ibid., Section 22.
[874] Ibid., Section 7.
[875] Further information about the estimates process is available at (http://www.aph.gov.au/senate/pubs/briefs/brief05.htm).
[876] See, for example, Australian Security Intelligence Organisation 2010, pp. 54–55.

The Legal and Constitutional Affairs Committee deals with the Attorney-General's Department (which includes ASIO). The Foreign Affairs, Defence and Trade Committee deals with the Department of Defence (which includes DIGO, DIO and DSD) and the Department of Foreign Affairs and Trade (which includes ASIS). The Finance and Public Administration Committee deals with the Department of Prime Minister and Cabinet (which includes the ONA). The IGIS is also accountable to the Senate Finance and Public Administration Committee.

4. OVERSIGHT BY INDEPENDENT BODIES

4.1 Inspector-General of Intelligence and Security (IGIS)

The IGIS is not part of any government department or agency. It is an independent statutory office established under the Inspector-General of Intelligence and Security Act 1986 (Cth).

4.1.1 Oversight Responsibilities

The IGIS is responsible for ensuring that each member of the AIC conducts their activities legally, behaves with propriety, complies with any directions and guidelines from the responsible minister and has regard for human rights.[877] The focus is not, at least in a direct sense, on efficiency or effectiveness or financial management. The responsibilities of the IGIS vary in respect of each of the six members of the AIC and are broadest in respect of ASIO.

4.1.2 Composition

The Inspector-General is appointed by the Governor-General[878] on the advice of the Prime Minister.

Before the Prime Minister makes a recommendation to the Governor-General, he or she must consult with the Leader of the Opposition in the House of Representatives.[879] To ensure the independence of the office, the IGIS is appointed for a fixed term of five years and can be dismissed only on limited grounds.[880] An IGIS cannot be appointed more than twice.[881] He or she is directly accountable to the Prime Minister.

4.1.3 Methods of Oversight

4.1.3.1 Inspections

Inspections usually involve visiting agencies and reviewing selected files or other records or searching on agency systems. Some inspections are regular, for example, ASIO requests for special power warrants are examined each month. Other inspections are done as projects. For example, in 2008 the IGIS searched ASIO records to determine what, if any, information was held relating to currently serving politicians. Currently, a project is being

[877] Inspector-General of Intelligence and Security Act 1986 (Cth), Section 8.
[878] The Governor-General is the Queen's representative in Australia and is appointed by the Queen on the advice of the Prime Minister.
[879] Inspector-General of Intelligence and Security Act 1986 (Cth), Section 6.
[880] Ibid., Sections 26, 30.
[881] Ibid., Section 26(2).

undertaken by the IGIS to examine the policies, procedures and practices of the members of the AIC relating to the exchange of information with foreign organisations.

4.1.3.2 Inquiries

The scope for the IGIS to conduct inquiries is significantly greater than that of the PJCIS. An inquiry may be initiated in one of three ways.

First, the IGIS may conduct inquiries at his or her own motion.[882] For example, in 2007, an inquiry was conducted into the independence and integrity of ONA's strategic assessments.[883]

Second, the IGIS is empowered to receive and investigate complaints about the members of the AIC.[884] Many of these complaints are handled by administrative rather than investigative means. Other complaints are dealt with by way of a preliminary inquiry[885] or by escalation to a full inquiry.[886] In 2005, a number of complaints were made to the IGIS about the treatment of Scott Parkin, a US citizen in Australia on a temporary visa who had been detained and removed from Australia after ASIO issued an adverse security assessment and his visa was cancelled. Similarly, in 2006, a member of the public complained about an adverse security assessment made of Rhuhel Ahmed and the consequential denial of a visa to visit Australia. Ahmed had planned to visit Australia to promote the release of a new film, *The Road to Guantanamo*. The IGIS conducted inquiries into both of these cases.

Finally, inquiries may be conducted at the request of the Prime Minister or responsible Minister. The Prime Minister or responsible Minister may request the IGIS to inquire into a matter relating to an intelligence agency.[887] A former IGIS noted that such requests were not common in practice 'because the office is vigilant and proactive about issues which warrant an inquiry'.[888] One example of such an inquiry was the request in April 2000 by the Minister for Defence that the IGIS inquire into allegations that intelligence information relevant to the deaths of five men at Balibo on 16 October 1975 had not been acted upon.[889] The powers of the Prime Minister to request an inquiry be conducted were expanded in late 2010. The Prime Minister may now request the IGIS to inquire into an intelligence and security matter relating to any Commonwealth agency (as opposed to the IGIS being limited to inquiring into the activities of members of the AIC).[890]

4.1.4 Inquiry Powers

Section 17 specifies that inquiries should be conducted in such manner as the IGIS thinks fit. However, inquiries must be conducted in private. In all other respects, the IGIS has investigatory powers similar to those of a Royal Commission. These include powers to compulsorily obtain information and documents, to enter premises occupied or used by an AIC agency, to issue notices to persons to appear before the IGIS to answer questions

[882] Ibid., Section 8.
[883] Inspector-General of Intelligence and Security 2007. Only the Key Judgments section of this report is unclassified.
[884] Inspector-General of Intelligence and Security Act 1986 (Cth), Section 8, Pt II Div. 2.
[885] Ibid., Section 14.
[886] Ibid., Section 8.
[887] Ibid., Sections 8, 9(1)–(2).
[888] Inspector General of Intelligence and Security 2009, p. 5.
[889] Inspector General of Intelligence and Security 2001.
[890] Inspector-General of Intelligence and Security Act 1986 (Cth), Section 9(3)–(4).

relevant to the matter under inquiry, and to administer an oath or affirmation when taking such evidence.[891]

4.1.5 Security of Information

The IGIS may obtain documents with a national security or protective security classification for the purposes of an inquiry. However, before removing these documents from the possession of the agency, the IGIS must make arrangements with the head of the relevant agency for the protection of those documents while they remain in the IGIS' possession, and for their return.[892]

Section 34 imposes obligations of secrecy on the IGIS and his or her staff. It is prohibited to make a record of, or divulge or communicate to any person any information acquired by reason of being employed as part of the Office of the IGIS.[893] There are very limited exceptions for disclosure of information to a court and to a Royal Commission.[894]

4.1.6 Annual Reports

The IGIS is required to provide an annual report to the Prime Minister of the operations undertaken during that year, including any inquiry or inspection.[895] Before tabling the report in the Parliament, which he or she must do as soon as practicable,[896] the Prime Minister may delete any parts of the report as he or she considers necessary in order to avoid prejudice to security, the defence of Australia, Australia's relations with other countries, law enforcement operations or the privacy of individuals.[897] The full report must be shown to the Leader of the Opposition in the House of Representatives; however, he or she is required to treat as secret any part of the report that is not tabled in a House of the Parliament.[898]

4.1.7 Reports of Inquiries and/or Inspections

There are additional provisions regarding reports of inquiries containing (either expressly or implied) critical views of an individual or Commonwealth agency. In particular, the IGIS must give the individual or the head of the Commonwealth agency an opportunity to make either written or oral submissions in relation to the matter that is the subject of the inquiry.[899] If the views are critical of a Commonwealth agency, the IGIS must also give the responsible minister a reasonable opportunity to discuss the proposed report with him or her.[900]

Even if there are no critical views expressed in a report, the IGIS must nevertheless prepare a draft report setting out his or her conclusions and recommendations and give a copy to the head of the relevant agency or, if the conclusions and recommendations relate to the head of the relevant agency, to the responsible Minister. If the head of the agency or responsible Minister makes comments on the draft report, the IGIS must include such of

[891] Ibid., Sections 18, 19.
[892] Ibid., Section 20.
[893] Ibid., Section 34.
[894] Ibid., Sections 34, 34A.
[895] Ibid., Section 35(1)–(2B).
[896] Ibid., Section 35(4).
[897] Ibid., Section 35(5).
[898] Ibid., Section 35(3).
[899] Ibid., Section 17(4)–(5).
[900] Ibid., Section 17(9).

those comments as are relevant to the final report.[901] Once the final report has been prepared, it must be provided to the head of the agency and/or the responsible Minister (depending upon who the draft report was provided to). If the inquiry was conducted as a result of a request by the Prime Minister, the final report must also be provided to him or her.[902]

If the IGIS completes an inspection of an intelligence agency, the IGIS may report on the inspection to the responsible Minister or the head of the relevant agency.[903]

4.2 Commonwealth Ombudsman

The Ombudsman is an independent statutory office established by the Ombudsman Act 1976. The Act provides that the Ombudsman is to investigate the administrative actions of Australian Government departments and prescribed authorities in response to complaints or on the Ombudsman's own motion.[904] ASIO and the IGIS are excluded from the operation of the Ombudsman Act 1976 (Cth).[905] ASIS, the ONA, the DSD, the DIO and the DIGO fall within the Ombudsman's jurisdiction but, in practice, people seeking to make complaints about them are referred to the IGIS.[906]

4.3 Australian National Audit Office (ANAO)

The ANAO is a specialist public sector agency responsible for auditing the activities of most Commonwealth agencies,[907] including each of the members of the AIC.[908] The head of the ANAO, the Auditor-General, is an independent officer of the Commonwealth Parliament. The extensive powers of the Auditor-General to compel a person to give evidence or produce a document, or to order staff of the ANAO to enter premises, are set out in Part 5 of the Auditor-General Act 1997 (Cth).

The ANAO undertakes annual audits of the financial statements of ASIO, ASIS and the ONA; audits of the Department of Defence that include a consideration of the financial operations of the DIO, the DSD and the DIGO; and occasional performance audits of programs relevant to the intelligence and defence intelligence agencies, usually as part of a wider cross-government consideration of security issues.[909] For example, in July 2010, the ANAO announced that one potential audit was of ASIO's performance in providing security assessments of individuals.[910] These reports must be tabled in the Commonwealth Parliament, as well as being provided to the relevant Minister and to the head of the agency concerned.

4.4 Independent National Security Legislation Monitor

The Independent National Security Legislation Monitor Act 2010 (Cth) established a new office to review the operation, effectiveness and implications of Australia's counterterrorism

[901] Ibid., Section 21.
[902] Ibid., Section 22.
[903] Ibid., Section 25A.
[904] Ombudsman Act 1976 (Cth), Section 5.
[905] Ombudsman Regulations 1977 (Cth), regs. 4, 6.
[906] Australian Law Reform Commission 2004 [2.43].
[907] Auditor-General Act 1997 (Cth), Section 39, pt 4.
[908] Office of National Assessments 2006, p. 16.
[909] Flood 2004, p. 57.
[910] Australian National Audit Office 2010, p. 14.

and national security legislation. The Monitor's role in relation to the AIC is limited. The Monitor may assess legislation relating to the exercise by the AIC of counterterrorism and national security powers. However, it is not permitted to:

(1) Review the priorities of, and use of resources by, agencies that have functions relating to, or are involved in the implementation of, Australia's counterterrorism and national security legislation.

(2) Consider any individual complaints about the activities of Commonwealth agencies that have functions relating to, or are involved in the implementation of, Australia's counterterrorism and national security legislation.

These provisions are intended to minimise any overlap between the functions of the Monitor and those of the IGIS.

5. AD HOC INQUIRIES

The majority of ad hoc inquiries concerning the AIC have been conducted according to the procedures contained in the Royal Commissions Act 1902 (Cth). The power to initiate a Royal Commission lies with the Governor-General (on the advice of the Prime Minister). Some of the most significant inquiries have been:

(1) Royal Commission on Espionage (1954) (Justices WFL Owen, RFB Philp and GC Ligertwood)

This inquiry was established following the defection of two Soviet diplomats, Vladimar and Evdokia Petrov, to Australia. The terms of reference required the Royal Commission to examine whether any acts of espionage had been conducted in Australia by the Soviet Union.

(2) Royal Commission on Intelligence and Security (1974–77) (Justice Robert Hope)

The terms of reference required Hope to report on: the history of the AIC; make recommendations about the future of the AIC to enable them to serve Australia in the most efficient and effective way; recommend procedures for the review of adverse security decisions against individuals; and make recommendations about the machinery for ministerial control, direction and coordination of the security and intelligence services.

(3) Royal Commission on Australia's Security and Intelligence Agencies (1983–84) (Justice Robert Hope)

This inquiry arose out of allegations that David Combe, former National Secretary of the Australian Labor Party, had compromised Australia's national security in his relationship with the First Secretary for the USSR Embassy in Canberra, Valery Ivanov. The Royal Commission found that Combe had been targeted by the Soviets but there was no evidence of intelligence breaches or security threats to Australia.

(4) Commission of Inquiry into the Australian Secret Intelligence Service (1994–95) (Justice Samuels and Michael Codd)

The terms of reference for this inquiry required the Commissioners to enquire into the effectiveness and suitability of existing arrangements for the control and accountability of ASIS, the organisation and management of ASIS, the protection of ASIS intelligence sources and methods, and the resolution of grievances and complaints relating to ASIS, and to consider whether any changes in existing arrangements were required or desirable.

(5) Inquiry into Australian Intelligence Agencies (2004) (Philip Flood)

The focus of this inquiry was on Australia's foreign intelligence agencies, as well as any linkages between these organisations and ASIO.

(6) Independent Review of the Intelligence Community (2011) (Robert Cornall and Rufus Black)

This review is being conducted in accordance with a recommendation of the Inquiry into Australian Intelligence Agencies (2004) that the AIC undergo further examination every five to seven years.

6. ANALYSIS

Given the highly intrusive nature of the powers possessed by the members of the AIC, particularly the domestic intelligence agencies in the counterterrorism context, it is imperative that clear avenues should be apparent for laypersons to make complaints. The IGIS is the key body to whom laypersons may make complaints. However, the IGIS has been strongly criticised for both its lack of transparency and the potential for the government to influence outcomes. Such criticisms were particularly pronounced in the context of a recently announced inquiry into claims that the Australian government was complicit in the rendition to Egypt of Australian citizen and former Guantanamo Bay detainee, Mamdouh Habib. Barrister Greg Barns commented:

> The contrast between an IGIS inquiry and an open judicial inquiry could not be starker. If the allegations made about the treatment of Mr Habib were the subject of a royal commission or some other independent judicial inquiry then it would be entirely up to the head of that inquiry as to how much of the inquiry's proceedings were open to the public, and the report would be his or hers alone and not subject to government editing.
>
> One would have thought that an allegation of Australian involvement, passive or active, in the illegal and notorious rendition activities undertaken by the CIA under the auspices of the war on terror should be subjected to public scrutiny given they involve serious matters of public policy, the rule of law and respect for human rights.[911]

The nature of the powers vested in the members of the AIC make it imperative that any claims of abuses of power should be carefully and openly scrutinised. It is, of course, undeniable that there will be some instances in which it is necessary to keep material relating to the operational activities of intelligence agencies secret. However, there should not be a blanket rule that complaints about intelligence agencies should be heard in private. The onus should rest upon the director of the intelligence agency affected to justify

[911] Barns 2011.

why such secrecy is necessary. Similar arguments could be made in relation to the reporting obligations of the members of the AIC. Each member of the AIC should be required, so far as possible, to produce an unclassified report of its activities for the relevant year.

As already noted above, the IGIS has also been criticised for being beholden to the government of the day or at least too cautious in criticising the AIC. Associate Professor Andrew Lynch commented in relation to the IGIS' inquiry into the Ul-Haque case:[912]

> Without doubt, ASIO will have been relieved by the IGIS report. Despite the judge's remarks [that ASIO officers had committed a number of criminal offences], it found against referring the actions of the two agents to prosecuting authorities, saying there was insufficient evidence of their intention to commit an offence.
>
> That may be the case, but even so the IGIS report is surprisingly mild in tone. No direct criticism of the agents' conduct is among the inspector's formal findings – and yet their actions unquestionably distorted the investigation of Mr Ul-Haque, leading to the botched attempt to prosecute him.[913]

This suggests that even if the formal framework of oversight is adequate, the effectiveness of this framework is strongly dependent upon the attitude of those enforcing it.

In any event, oversight by independent and parliamentary bodies is not sufficient to ensure public confidence in the activities of the AIC. Effective judicial supervision and review is also required. The difficulties with holding intelligence agencies to account for their activities in the judicial arena again centre upon the secrecy that attaches to these activities. Notably, Australia's freedom of information legislation does not apply to the members of the AIC or to the IGIS.[914] The obvious consequence of this is that many persons will be unable to discover whether there are grounds for challenging a decision made by a member of the AIC. Furthermore, even if court proceedings are initiated, the cases of Sheik Mansour Leghaei and Scott Parkin, who both attempted to challenge adverse security assessments made by ASIO, demonstrate how difficult it is to obtain a court order requiring ASIO to produce relevant documents.[915]

[912] Inspector General of Intelligence and Security 2008.
[913] Lynch 2008.
[914] *Freedom of Information Act 1982* (Cth), Section 7 and Schedule 2, Divisions 1 and 2.
[915] For a brief discussion of these cases, see: McGarrity 2008.

7. APPENDIX 1: MEMBERS OF THE AUSTRALIAN INTELLIGENCE COMMUNITY (AIC)

Body	Statutory Basis	Functions	Minister
ONA	Office of National Assessments Act 1977 (Cth)	(1) Assessing and reporting on international matters that are of political, strategic and economic significance to Australia. (2) Co-ordinating the foreign intelligence activities that Australia engages in. (3) Evaluating and reporting on the foreign intelligence activities that Australia engages in having regard to Australia's foreign intelligence priorities and requirements.	Prime Minister
ASIO	ASIO Act 1979 (Cth)	ASIO is Australia's domestic intelligence agency. Its main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's security. This includes providing security assessments and protective security advice, and collecting foreign intelligence in Australia.	Attorney General
ASIS	Intelligence Services Act 2001 (Cth)	(1) Collecting human intelligence about the capabilities, intentions or activities of people or organisations outside Australia. (2) Conducting counter-intelligence activities. (3) Liaising with intelligence or security services of other countries.	Foreign Affairs Minister
DSD	Intelligence Services Act 2001 (Cth)	(1) Collecting geospatial and imagery intelligence about the capabilities, intentions or activities of people or organisations outside Australia from the electromagnetic spectrum or other sources. (2) Providing information security products and services to the government and the Australian Defence Force.	Defence Minister

DIGO	Intelligence Services Act 2001 (Cth)	(1) Obtaining intelligence about the capabilities, intentions or activities of people or organisations outside Australia in the form of electromagnetic energy or electrical, magnetic or acoustic energy. (2) Providing assistance to Commonwealth and State authorities in relation to cryptography, and communication and computer technologies.	Defence Minister
DIO	No statutory basis	(1) Providing all-source intelligence assessments to support Department of Defence decision making and the planning and conduct of Australian Defence Force operations. (2) Maintaining databases for use by the Department of Defence and the Australian Defence Force.	Defence Minister

REFERENCES

Please note that this does not purport to be an exhaustive list of the books, articles etc dealing with the AIC. In particular, there is a wealth of material dealing with the expanded powers of ASIO post-9/11 that I have not included because this topic is outside the scope of this country report.

Auditor-General Act 1997 (Cth), available at (http://www.austlii.edu.au/au/legis/cth/consol_act/aa1997157/).

Australian Law Reform Commission (2004), *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC Report No. 9.

Australian National Audit Office (July 2010), *Audit Work Program – July 2010*, Commonwealth of Australia, available at (http://www.anao.gov.au/uploads/documents/Audit_Work_Program_July2010.pdf).

Australian Security Intelligence Organisation (2010), *ASIO Report to Parliament 2009–10*.

Australian Security Intelligence Organisation Act 1979 (Cth).

Australian Parliament, Parliamentary Joint Committee on Intelligence and Security (June 2010), *Review of Administration and Expenditure No. 8 – Australian Intelligence Agencies* [1.48]-[1.53].

Barns G. (17 January 2011), 'Secret Inquiries into Secret Crimes', Australian Broadcasting Corporation Online, *The Drum Unleashed*, available at (http://www.abc.net.au/unleashed/43038.html).

Born H., Johnson L.K., I. and Leigh, eds. (2005), *Who's Watching the Spies: Establishing Intelligence Service Accountability*, Potomac Books Inc., United States.

Cain F. (2004), 'Australian Intelligence Organisations and the Law: A Brief History', *University of New South Wales Law Journal*, Vol. 27(2), pp. 296–318.

Cain F. (1994), *The Australian Security Intelligence Organisation: An Unofficial History*, Spectrum Publications, Australia.

Carnell Ian (24 October 2006), 'Accountable Intelligence Agencies – Not an Oxymoron', Paper delivered at the National Security and Counter-Terrorism Summit.

Carnell I. and N. Bryan (March 2006), 'Watching the Watchers: How the Inspector-General of Intelligence and Security Helps Safeguard the Rule of Law', *Administrative Review*, No 57, pp. 33–48.

Chalk P. and W. Roseanau (2004), *Confronting 'The Enemy Within': Security Intelligence, the Police and Counterterrorism in Four Democracies*, Rand Corporation, United States.

Church of Scientology v Woodward (1982) 154 CLR 25, available at (http://www.austlii.edu.au/au/cases/cth/high_ct/154clr25.html).

Cotton J. and J. Ravelhill (eds) (2007), *Trading on Alliance Security: Australia in World Affairs, 2001–2005*, Oxford University Press, United Kingdom (especially James Cotton, 'After the Flood: Foreign Policy and the Management of Intelligence', pp. 329–351).

Flood P. (July 2004), *Report of the Inquiry into Australian Intelligence Agencies.*

Freedom of Information Act 1982 (Cth), available at (http://www.austlii.edu.au/au/legis/cth/consol_act/foia1982222/).

Gordon S. (November 2005), 'Re-shaping Australian Intelligence', *Security Challenges*, No 1(1), pp. 27–58.

Gyngell A. and M. Wesley (2003), *Making Australian Foreign Policy*, Cambridge University Press, United Kingdom.

Hocking J. (2004), *Terror Laws: ASIO, Counter-Terrorism and the Threat to Democracy*, University of New South Wales Press, Australia.

Hubbard P. (December 2005), 'Freedom of Information and Security Intelligence: An Economic Analysis in an Australian Context', *Open Government: A Journal on Freedom of Information*, No 1(3), pp. 4–22.

Inspector General of Intelligence and Security (May 2009), *Submission on Issues Paper 35: Review of the Royal Commissions Act*.

Inspector General of Intelligence and Security (2008), *Report of Inquiry into the Actions Taken by ASIO in 2003 in Respect of Mr Izhar Ul-Haque and Related Matters*.

Inspector-General of Intelligence and Security (December 2007), *Report on the Independence and Integrity of ONA Assessments*.

Inspector General of Intelligence and Security (September 2001), *Balibo Inquiry – Balibo Killings 1975 and Intelligence Handling – A Report of an Inquiry by the Inspector-General of Intelligence and Security*.

Inspector-General of Intelligence and Security Act 1986 (Cth), available at (http://www.austlii.edu.au/au/legis/cth/consol_act/ioiasa1986436/).

Intelligence Services Act 2001 (Cth), available at (http://www.austlii.edu.au/au/legis/cth/consol_act/isa2001216/).

Lee H. P. (October 1989), 'The Australian Security Intelligence Organisation – New Mechanisms for Accountability', *International and Comparative Law Quarterly*, No 38, pp. 890–905.

Lynch A. (21 November 2008), 'AFP and ASIO Under Spotlight Over Terrorism Cases', *The Australian*.

McGarrity N. (2008), 'Review of the Proscription of Terrorist Organisations: What Role for Procedural Fairness?', *Australian Journal of Administrative Law*, Vol. 16, pp. 45–66.

McKnight D. (1994), *Australia's Spies and Their Secrets*, Allen and Unwin, Australia.

Marr D. and M. Wilkinson (2003), *Dark Victory*, Allen and Unwin, Australia.

Office of National Assessments (2006), *The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight.*

Office of National Assessments Act 1977 (Cth), available at (http://www.austlii.edu.au/au/legis/cth/consol_act/oonaa1977298/).

Ombudsman Act 1976 (Cth), available at (http://www.austlii.edu.au/au/legis/cth/consol_act/oa1976114/).

Ombudsman Regulations 1977 (Cth), available at (http://www.austlii.edu.au/au/legis/cth/consol_reg/or1977223/).

Richelson J. and D. Ball (1985), *The Ties that Bind: Intelligence Cooperation between the UK/USA Countries, the United Kingdom, the United States of America, Canada, Australia and New Zealand*, Allen and Unwin, Australia.

Swieringa M. (Autumn 2006), 'Intelligence Oversight and the War on Terrorism', *Australasian Parliamentary Review*, No 21(1), pp. 135–142.

Toohey B. and W. Pinwill (1989), *Oyster: The Story of the Australian Secret Intelligence Service*, William Heinemann, Australia.

Weller G. R. (1999), 'Oversight of Australia's Intelligence Services', *International Journal of Intelligence and Counterintelligence*, No 12(4), pp. 484–503.

Wright-Neville D. (2010), 'The Australian Intelligence Community', *Democratic Oversight of Intelligence Services*, pp. 33–58.

WEBSITES

Much of the basic information contained in this country report has been taken from the websites of the members of the AIC and the IGIS. These websites are:

ONA – www.ona.gov.au
ASIO – www.asio.gov.au
ASIS – www.asis.gov.au
DIGO – www.defence.gov.au/digo
DIO – www.defence.gov.au/dio/
DSD – www.dsd.gov.au
IGIS – www.igis.gov.au

ANNEX A: COUNTRY CASE STUDIES

XI. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN CANADA

CRAIG FORCESE

1. OVERVIEW

The Canadian civilian national security sector contains a large number of agencies. Given the mandate of this project, in this paper I shall focus on the two most important civilian national security agencies. These bodies are: the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP).

1.1 Canadian Security Intelligence Service

The Canadian Security Intelligence Service Act[916] created CSIS and charged it with several functions, the most important of which is listed in Section 12: collecting, analysing and retaining information and intelligence on 'threats to the security of Canada'.[917] CSIS is, therefore, principally a 'security intelligence' agency. It does not conduct law enforcement functions.

The expression 'threats to the security of Canada' is carefully defined in Section 2 of the statute. Probably by necessity, each of the categories of threat found in Section 2 is broad and vague, and thus capable of expansive definition. Reduced to its core, the concept of 'threat' includes espionage and sabotage, detrimental foreign-influenced activities, political violence and terrorism, and subversion.

CSIS's Section 12 security intelligence function is not geographically limited. It may and does operate abroad in performing this function. However, unlike some allied agencies, CSIS is not principally concerned with extracting foreign intelligence; that is, intelligence relating to something other than threats to the security of Canada.

1.2 The Royal Canadian Mounted Police

A second key agency is the Royal Canadian Mounted Police. Constituted by the Royal Canadian Mounted Police Act,[918] the RCMP is Canada's national police force and performs policing functions in relation to drugs and organised crime, financial crimes and border integrity. While primarily a law enforcement body, the RCMP has historically also played an important national security function.

[916] Canadian Security Intelligence Service Act, RSC 1985, c C-23, Section 3 (hereafter the 'CSIS Act').
[917] CSIS Act, Section 12.
[918] Royal Canadian Mounted Police Act, RSC 1985, c R-10, Section 3 (hereafter the 'RCMP Act').

Most obviously, the RCMP performs a protective policing role, providing security for federal political leaders, judges and internationally protected persons, such as diplomats, and acting as aircraft protective officers on select flights.[919]

The RCMP is also charged with investigating criminal acts of sufficient gravity to be a national security threat—that is, conduct that is both criminal and falls within the definition of a 'threat to the security of Canada' as that term is used in the CSIS Act. More than that, the Security Offences Act charges the RCMP with 'apprehension of the commission' of these offences, tasking the police force with a pre-emptive function and not simply a reactive role.

2. THE MANDATE AND FUNCTIONS OF RELEVANT OVERSIGHT AND REVIEW BODIES

It is important to note at the outset that Canada does not possess an overarching, specialised national security or intelligence review body. Instead, most review is conducted by review bodies focused on specific security or intelligence agencies, subject to occasional involvement by other bodies whose subject matter jurisdiction is general and may occasionally implicate intelligence agencies (e.g., data protection agencies).

2.1 The Question of a Parliamentary Role

It is also notable that Canada does not have a statutorily-created 'committee of parliamentarians' involved in national security accountability. Nevertheless, both the Senate and the House of Commons have national security and defence committees.[920]

In principle, these regular parliamentary committees could play a key role in holding Ministers (and, de facto, their officials) to account. It is true that members of these parliamentary committees are not security cleared and in the regular course are not provided with protected information, whether of Canadian or foreign origin. Research assistance may be provided by the Library of Parliament, but these individuals are not themselves security cleared, given access to protected information or necessarily subject matter experts.

Nevertheless, Parliament has powers to summon and even compel the appearance of officials,[921] including Ministers,[922] and parliamentary committees may 'send for persons, papers and records'.[923] Parliament and its committees may administer oaths requiring truthful responses,[924] a rarely utilised power. Parliament (and by extension, its committees) also possesses contempt powers[925]—that is, the power to impose a sanction for non-cooperation.

[919] RCMP, *Protective Policing*, available at (www.rcmp-grc.gc.ca/pp/protect-policing-police-eng.pdf).
[920] Standing Senate Committee on National Security and Defence; Special Senate Committee on the Anti-terrorism Act; House of Commons Standing Committee on Public Safety and National Security; House of Commons Standing Committee on Defence.
[921] Lee 1999.
[922] Ibid., p. 129 ('[u]nder the law, Ministers of the Crown enjoy no special status or privilege before the House or a committee').
[923] Parliament of Canada, House of Commons *Standing Orders of the House of Commons…*, Order 108(1).
[924] Parliament of Canada Act, RSC 1985 c P-1, Sections 10–13.
[925] Maingot 1997, p. 193.

Of note in relation to these powers is recent controversy over Parliament's capacity to extract protected information from the executive over Canada's military deployment in Afghanistan. In April 2010, the House of Commons Speaker ruled that the House of Commons can, as a matter of parliamentary privilege, compel the government to produce uncensored documents relating to the transfer of Afghan detainees to Afghan authorities by the Canadian Forces. He also opined that Parliamentarians and the executive branch might wish to concoct a compromise solution rather than compel the documents that could truly prejudice national security—indeed, that was the ultimate outcome with documents now being vetted by a panel of former judges prior to being supplied to a special, ad hoc parliamentary committee.

This is the only time in Canadian parliamentary history in which Parliament insisted on viewing protected information, and persisted to the point of compelling a ruling of the Speaker on parliamentary privilege, and the Speaker's ruling on this point represents the first intervention by that official in such a matter.

The more typical pattern is for parliamentary committees—and Parliament as a whole—not to play a systemic or concentrated role in reviewing the activities of Canada's security agencies. Indeed, some critics describe their performance in this area as utterly inadequate.[926]

The shortcomings of parliamentary review extend to what should be a pre-eminent parliamentary role: examining (at least) security agency financing. In practice, in this as in other areas, Parliament's scrutiny has been modest (and, in some cases, close to token). At least for the last two budgetary cycles, the House of Commons Standing Committee on Public Safety and National Security has apparently dealt with the total budget of not only CSIS and the RCMP but also other (very large) agencies that fall within the Department of Public Safety in a single two-hour meeting.[927]

2.2 CSIS Oversight and Review

2.2.1 Oversight

Institutionally, CSIS is headed by a Director, charged with the 'control and management of the Service' under the direction of the Minister of Public Safety.[928] The latter is specifically empowered to 'issue to the Director written directions with respect to the Service'.[929] The Director, meanwhile, is obliged to consult the Deputy Minister of Public Safety on 'the general operational policies of the Service' and on any other matter that the Minister directs.[930]

These and other provisions in the Act create a more aggressive level of political oversight than exists for law enforcement (which enjoys greater 'police independence' in Canadian law).

[926] See, e.g., Bland & Rempel 2005, p. 1.
[927] Parliament of Canada, House of Commons, Standing Committee on Public Safety and National Security, *Minutes of Proceedings*, 18 March 2010.
[928] CSIS Act, Subsection 6(1).
[929] CSIS Act, Subsection 6(2).
[930] CSIS Act, Section 7.

2.2.2 Composition of Review Bodies

CSIS is also subject to several layers of review by specialised review agencies—that is, bodies that conduct post hoc assessment of past actions. First, the CSIS Director is obliged to prepare reports on the operational activities of CSIS on an annual basis, or more frequently on demand of the Minister of Public Safety, and to submit these documents to the Minister and the CSIS Inspector General.[931] This latter official is appointed by the Governor-in-Council (essentially, the federal Cabinet) and is responsible to the Deputy Minister of Public Safety.

Described as the minister's 'eyes and ears' in the Service, the Inspector General monitors compliance by the Service with its operational policies and examines its operational activities.[932] To this end, the Inspector General is given full access to CSIS's information, except Cabinet confidences.[933] The Inspector General certifies whether the reports provided by the Director are adequate and whether they reveal any action of the Service that the Inspector General views as an unauthorised, unreasonable or unnecessary exercise of its powers.[934]

The Minister transmits the Inspector General's report and certificate to a second body, the Security Intelligence Review Committee (SIRC).[935] The executive appoints the members of SIRC for five-year terms, after consultation with the leaders of official parties in the House of Commons.

2.2.3 Investigative Powers and Access to Information

Like the Inspector General, SIRC has broad rights to CSIS information.[936] It may not see Cabinet confidences but is entitled to all other information in the Service's possession, including data supplied to CSIS by foreign governments and agencies.[937] In SIRC's words, 'SIRC has the absolute authority to examine all of the Service's activities, no matter how sensitive and no matter how classified that information may be'.[938]

Members of SIRC and its employees must comply with all security requirements under the CSIS Act and take an oath of secrecy.[939] They are also 'persons permanently bound to secrecy' under the Security of Information Act[940] (Canada's official secrets law) and are therefore subject to that statute's criminal penalties for wrongful disclosure of sensitive information.

SIRC researchers generally review sensitive CSIS materials in secure SIRC offices at CSIS facilities. There will be some instances, however, when information is moved to SIRC's own facilities, not least in instances where that information is at issue in complaints adjudicated before SIRC.

---

[931] CSIS Act, Section 33.
[932] CSIS Act, Section 30.
[933] CSIS Act, Section 31. Cabinet confidences are, in essence, the papers supporting or describing Cabinet deliberations. For a definition of these papers, see Canada Evidence Act, Section 37; Access to Information Act, Section 69.
[934] CSIS Act, Section 33.
[935] Ibid.
[936] CSIS Act, Subsection 39(2).
[937] O'Connor and the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism…,* at 278.
[938] SIRC, 'Frequently Asked Questions'.
[939] CSIS Act, Section 37.
[940] Security of Information Act, RSC 1985, c O-5.

2.2.4 Functions

SIRC is tasked with, among other things, reviewing the performance by the Service of its duties and functions, including reviewing reports of the Director and certificates of the Inspector General.[941] SIRC may order the Inspector General to complete a review or may conduct its own review, where deemed more appropriate than a review by CSIS or the Inspector General, '[f]or the purpose of ensuring that the activities of the Service are carried out in accordance with this Act, the regulations and directions issued by the Minister… and that the activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers'.[942] For example, in examining operational matters (such as targeting, management of human sources and information-sharing with other foreign and domestic agencies), SIRC ascertains whether 'the Service had reasonable grounds to suspect a threat to the security of Canada; the level and intrusiveness of the investigation was proportionate to the seriousness and imminence of the threat; and the Service collected only that information strictly necessary to fulfil its mandate to advise the Government of a threat'.[943] In essence, SIRC is principally concerned with reviewing CSIS activities for legality and compliance with prescribed policies and procedures. In the last two years, however, SIRC has adopted a broader approach, going beyond compliance review to inquire as to whether, for instance, CSIS has effectively allocated resources to such things as investigations and relationships with partners.

In describing its review process, SIRC notes that:

> SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work. As part of this process, researchers may arrange briefings with CSIS employees, as well as examine individual and group targeting files, human source files, intelligence assessments and warrant documents, plus files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources that vary between reviews. The goal is to create a diverse pool of information so that SIRC can ensure it has thoroughly reviewed and completely understood the issues at hand.[944]

Among the specific matters that the CSIS Act charges SIRC with reviewing are the information-sharing arrangements entered into by CSIS with domestic Canadian and foreign agencies and police services. In fact, SIRC has conducted semi-regular reviews of international[945] and, in the more distant past, domestic information-sharing.[946]

SIRC has also reviewed the Integrated Threat Assessment Centre (ITAC),[947] a body created in 2004 and hosted by CSIS. ITAC's primary function 'is to produce comprehensive threat assessments, which are distributed within the intelligence community and to relevant first-

[941] CSIS Act, Section 38.
[942] CSIS Act, Section 40.
[943] SIRC, *Annual Report* 2003–2004, p. 16.
[944] SIRC, *Annual Report 2009–2010*.
[945] See, e.g., SIRC, *Review of CSIS's Exchanges of Information with Close Allies*; SIRC, *Review of CSIS's collaboration and exchanges of intelligence post-9/11*; SIRC, *Review of Foreign Arrangements with Countries Suspected of Human Rights Violations*. See: SIRC, 'List of SIRC Reviews'.
[946] SIRC, *Domestic Exchanges of Information 1999–2000*.
[947] SIRC, *Review of the Integrated Threat Assessment Centre*.

line responders, such as law enforcement, on a timely basis'.[948] It is staffed with personnel from various government security-related agencies.

SIRC reports of this sort are confidential and are not released publicly—although redacted versions are sometimes acquired by members of the public and press through the Access to Information Act, discussed below.

SIRC also has a complaints function. The most generic complaint concerns 'any act or thing done by the Service'.[949] Examples include allegations of unreasonable delays in CSIS security screening and of improper investigation of lawful activities.[950] Any person may make such a complaint concerning CSIS, directed first to the CSIS Director. SIRC may investigate non-frivolous, good faith complaints if the Director fails to respond in a period of time the committee views as reasonable, or provides an inadequate response.[951] These investigations are held in private, subject to a right by the parties to make representations on at least an *ex parte* basis (that is, in private, without the complainant).[952] In balancing national security and fairness, SIRC may disclose summaries of evidence produced on an *ex parte* basis to the other parties.[953] In *ex parte* proceedings, a senior SIRC counsel (or in some instances, an outside legal agent retained by SIRC) 'will cross-examine witnesses on [the complainant's] behalf and may provide [the complainant] with a summary of the information presented in [the complainant's] absence'.[954] In performing its investigative functions, the committee has broad powers to subpoena persons and documents.[955]

The outcome of the SIRC investigation is conveyed to the Minister and the CSIS Director, along with SIRC's recommendations. SIRC recommendations are not binding on the government.[956] The complainant is also notified of the committee's finding,[957] subject to security requirements on disclosure of information.[958]

SIRC also has more general reporting functions. It prepares special reports where requested by the Minister or at any other time[959] and an annual report, tabled by the Minister in Parliament,[960] which in practice contains summaries of the committee's investigations and is a public document.

2.2.5 Financing

In discussing its review function, SIRC notes '[b]ecause of the small size of SIRC in relation to CSIS, the Committee operates on the basis of risk management. Since it is not capable of examining all of the Service's activities in any given period, it must carefully choose which issues to examine'.[961] It is perhaps significant that while CSIS has increased in size and budget since 9/11, SIRC has not grown proportionately (although it has grown in

[948] CSIS, *Backgrounder No. 13…*, July 2006.
[949] CSIS Act, Section 41.
[950] O'Connor and the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism…,* at 274.
[951] CSIS Act, Section 41.
[952] CSIS Act, Section 48.
[953] SIRC, *Rules of Procedure of the Security Intelligence Review Committee in Relation to its Function under Paragraph 38(C) of the Canadian Security Intelligence Service Act (1985),* Section 48.
[954] SIRC, 'Complaints'.
[955] CSIS Act, Section 50.
[956] *Thomson v. Canada (Deputy Minister of Agriculture)*, (1992), 1 SCR 385 (Supreme Court of Canada).
[957] CSIS Act, Section 52.
[958] CSIS Act, Section 55.
[959] CSIS Act, Section 54.
[960] CSIS Act, Section 53.
[961] SIRC, 'List of SIRC Reviews'.

absolute terms). SIRC had a staff of 20 and a total budget in 2008–09 of CAD$2.4 million. Its budget in 2000–01 was CAD$1.8 million, with a staff of 16. In comparison, CSIS had 2910 full time personnel in 2008–09, up from 2091 in 2000–01, and a budget of CAD$430 million in 2008–09, up from CAD$248 million in 2000–01. Put schematically, the comparison of CSIS and SIRC resources is as follows:

Table 1: Change in Resources (2000-2009)

	Budget	Personnel
CSIS	+173%	+133%
SIRC	+139%	+125%

2.2.6 Concerns

Critiques of SIRC are relatively muted, and indeed SIRC has a relatively low profile and its reports generally attract little attention in the media. To summarise, however, the complaints of which this author is aware from discussions with the policy and legal community:

1. SIRC's public, annual reports are generally opaque and anodyne. In many instances, they may provide insufficient bases for parliamentarians or members of the public to assess independently CSIS activities.
2. SIRC critiques of CSIS performance are often reactive rather than proactive; that is, they respond to behaviour or instances already raised by others rather than independently unearthing doubtful activities.
3. The SIRC complaints process is a frustrating and time-consuming expenditure of effort, with little appreciable gain for the complainant given SIRC's lack of meaningful powers to compel a change of CSIS or government behaviour.

2.3 RCMP Oversight and Review

For its part, the RCMP is headed by a Commissioner who, 'under the direction of the Minister [of Public Safety], has the control and management of the Force'.[962] In reality, however, the level of ministerial direction is constrained by the concept of police independence.

Police independence is a common law construct, now with a constitutional imprimatur.[963] At its core, it means that the police (in performing at least their criminal investigation role) are not agents of the Crown or under the direction of the political executive. This doctrine attempts to remove political influence from ordinary police decision making.

Perhaps because of concerns about police independence, the RCMP is also subject to a much less robust form of 'review'—that is, after-the-fact assessment of performance—than is CSIS. Unlike CSIS, the RCMP had no specialised national security review mechanism at the time of this writing. At best, review was conducted through the Commission of Public Complaints (CPC) against the RCMP.[964] The CPC does not perform the sort of auditing function undertaken by SIRC—that is, it does not conduct reviews of the sort discussed above. Instead, it addresses complaints concerning RCMP conduct. Even in relation to

[962] RCMP Act, Section 5.
[963] *R v. Campbell*, (1999) 1 SCR 565 (Supreme Court of Canada), para. 29.
[964] RCMP Act, Section 45.29.

complaints, however, the CPC does not have the same powers as do SIRC to view secret information. The CPC's former chairs have repeatedly underscored the body's failings as an effective review body in the national security area[965] and these persons have recommended an enhanced CPC, a call echoed by other bodies.[966]

By the time of this writing, however, the government had tabled a bill in Parliament that would strengthen the CPC but would still not give it SIRC-like powers.[967] In essence, the new bill would make the RCMP itself competent to decide whether the national security information being sought by the Commission is relevant and necessary to that body's work, subject to a subsequent assessment by a former judge that is not binding.

2.4 Officers of Parliament

'Officer of parliament' is the term given to a series of special review bodies established in a select area whose members are appointed jointly by the executive and Parliament, enjoy substantial security of tenure and report directly to Parliament rather than to Parliament via the executive.

Three of these officers perform functions of potential relevance in national security matters.

2.4.1 Information and Privacy Commissioners

First, Canada has a freedom of information law—the Access to Information Act—that permits Canadian citizens and residents to request information in the possession of government. Not surprisingly, there are numerous exceptions allowing the government to deny access to this information, including several related to national security. In most instances where a provision of the Act is invoked to deny access, the requester may complain to a special 'officer of parliament' created by the Act—the Information Commissioner.

This Commissioner has extensive powers to conduct investigations, but has no power to compel the release of the information to the requester if the Commissioner feels that such release is warranted. Instead, to compel disclosure, the Information Commissioner, or any requester dissatisfied with the outcome of the Commissioner's investigation, must bring an application in the Federal Court.[968]

The Privacy Commissioner performs a function analogous to the Information Commissioner in relation to personal information held by the government. A Canadian citizen or resident may request personal information about themselves from the government, subject to exceptions (including several related to national security) whose use may be scrutinised after a complaint by the Privacy Commissioner.

The Privacy Commissioner is also charged with policing the use to which personal information is put by the government. The government must generally keep a record of the

[965] See, e.g., Heafey 2005.
[966] O'Connor and the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism…,* at 118.
[967] The bill terminated when Parliament was dissolved in April 2011 for an election. However, the same political party was returned to government after the election and the same law project seems likely to be re-introduced into the new Parliament.
[968] Access to Information Act, RSC 1985, c A-1, Sections 41 & 42.

use to which personal information is put, as well as any reason for which this information is disclosed within and between governments.

Where the government uses or discloses personal information in a fashion inconsistent with the Act, an individual may make a complaint to the Privacy Commissioner, triggering significant investigative powers. The Privacy Commissioner may also initiate an investigation on his or her own where he or she concludes that there are reasonable grounds.[969]

Where the Commissioner concludes that a government institution has failed to comply with these protections, he or she provides the head of that institution with a report setting out findings from the investigation and the Commissioner's recommendations.[970] This report may subsequently be included in the Privacy Commissioner's annual report to Parliament.[971]

2.4.2 Auditor General

Lastly, Canada also has a federal Auditor General. The Auditor General is 'the auditor of the accounts of Canada, including those relating to the Consolidated Revenue Fund'[972] (that is, the government's income). The Auditor General is also charged with reviewing the government's annual financial statement.[973] The Auditor General tables an annual report in Parliament[974] and may file other reports on matters of pressing urgency.

The Auditor General Act indicates that the 'Auditor General is entitled to free access at all convenient times to information that relates to the fulfillment' of his or her responsibilities and he or she 'is also entitled to require and receive from members of the federal public administration such information, reports and explanations as he deems necessary for that purpose', except where this authority is expressly excluded in another statute.[975]

The Auditor General has occasionally performed these auditing functions in relation to security agencies. In a report issued in March 2004, the Auditor General examined Canadian antiterrorism spending since 9/11 through 2003.[976] That study noted a lack of coordination and information-sharing on public security issues between government departments as they then existed, with various security-related agencies reporting to an array of different ministers.

2.5 Commissions of Inquiry

Occasionally, the government may also create ad hoc independent commissions to probe particular public policy issues or scandalous events, employing its powers to do so under the Inquiries Act.[977] Recent examples in the national security area include the 2004 O'Connor inquiry[978] (Arar inquiry), the 2006 Major inquiry[979] (Air India inquiry), and the 2006 Iacobucci internal inquiry.[980]

[969] Ibid., Section 29.
[970] Ibid., Section 37.
[971] Ibid., Sections 37, 38 & 39.
[972] Auditor General Act, RSC 1985, c A-17, Section 5.
[973] Ibid., Section 6.
[974] Parliament of Canada, House of Commons, *Standing Orders of the House of Commons…*, Order 108.
[975] Ibid., Section 13.
[976] Office of the Auditor General of Canada, 'Chapter 3: National Security in Canada…, March 2004.
[977] Inquiries Act, RSC 1985 c I-11.
[978] Parliament of Canada, Order-in-Council, P.C. 2004-0048 (2004-02-05).

In recent practice, these Commissions have been an important means of holding security agencies to account. Commissions generally have extensive powers to compel the attendance of witnesses and the production of information. Even so, government national security confidentiality claims were endemic in the Arar, Iacobucci and Major inquiries. Indeed, in the Arar inquiry, the Commission itself was forced to seek a court order permitting it to issue certain paragraphs in its final report that the government considered prejudicial to national security.

Moreover, the executive establishes these inquiries and their terms of reference—Parliament has no role under the Inquiries Act. As such, inquiries are relatively uncommon and mandates are confined to matters that the executive views as desirable. Inquiries are not, in other words, open-ended judicial investigations triggered via actors other than the executive.

3. CONCLUSION

The Canadian system of accountability compares reasonably well to the standards expressed by the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[981] There are, however, obvious shortcomings:

- **Mandate and powers of review institutions**: SIRC is an appropriate model that, on paper, has substantial powers to review CSIS activities. It is, however, a very small operation, one whose growth has not kept pace with the expansion of CSIS and which, by its own account, must be selective in its review functions. In these circumstances, questions should be asked about how effective it is able to be (compared to what might be the case if it were more amply resourced), and the extent to which it can independently identify shortcomings in CSIS practices. The RCMP has no review body close in function or form to SIRC, and the model proposed by the government in a recent bill tabled in Parliament revamps the RCMP public complaints commission, but without according that body SIRC-like powers to see secret information.
- **Complaints and effective remedy**: SIRC is only competent to make recommendations, and has no binding powers. The RCMP public complaints commission has no binding powers, or capacity to see secret information.

The key lesson of design to be taken from the Canadian experience is this: First, empower a single body with competence to review and make binding orders (including with respect to compensation) and charge that body with functions in relation to all security and intelligence bodies, rather than establishing separate bodies with different powers for different agencies. The latter approach—the one pursued by Canada—leaves too much to 'fall between the cracks' and go without remedy. Second, government must resource that body appropriately so that it can properly perform its mandate.

[979] Parliament of Canada, Order-in-Council, P.C. 2006-0293 (2006-05-01).
[980] Parliament of Canada, Order-in-Council, P.C. 2006-1526 (2006-12-11).
[981] UN Special Rapporteur 2010.

REFERENCES

Access to Information Act, RSC 1985, c A-1, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-a-1/latest/rsc-1985-c-a-1.html).

Auditor General Act, RSC 1985, c A-17, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-a-17/latest/rsc-1985-c-a-17.html).

Bland D. & R. Rempel (2005), 'A Vigilant Parliament: Building Competence for Effective Parliamentary Oversight of National Defence and the Canadian Armed Forces', *Institute for Research on Public Policy*, Vol. 5.

Canada Border Services Agency Act, SC 2005, c 38, available at (http://www.canlii.org/en/ca/laws/stat/sc-2005-c-38/latest/sc-2005-c-38.html).

Canada Evidence Act, RSC 1985, c C-5, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-5/latest/rsc-1985-c-c-5.html).

Canadian Air Transport Security Authority Act, SC 2002, c 9, available at (http://www.canlii.org/en/ca/laws/stat/sc-2002-c-9-s-2/latest/sc-2002-c-9-s-2.html).

Canadian Security Intelligence Service (July 2006), *Backgrounder No. 13: The Integrated Threat Assessment Centre (ITAC)*.

Canadian Security Intelligence Service Act, RSC 1985, c C-23, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-23/latest/rsc-1985-c-c-23.html).

Heafey, S. (3 October 2005), *Civilian Review of the RCMP's National Security Activities*, CACOLE Conference 2005, Montreal, Quebec.

Immigration and Refugee Protection Act (IRPA), SC 2011, c 27, available at (http://www.canlii.org/en/ca/laws/stat/sc-2001-c-27/latest/sc-2001-c-27.html).

Inquiries Act, RSC 1985 c I-11, available at (http://www.canlii.org/en/ca/_laws/stat/rsc-1985-c-i-11/latest/rsc-1985-c-i-11.html).

Lee D. (1999), *The Power of Parliamentary Houses to Send for Persons, Papers and Records*, University of Toronto Press, Toronto.

Maingot J. (1997), *Parliamentary Privilege in Canada,* McGill-Queen's Press, Montreal.

National Defence Act (NDA), RSC 1985, c N-5, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-n-5/latest/rsc-1985-c-n-5.html).

O'Connor Dennis R. and the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (2006), *A New Review Mechanism for the RCMP's National Security Activities*, Publishing and Depository Services, Ottawa, available at (http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf).

Office of the Auditor General of Canada (March 2004), 'Chapter 3: National Security in Canada—The 2001 Anti-Terrorism Initiative' in *Report of the Auditor General of Canada to*

the House of Commons, available at (http://www.oag-bvg. gc.ca/internet/docs/20040303ce.pdf).

Parliament of Canada, Order-in-Council (2004-02-05), P.C. 2004-0048.

Parliament of Canada, Order-in-Council (2006-05-01), P.C. 2006-0293.

Parliament of Canada, Order-in-Council (2006-12-11), P.C. 2006-1526.

Parliament of Canada, House of Commons, Standing Committee on Public Safety and National Security (18 March 2010), *Minutes of Proceedings*, available at (http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4360754&Language=E&Mode=1&Parl=40&Ses=3).

Parliament of Canada, House of Commons (May 2011), *Standing Orders of the House of Commons: Including the Conflict of Interest Code for Members*, available at (http://www.parl. gc.ca/About/House/StandingOrders/toc-f.htm).

Parliament of Canada Act, RSC 1985 c P-1, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-p-1/latest/rsc-1985-c-p-1.html).

Privacy Act, RSC 1985, c P-21, available at (http://www.canlii.org/en/ca/ laws/stat/rsc-1985-c-p-21/latest/rsc-1985-c-p-21.html).

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c 17, available at (http://www.canlii.org/en/ca/laws/stat/sc-2000-c-17/latest/sc-2000-c-17.html).

R v. Campbell (1999), 1 SCR 565 (Supreme Court of Canada).

Royal Canadian Mounted Police, *Protective Policing*, available at (http://www.rcmp-grc.gc.ca/pp/protect-policing-police-eng.pdf).

Royal Canadian Mounted Police, *Organizational Structure,* available at (http://www. rcmp-grc.gc.ca/about-ausujet/organi-eng.htm).

Royal Canadian Mounted Police Act, RSC 1985, c R-10, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-r-10/latest/rsc-1985-c-r-10.html).

Security Intelligence Review Committee (2010), *Annual Report 2009/2010*, available at (http://www.sirc-csars.gc.ca/pdfs/ar_2009-2010-eng.pdf).

Security Intelligence Review Committee (2004), *Annual Report* 2003–2004, available at (http://www.sirc-csars.gc.ca/anrran/2003-2004/pgi-eng.html).

Security Intelligence Review Committee (2010), 'Frequently Asked Questions', available at (http://www.sirc-csars.gc.ca/faqfqs/index-eng.html).

Security Intelligence Review Committee (2010), 'Complaints,' available at (http://www.sirc-csars.gc.ca/cmpplt/index-eng.html).

Security Intelligence Review Committee (2010), 'List of SIRC Reviews', available at (http://www.sirc-csars.gc.ca/opbapb/lsrlse-eng.html).

Security Intelligence Review Committee (June 2006), *Review of CSIS's collaboration and exchanges of intelligence post-9/11* (TOP SECRET).

Security Intelligence Review Committee (June 2005), *Review of Foreign Arrangements with Countries Suspected of Human Rights Violations* (TOP SECRET).

Security Intelligence Review Committee (March 2005), *Review of the Integrated Threat Assessment Centre* (TOP SECRET).

Security Intelligence Review Committee (August 2004), *Review of CSIS's Exchanges of Information with Close Allies* (TOP SECRET).

Security Intelligence Review Committee (January 2000), *Domestic Exchanges of Information 1999–2000* (TOP SECRET).

Security Intelligence Review Committee (1985), *Rules of Procedure of the Security Intelligence Review Committee in Relation to its Function under Paragraph 38(C) of the Canadian Security Intelligence Service Act*, Section 48, available at (http://www.sirc-csars.gc.ca/cmpplt/rulreg-eng.html).

Security of Information Act, RSC 1985, c O-5, available at (http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-o-5/latest/rsc-1985-c-o-5.html).

Special Senate Committee on the Anti-terrorism Act (February 2007), *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, available at (http://www.parl.gc.ca/Content/SEN/Committee/391/anti/rep/rep02feb07-e.pdf).

Thomson v. Canada (Deputy Minister of Agriculture) (1992), 1 SCR 385 (Supreme Court of Canada).

UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Combating Terrorism (2010), *Compilation of good practice on legal and institutional and measures that ensure respect for human rights by intelligence agencies,* UN General Assembly, A/HRC/14/46.

ANNEX A: COUNTRY CASE STUDIES

XII. PARLIAMENTARY AND SPECIALISED OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE UNITED STATES

KATE MARTIN[982]

1. SCOPE OF STUDY

This chapter outlines the ways in which legislative oversight is exercised over those federal agencies that engage in domestic intelligence activities in the United States.

1.1 Federal departments and agencies covered

United States government entities engaged in domestic intelligence activities as defined in the Terms of Reference (ToR) include the following:

- The Federal Bureau of Investigation (FBI), which has the lead on these activities and which also conducts law enforcement activities;
- The Department of Justice, of which the FBI is formally a component;
- The National Counter Terrorism Center, part of the Office of the Director of National Intelligence;
- The Department of Homeland Security (DHS); and
- Both the Central Intelligence Agency (CIA) and the National Security Agency (NSA), while primarily concerned with foreign intelligence, have some authority to gather and analyse domestic intelligence.

Per the ToR, this paper will not examine oversight of strictly law enforcement activities. Instead, it will highlight general approaches to oversight and provide some specific examples; a comprehensive listing of oversight activities would be much longer.

1.2 Domestic intelligence activities covered

We understand that this study is intended to inform the European Parliament's approach to establishing oversight of EU security agencies, which do not have the power to intercept communications, question individuals or search private property. Their domestic intelligence activities reportedly consist of sharing information and personal data, joint analysis and dissemination of information, as well as the collection of open source information.

There is no exact analogue for this division of powers among US government agencies. The major domestic intelligence agencies have the authorities listed above, as well as the authority to collect personal data and arrest individuals. The FBI, for example, is the lead federal law enforcement agency and also the lead domestic intelligence agency. The CIA is the exception because it has no arrest powers and its domestic intelligence activities are

[982] Director, Center for National Security Studies, Washington DC, USA; kmartin@cnss.org.

more limited, although it does have the authority to collect information on individuals in the US, both citizens and others.

This difference in agency powers affects how oversight is conducted in the United States because many civil liberties concerns about domestic intelligence activities involve either arrests or the collection of information by intelligence agencies about individuals or organisations. In many instances, the legal restraints on domestic intelligence activities are stronger at the initial collection stage than the subsequent use or dissemination stages. Thus, issues relating to the sharing and analysis of information have more often been the province of technical discussions and reviews focused on implementation rather than broader policy discussions concerning what rules should apply.

2. THE GENERAL MANDATE AND FUNCTIONS OF OVERSIGHT COMMITTEES

Oversight is conducted by individual committees in each house of Congress. Some agencies are subject to oversight by more than one committee in the same legislative chamber.

The congressional committees, which are mainly responsible for conducting oversight of domestic intelligence activities in addition to the relevant subcommittees of the Appropriations Committees, include the Judiciary Committees, the Homeland Security Committees and the Select Intelligence Committees in each house.[983]

As a general matter, Congress has the authority to conduct oversight of all activities by domestic intelligence agencies. There are some unresolved, mostly theoretical disagreements between the Executive Branch and Congress on the scope of Congress' authority, but those disagreements are mostly about oversight of intelligence, diplomacy and military activities abroad. In practice, what activities are reviewed and how extensively they are reviewed varies widely. Many different factors influence the focus, extent and usefulness of congressional oversight at any particular time.

2.1 Authorising authority

Congress' real oversight power derives from its authority to create agencies and authorise their activities. The Congress as a whole votes to authorise the activities of the intelligence agencies and to fund existing agencies. It has the sole authority to create, abolish and reorganise the intelligence agencies and to assign or reassign functions to specific agencies.984 A basic constitutional principle in the United States is that, with one exception not relevant here, US government agencies must find positive authority in legislative enactments for each and every activity, which authority can be found in very specific or very general language.

[983] The rules of the respective committees are online (except for the Senate Homeland Security and Governmental Affairs Committee): House Judiciary at (http://judiciary.house.gov/hearings/printers/112th/Rules_of_Procedure_112.pdf); House Homeland Security at (http://homeland.house.gov/legislation/committee-rules); House Intelligence at (http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/112th%20Committee%20Rules%20Chairman's%20Mark.pdf); Senate Judiciary at (http://judiciary.senate.gov/about/committee-rules.cfm); and Senate Intelligence at (http://intelligence.senate.gov/pdfs/11120.pdf).

[984] US Constitution, Article I, Section 8; cited in Martin 2004, pp. 146–171.

2.2 Spending authority

All monies spent for domestic intelligence activities must be appropriated by Congress. Congress enacts yearly funding measures, in which it can define the exact purposes for which money may be spent and may prohibit expenditures for other purposes.[985]

2.3 Specific oversight / investigative authority

Congress, usually through its committees, also has the power to oversee and to investigate specific domestic intelligence programs or activities. It has authority to conduct oversight of agencies' administration and management issues, operations and finances.

3. CRITICAL EXAMINATION OF OVERSIGHT ACTIVITIES

3.1 Some general comments

Legislative oversight of domestic intelligence activities must be understood as a species of congressional oversight more generally. Congressional oversight has evolved into a highly complex set of rules and practices, focused on an enormous number of activities by an extremely large Executive Branch workforce, which itself is organised in a highly complex way.

Domestic intelligence activities frequently involve certain features, which while not unique to domestic intelligence activities, pose additional challenges to oversight. They frequently involve classified information and joint or inter-agency activities; such activities also frequently include interaction with state and local law enforcement authorities, and they involve issues related to the protection of privacy and civil liberties.

On the one hand, an enormous amount of information and analysis is generated by oversight practices, which is available both to the legislature and in many cases to the public. On the other hand, the breadth and complexity of both oversight mechanisms and domestic intelligence activities make it a challenge both to 'see the big picture' and to determine what aspects are most in need of oversight and legislative attention. The most basic oversight challenge is the need for adequate resources, but even plentiful oversight resources do not resolve how to balance the competing demands on the legislature's time and attention. Increased partisanship in the past few years has also complicated the task of oversight.

Since the 9/11 attacks, there has been extensive attention to and oversight of the sharing of information, including personal data, among intelligence agencies, between federal agencies and state and local law enforcement and with international partners. Oversight of these activities is carried out in the same ways as oversight of any domestic intelligence activity. Oversight has been successful in producing important reports and analyses of the issue; it has been less successful in illuminating potential problems or solutions.

[985] US Constitution, Article I, Section 9; cited in Martin 2004.

3.2 Purposes/functions of oversight of domestic intelligence activities

Scholars have outlined the functions of congressional oversight as the following:[986]

- Improve the efficiency and effectiveness of government operations;
- Evaluate programs and performance;
- Detect and prevent waste, abuse, or illegal conduct;
- Protect civil liberties;
- Gather information to develop legislative proposals;
- Ensure administrative compliance with legislative intent; and
- Prevent executive encroachment on legislative authority and prerogatives.

Congressional oversight also plays an important role in keeping the public informed. Most fundamentally, the purpose of legislative oversight is to determine the mission, organisation, authorities, resources of and limitations on domestic intelligence activities.

4. CONGRESSIONAL METHODS OF OVERSIGHT

Members of Congress and their staff obtain and analyse information about domestic intelligence activities in many different ways. They include the following:

4.1 Committee and Subcommittee Hearings

There are frequent hearings where Members ask questions of agency personnel or outsiders. Such hearings scrutinise the annual budget request for the agency; conduct general oversight of the agency; consider proposed legislation; or examine any specific subject that the Committee or Subcommittee Chair determines is deserving of a hearing. If agency personnel are testifying, the Committee requests either a specific official or the official most knowledgeable about the subject and they may be required to testify under oath. Committee staff members usually prepare background materials for the Members and draft possible questions. Members of the public may also suggest possible questions for consideration by the Member, usually by private correspondence without public notice.

Such hearings are open to the public and can be watched live on the web. A public transcript is also prepared. However, if classified information is discussed the entire hearing or a portion will be closed to the public. After the formal hearing is finished, Members are usually allowed additional time to submit written questions to the witnesses. However, agency witnesses may delay their answers or never respond at all. Such questions and answers are also publicly available unless marked classified, although members of the public may have to know to ask a legislative staff member.

Public hearings signal to agencies that the subject is one of importance to the Committee. They can be very useful in requiring agency officials to answer questions and to do so on the public record. They also work well to focus public and media attention on a problem. In recent years, however, they have not proved very useful in providing an in-depth examination of complex issues. All too often, Members use the time to make statements, rather than pursue real inquiries and obtain information.

[986] Mullen 2006 and Kaiser 1997.

4.2 Informal communications with agency officials

There may also be informal communications between Members or their staff and agency officials. Agency personnel also conduct informal non-public briefings on specific subjects, usually for Committee staff, but sometimes for Members. Usually, there are no public records, or sometimes records at all, of such communications.

Members may also write letters requesting information at any time. Such letters are apt to receive a much quicker response if they are from the Chair or Ranking Member of a Committee with jurisdiction over agency activities. Letters from an agency are generally publicly available unless they contain classified information.

Such communications are an important means for staff to understand how the agencies actually work. They are not useful in educating the public. They may also contribute to confusion about the role of the legislative committees and a view that they function as proxies for the intelligence agencies with the rest of Congress and the public, rather than overseers.

4.3 Reports done by congressional support agencies

Congress has established three semi-independent organisations to provide objective non-partisan analysis and information to Members. The reports issued by these entities are an invaluable resource for congressional staff and the public seeking to understand the specifics of complicated issues or track various controversies. They include:

i. The Congressional Budget Office (CBO), which provides monetary estimates of government programs.[987] The CBO is the least important for oversight of domestic intelligence activities.

ii. The Congressional Research Service (CRS).[988] CRS reports are not classified but are publicly available only as a result of NGO efforts.[989] They are an invaluable resource for understanding the legal frameworks and issues regarding information sharing.

iii. The Government Accountability Office (GAO) is the most important support agency in terms of providing information, analysis and reports on domestic intelligence activities, including sharing of personal data.

4.4 GAO oversight

The Government Accountability Office is the largest of the three agencies that provide staff support, research, review and analysis for Congress. It is deemed a congressional rather than executive branch entity, although the Director is appointed by the President, with the advice and consent of the Senate, for a 15-year non-renewable term.[990] It has been reported that as of March 2008, 'there were 1,000 GAO employees with Top Secret security

[987] Congressional Budget Office website, 'CBO's Role and Work'.
[988] Congressional Research Service website, 'About the CRS'. See also: CRS (2011), 'Congressional Oversight Manual', Report RL30240.
[989] Aftergood 2011.
[990] CRS (2008), 'GAO: Government Accountability Office and Government Accounting Office', Report RL30349.

clearances out of 3,153 total staff. Of those, 73 held even higher clearances for access to intelligence information'.[991]

In its own words, GAO's mission is to 'provide Congress with timely information that is objective, fact-based, nonpartisan, non-ideological, fair and balanced'. It performs audits, investigates allegations of illegality, reports on how well government programs are meeting their objectives, and writes policy analyses and options for congressional consideration.[992]

The GAO has produced an extensive library of reports on sharing intelligence information and personal data among federal agencies and between the federal, state and private sectors.[993] Its reports are essential reading for doing effective oversight. They provide a roadmap of activities as well as an analysis of how to measure successful implementation of legislative requirements. The one weakness in GAO oversight activities has been the resistance of the CIA to allow GAO staffers to review its most sensitive information.[994]

4.5 Legislatively required reports by agencies to Congress

4.5.1

Congress sometimes creates offices within agencies with responsibility to make direct reports to Congress of that office's observations and recommendations. For example, Congress created a Chief Privacy Officer and an Office for Civil Rights and Civil Liberties within the Department of Homeland Security. Congress requires the DHS Privacy Office to report quarterly regarding the advice it has provided concerning Department actions and the Department's response, and on the complaints received by the DHS and their nature.[995]

However, an extensive body of law has been generated on how much independence such an officer can have in relaying reports to Congress without reflecting the views of the Cabinet Secretary in charge of the agency. The Executive Branch takes the position that such personnel are ultimately subordinate to the President and the Congress may not intrude on the President's constitutional authority by requiring reports that are not reviewed in advance by higher level agency officials and at a minimum acknowledge and include their views.[996] Nevertheless, in practice, this process can still work to provide a somewhat independent view to the Congress. Whether it does so will depend on a variety of factors, such as the character of the individual serving as Privacy Officer, the politics of the particular controversy, and the potential political and public fall-out if it were to become known that the agency was attempting, in essence, to censor a report by the Privacy Officer.

4.5.2

Congress by law may also require other kinds of reporting by agencies to aid in oversight. Congress may require one-time reports on a particular matter either by the intelligence agency itself or sometimes by the Inspector General of the agency (Inspectors General

[991] Aftergood 2008a.
[992] Government Accountability Office website, 'About the GAO'.
[993] Government Accountability Office website, 'GAO Careers: Homeland Security and Justice' and 'Topic Collection: Homeland Security Products'.
[994] Aftergood 2008a.
[995] United States (2007), Public Law 110-53; see for example: Department of Homeland Security (2010), 'Privacy Office Second Quarter Fiscal Year 2010 Report to Congress'.
[996] Department of Justice Office Legal Counsel memo (2008), 'Constitutionality of Direct Reporting Requirement in Section 802(e)(1) of the Implementing Recommendations of the 9/11 Commission Act of 2007'.

provide internal Executive Branch oversight, but have some degree of independence).[997]

The Congress may also require periodic ongoing reports by agencies. It has done so, for example, with regard to data-mining programs used by agencies to analyse personal information on Americans. Such reports can be invaluable information compilations, which would otherwise be unavailable. But there are many complaints that Congress requires too many reports, which results in some reports not being completed on time, if completed at all.[998]

Agencies also publish reports not specifically required by Congress, which may be useful for oversight. For example, DHS reports include many relating to the sharing of personal data, including ones on data-mining and passenger records.[999] There are several excellent government websites that contain expansive libraries of such reports and other materials, including the Homeland Security Digital Library and a library of Issues, Resources, and Training for Fusion Centers.[1000]

4.6 Reports by independent commissions

From time-to-time, Congress may establish an independent commission to prepare an in-depth report. This usually happens only on matters of great importance, such as the 9/11 attacks. Congress can choose the method of appointment of the commissioners, provide funding for staff and other resources, and direct the objects of study.

Congress created two prominent commissions in the wake of the 9/11 attacks, whose recommendations were then seriously debated by the Congress. Their recommendations enacted into law included new mechanisms for sharing intelligence information, both domestic and foreign, which are called the Information Sharing Environment.[1001] On the other hand, Congress frequently establishes study commissions, whose recommendations are simply ignored. Sometimes, it is understood from the beginning that establishment of a commission is simply a way for Congress to defer a problem with the hope that it will disappear.

4.7 Congressional staff investigations

In addition to regularly held hearings, congressional committees may also undertake extensive investigations of particular matters. These investigations may be triggered by anything from confidential disclosures of government employees or former employees to rumours and reports in the news media. Public controversy is most likely to result in investigations.

Whether such investigations are conducted is up to the Chair(s) of the relevant Committee(s). However, Chairs may be dependent upon the leadership of the respective chamber to provide sufficient resources, depending on the extent of the investigation. On rare occasions, more than one Committee may decide to undertake a joint investigation or

[997] See for example: Office of the Inspectors General (2009), 'Report on the President's Surveillance Program'.
[998] See, for example, the GAO report on the failure of the DHS to fully address reporting requirements: Government Accountability Office (2010), 'Quadrennial Homeland Security Review: 2010 Reports Addressed Many Required Elements, but Budget Planning Not Yet Completed'.
[999] Available at: Department of Homeland Security website (http://www.dhs.gov/files/publications/editorial_0514.shtm).
[1000] See reference list for more complete information.
[1001] United States (2004), Public Law 108-458.

both houses of Congress may conduct a joint investigation. After the 9/11 attacks, but before the establishment of the independent commission mentioned above, both houses of Congress undertook a 'Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001'. The report of that investigation is publicly available and provides a wealth of detail about the rules and actual practices of the intelligence agencies.

Such investigations usually result in publication of a comprehensive and detailed report, which may contain recommendations for administrative or legislative reforms. Sometimes, such reports also result in referrals to the Department of Justice for further civil or criminal investigation. If, however, the report is kept classified, it will be difficult to know what actions if any are taken in response to the report.

If staff resources are available, such reports may be as in-depth and extensive as those undertaken by the GAO. A key difference is that the direction and conclusions of staff reports are ultimately within the control of the Members of the Committee. This sometimes results in reports signed only by the majority with the minority writing a dissenting report.

4.8 Congressional confirmation/impeachment of senior officials

Under the Constitution, the President nominates agency heads, which must be approved by the Senate.[1002] The relevant Senate committee usually holds a public hearing on a nomination. If the committee votes favourably on the nomination, it is then sent to the entire Senate for a vote. These confirmation hearings serve an important role in determining a nominee's vision for the agency; sometimes they are also used to obtain a commitment from a nominee to respect the congressional oversight process itself. Withholding a vote on the President's nominee is also sometimes used as leverage by Senators to obtain information from the Executive Branch. The rules of the Senate permit this leverage to be exercised by one Senator and there is widespread criticism of the practice.

Most agency heads serve at the pleasure of the President. However, the Constitution also gives the Congress the power of impeachment, a process by which Congress can remove from office Executive Branch officials. This power is rarely used. In some cases, most notably, the FBI Director, Congress has provided for a set term of years and that an individual may not serve more than one term.[1003] While the President may still fire the FBI Director, the law is intended to minimise the political nature of the office.

4.9 Establishing oversight structures within agencies or organising bureaucracies to increase oversight

Congress frequently uses its law-making authority to provide for greater oversight, especially regarding domestic intelligence activities. Thus, the laws regulating collection, use and sharing of domestic intelligence are frequently evaluated in terms of their potential to assure oversight, for example by requiring judicial or high-level official approval for certain activities.

[1002] US Constitution, Article II, Section 2.
[1003] CRS (2005), 'Nomination and Confirmation of the FBI Director: Process and Recent History,' Report RS20963.

4.10 Statutory regulation of domestic intelligence activities

Finally, drawing a clear line between legislative oversight and legislative law-making may be overly formalistic. Since the 9/11 attacks, the US Congress has devoted much time and attention to issues relating to the sharing of intelligence information among agencies, starting with provisions of the 'Patriot Act'.[1004]

The current rules concerning use and sharing of domestic intelligence sharing are almost as complex as the existing mechanisms for exercising oversight over compliance with those rules. Other 'fixes' have been much simpler; for example, setting up offices where FBI and CIA personnel work side-by-side to overcome the agencies' historical reluctance to share information.

4.11 Summary

There is no lack of information available to congressional overseers. However, the success of oversight efforts depends upon the capability and willingness of the overseers first to review and synthesise what is likely to be lengthy, detailed and sometimes technical reporting. Effective oversight also requires a detailed understanding of the complexity of the applicable legal regimes and bureaucratic organisations. All this requires well-informed professional staff with the necessary background and expertise, and time and resources. Finally, it requires Members of Congress with an interest in and commitment to conducting real oversight and following through on conclusions or recommendations.

This process is also likely to be complicated by public opinion and media reporting, which can serve either as an incentive for effective oversight or make such oversight more difficult by making it a subject of partisan attacks.

5. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

The only formal oversight entity, which is not part of Congress, is the Privacy and Civil Liberties Oversight Board. Its creation was recommended by the 9/11 Commission's Report. In August 2007, Congress created the Board as an independent agency within the Executive Branch. The Board is intended to serve as an advisory body to assist in ensuring that privacy and civil liberties concerns are appropriately considered in counterterrorism laws and policies, specifically including information sharing. The Board consists of five Members appointed by the President and confirmed by the Senate, including a full-time Chair and a small staff. The Board has subpoena power and must provide periodic reports. As of this writing, Members of the new Board have not yet been appointed and it has not yet started to function. When it does, it is likely that it will focus on government surveillance of Americans, including the collection, use and sharing of personal data.

6. COMPOSITION OF OVERSIGHT COMMITTEES

The membership and jurisdiction of the Committees in each House of Congress are determined by the Rules of that House, which are adopted by the Members at the beginning of each two-year congressional term. A member of the majority party in that

[1004] De Rosa, Dinh and Martin 2005.

house always serves as the Chair of each Committee and the majority party always has more members on any Committee than does the minority. Decisions are made by majority vote after more or less formal or informal discussion.

As 'Select' Committees, Members and leaders on the Intelligence Committees are handpicked by the Congressional leadership, rather than by a vote of their colleagues, as is the case for other Committees. Both Intelligence Committees have term limits for their Members, designed to ensure a steady rotation of membership.

For the House Intelligence Committee, the majority political party gets a substantial majority on the Committee as well. In the Senate Intelligence Committee, by contrast, the majority party gets only a one-vote advantage. The membership structure of both Intelligence Committees allows for the inclusion of Members (at least one from each political party) who also serve on each of several other committees that have an interest in intelligence matters: the Appropriations Committees, the Armed Services Committees, the Judiciary Committees, and the Committees on Foreign Relations (in the Senate) and Foreign Affairs (in the House of Representatives). This can be especially useful when particular matters come within the jurisdiction of more than one committee, although it can also result in those Members who sit on both committees wielding greater influence than their colleagues.

In the Senate, one mechanism to foster bipartisanship has been to have the minority party's leading member on the committee serve as the vice chair and, in the chair's absence, as acting chair. This set-up deters both parties from partisan politicking since, on any given day, the absence of the chair could result in the minority party's exercising of the chair powers. This arrangement can result in a close working relationship between the chair and the vice chair, especially when the two handle extremely sensitive matters, which are sometimes not shared with the full committee. The House of Representatives Intelligence Committee, on the other hand, has no such formal procedure for shared leadership.

7. INVESTIGATIVE POWERS AND ACCESS TO INFORMATION

There has been a continual tug of war between Congress and the Executive Branch over Congress' access to information held by the Executive, especially information which is classified and relates to intelligence activities.[1005] Note that not all information concerning domestic intelligence activities discussed herein is classified. By and large, disagreements are resolved through negotiation and Congress usually obtains the information that it requests. It is less clear how fully the Executive Branch complies with legislated requirements to keep the Congress currently and fully informed of all intelligence activities when it is not asked specific questions.[1006]

As a matter of both principle and law, the more prevalent view held by the Congress is that there is no permissible limitation on its access to intelligence information—including that which reveals sources and methods. The constitutional argument is that Congress needs classified national security information in order to carry out its constitutional responsibilities

[1005] There is a long and rich history concerning congressional efforts to obtain information, which is discussed in the works cited in the reference list.
[1006] The Intelligence Oversight Act requires the Executive to keep the intelligence committees 'fully and currently informed of the intelligence activities of the United States…'. The scope of intelligence activities covered by this requirement is both broader and more narrow than the activities addressed in this paper.

and that the Constitution vests shared responsibilities in the Congress and the President for making decisions about national security and foreign policy matters. This view is reflected in the House and Senate Rules governing the Intelligence Committees that have set up a procedure whereby, after giving the President an opportunity to register his disagreement and state his views, the House or the Senate as a whole may vote to declassify and publicly release classified information.

At times, the Executive Branch has resisted providing highly classified information to staff on the Judiciary Committees and sought to limit its distribution to staff from the Intelligence or sometimes the Armed Services Committees. In recent years, this issue has been addressed when some Judiciary Committee staff have been given the highest level clearances and then allowed access to such information.

The Executive Branch may also resist turning over information to the Congress that pertains to individual Americans either on the basis of their privacy rights or because the information is part of an ongoing law enforcement investigation or prosecution and as such should not shared outside the Executive branch.

It is unlikely that there will be a definitive resolution to the ongoing disagreement between the Congress and the President—as well as among constitutional scholars—as to whether Congress is in fact entitled to all information or whether the President has the right to withhold more than a small amount of information concerning his personal deliberations with his personal advisors.

In addition to the leverage that Congress may exercise through appropriations, confirmations, etc., it may also subpoena officers of the Executive Branch. That power is rarely although sometimes used and its scope is also the subject of disagreement. The GAO also has the authority to file suit to compel an agency to turn over records.

Finally, congressional oversight efforts frequently use public or media reports not only as a basis for asking questions, but sometimes also as evidence of particular practices. They may also rely upon expert studies by academics or other institutions outside of government.[1007]

8. PROTECTION OF INFORMATION

Protections for classified information by the legislative body mirror in many respects the protections and procedures applicable to the Executive Branch. Members of the House and Senate, like the President, are deemed to have the necessary clearance for access to classified information by virtue of their election. They are not subject to background checks.

After a Member of the House allegedly disclosed classified information in a public speech on the floor of the House, the House adopted a rule requiring its Members to sign an oath not to disclose classified information. Nevertheless, there are deliberate and inadvertent disclosures by Members from time-to-time, which are treated either as a matter for discipline by the legislative chamber itself or ignored (these individual disclosures are outside the procedures for legislative disclosures discussed in the previous section). The usual penalty for disclosure of classified information is being removed from the Intelligence Committee. Members are immune from prosecution for any statements, including

[1007] e.g., Richelson 2007.

disclosures of classified information, made on the floor of the Congress, but not for other types of statements.

Congressional staff who are selected by Members to serve in positions requiring access to classified information are required to undergo background checks in order to be granted a security clearance. They are also obliged to sign non-disclosure agreements. Violation of such agreements may result in loss of clearance, loss of job and in some instances criminal prosecution.

The Intelligence and Armed Services Committees operate both publicly and in secret. The Intelligence Committees have extensive physical security facilities, including secure meeting rooms. The Judiciary Committees rarely hold *in camera* non-public hearings. Witnesses from the intelligence agencies sometimes testify in open public hearing and sometimes in closed sessions. Non-government witnesses usually testify in public. Sometimes the written record of a closed hearing is later declassified and made public.

9. REPORTING BY OVERSIGHT BODIES

As outlined above, congressional committees and the other oversight bodies regularly publish reports on their inquiries and investigations. The Intelligence Committees regularly publish a report outlining their activities for the past year or two.[1008]

Such reports are frequently based on examination of classified information. When the report itself contains mostly classified information, it will not be released. More often, the initial version of a report may contain both classified and unclassified information. The committee or other oversight body will then engage in a process of negotiation and discussion with the Executive Branch to allow release of the report, through declassification, substitution of unclassified material for classified material, or sometimes issuance of a public report with a classified annex.

10. CONCLUSION

Committee and GAO investigations, agency reporting requirements, and committee hearings are all effective oversight mechanisms. Public reporting, when possible, is very helpful. Legislative power to compel oversight when necessary, for example, through funding authority, is also key. Effective oversight ultimately depends on a shared understanding with the Executive that the legislature is entitled to classified information and that oversight is a good thing for the agencies. Devotion of adequate resources, in particular professional and experienced staff, who become experts on intelligence matters (while not becoming too identified with the agencies), is critical.

[1008] Senate Select Committee on Intelligence (2011), 'Report of the Senate Select Committee on Intelligence, 2009–2011'.

REFERENCES

Aftergood Steven (2 March 2011), 'Public Access to CRS Reports Urged', *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, available at (http://www.fas.org/blog/secrecy/2011/03/crs_access.html).

Aftergood Steven (21 October 2010), 'GAO Role in Intel Oversight to be Determined', *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, available at (http://www.fas.org/blog/secrecy/2010/10/gao_role_tbd. html).

Aftergood Steven (4 August 2008a), 'GAO and Intelligence Oversight', *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, available at (http://www.fas.org/blog/secrecy/2008/08/gao_and_intel.html).

Aftergood Steven (3 March 2008), 'GAO Oversight Office at NSA Lies Dormant', *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, available at (http://www.fas.org/blog/secrecy/2008/03/gao_oversight_office_at_nsa_li.html).

Armed Services Committee, US Senate (20 November 2008), 'Inquiry into the Treatment of Detainees in US Custody', available at (http://armed-services.senate.gov/Publications/Detainee%20Report%20Final_April%2022%202009.pdf).

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (31 March 2005), 'Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction', available at (http://www.gpoaccess.gov/wmd/index.html).

Congressional Budget Office website, 'Congressional Budget Office's (CBO's) Role and Work', available at (http://www.cbo.gov/aboutcbo/budgetprocess.cfm).

Congressional Report (December 2002), 'Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001', US Government Printing Office, Washington DC, available at (http://www.gpoaccess.gov/serialset/creports/911.html).

Congressional Report (October 1994), 'Legislative Oversight of Intelligence Activities: the U.S. Experience', US Government Printing Office, Washington DC.

Congressional Research Service (CRS) (6 January 2011), 'Congressional Oversight Manual', Report RL30240, available at http://www.fas.org/sgp/crs/ misc/RL30240.pdf.

Congressional Research Service (CRS) (19 March 2010), 'The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress', Report R40602, available at (http://www.fas.org/sgp/crs/homesec/R40602.pdf).

Congressional Research Service (CRS) (27 January 2010), 'Protection of Classified Information by Congress: Practices and Proposals', Report RS20748, available at (http://www.fas.org/sgp/crs/secrecy/RS20748.pdf).

Congressional Research Service (CRS) (17 September 2009), 'Privacy and Civil Liberties Oversight Board: New Independent Agency Status', Report RL34385, available at (http://www.fas.org/sgp/crs/misc/RL34385.pdf).

Congressional Research Service (CRS) (updated 10 September 2008), 'GAO: Government Accountability Office and General Accounting Office', Report RL30349, available at (http://www.fas.org/sgp/crs/misc/RL30349.pdf).

Congressional Research Service (CRS) (updated 17 March 2005), 'Nomination and Confirmation of the FBI Director: Process and Recent History', Report RS20963, available at (http://www.fas.org/sgp/crs/natsec/RS20963.pdf).

Congressional Research Service website, 'About the Congressional Research Service (CRS)', available at (http://www.loc.gov/crsinfo/about/).

Davidson Roger (August 1990), 'The Legislative Reorganization Act of 1946, *Legislative Studies Quarterly*, Vol. XV, No 3.

Department of Homeland Security (December 2010), 'DHS Privacy Office: 2010 Data Mining Report to Congress', available at (http://www.hsdl.org/?view&doc=136066&coll=limited).

Department of Homeland Security (26 March 2010), 'Privacy Office Second Quarter Fiscal Year 2010 Report to Congress', available at (http://www.dhs.gov/xlibrary/assets/privacy/privacy_report_803_qtr_2_2010.pdf).

Department of Homeland Security (December 2009), 'DHS Privacy Office: 2009 Data Mining Report to Congress', available at (http://www.hsdl.org/?view&doc=120307&coll=limited).

Department of Homeland Security (December 2008), '2008 Report to Congress: Data Mining: Technology and Policy', available at (http://www.hsdl.org/?view&doc=105590&coll=limited).

Department of Homeland Security (6 July 2006), 'Data Mining Report: Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties', available at (http://www.hsdl.org/?view&doc=68698&coll=limited).

Department of Homeland Security and Bureau of Justice Assistance in the Department of Justice, 'Issues, Resources, and Training for Fusion Centers and State, Local, and Tribal Justice and Public Safety Agencies', available at (http://www.it.ojp.gov/default.aspx?area=privacy).

Department of Homeland Security Inspector General (October 2010), 'Information Sharing With Fusion Centers Has Improved, but Information System Challenges Remain', available at (http://www.dhs.gov/xoig/assets/mgmtrpts/ OIG_11-04_Oct10.pdf).

Department of Justice Office Legal Counsel memo (29 January 2008), 'Constitutionality of Direct Reporting Requirement in Section 802(e)(1) of the Implementing Recommendations of the 9/11 Commission Act of 2007', available at (http://www.justice.gov/olc/2008/privacy-officer-report.pdf).

De Rosa M., Dinh V. and K. Martin (6 July 2005), 'Section 203: Authority to Share Criminal Investigative Information' in *Patriot Debates*, Stewart A. Baker and John Kavanagh, eds., American Bar Association Standing Committee on Law and National Security, available at (http://apps.americanbar.org/natsecurity/ patriotdebates/section-203).

Fisher Louis (2003), *The Politics of Executive Privilege*, Carolina Academic Press, Durham NC.

Fisher Louis (1997), *Constitutional Conflicts Between Congress and the President, 4th edition, revised*, University Press of Kansas, Lawrence KS.

Fisher Louis (1981), *The Politics of Shared Power: Congress and the Executive*, Congressional Quarterly Press, Washington DC.

Fisher Louis (1972), *President and Congress: Power and Policy*, The Free Press, New York.

Government Accountability Office (16 December 2010), 'Quadrennial Homeland Security Review: 2010 Reports Addressed Many Required Elements, but Budget Planning Not Yet Completed', GAO-11-153R, available at (http://www.gao.gov/ new.items/d11153r.pdf).

Government Accountability Office (29 September 2010), 'Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results', GAO-10-972, available at (http://www.gao.gov/new.items/d10972.pdf).

Government Accountability Office (5 May 2010), 'Terrorist Watchlist Screening: FBI Has Enhanced Its Use of Information from Firearm and Explosives Background Checks to Support Counterterrorism Efforts', GAO-10-703T, available at (http://www.gao.gov/new.items/d10703t.pdf).

Government Accountability Office (17 March 2010), 'Intelligence, Surveillance, and Reconnaissance**:** Overarching Guidance Is Needed to Advance Information Sharing', GAO-10-500T, available at (http://www.gao.gov/new.items/d10500t. pdf).

Government Accountability Office (27 January 2010), 'Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security', GAO-10-401T, available at (http://www.gao.gov/new.items/d10401t.pdf).

Government Accountability Office (18 December 2009), 'Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed', GAO-10-41, available at (http://www.gao.gov/new.items/d1041.pdf).

Government Accountability Office (25 September 2009), 'Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing', GAO-09-904SP, available at (http://www.gao.gov/new.items/d09904sp.pdf).

Government Accountability Office (30 September 2008), 'USA Patriot Act: Better Interagency Coordination and Implementing Guidance for Section 311 Could Improve US

Anti-Money Laundering Efforts', GAO-08-1058, available (http://www.gao.gov/new.items/d081058.pdf).

Government Accountability Office (23 July 2008), 'Information Sharing: Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress', GAO-08-637T, available at (http://www.gao.gov/new.items/d08637t.pdf).

Government Accountability Office (17 April 2006), 'Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information', GAO-06-383, available at (http://www.gao.gov/new.items/d06383.pdf).

Government Accountability Office (17 March 2006), 'Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information', GAO-06-385, available at (http://www.gao.gov/new.items/d06385.pdf).

Government Accountability Office (21 October 2002), 'IRS and Terrorist-Related Information Sharing', GAO-03-50R, available at (http://www.gao.gov/new.items/d0350r.pdf).

Government Accountability Office (15 October 2001), 'Information Sharing: Practices That Can Benefit Critical Infrastructure Protection', GAO-02-24, available at (http://www.gao.gov/new.items/d0224.pdf).

Government Accountability Office website, 'About the Government Accountability Office (GAO)', available at (http://www.gao.gov/about/index.html).

Government Accountability Office website, 'Government Accountability Office (GAO) Careers: Homeland Security and Justice', available at (http://www.gao.gov/careers/hsj.html).

Government Accountability Office website, 'Topic Collection: Homeland Security Products', available at (http://www.gao.gov/docsearch/featured/ homelandsecurity.html).

Harvard Law Policy Review (Winter 2007), 'Congressional Power: A Dialogue', Vol. 1, No 1.

Homeland Security Digital Library collection website, The Naval Postgraduate School Center for Homeland Defense and Security, available at (http://www.hsdl.org/?search=&placeholder=&offset=0&all=report+to+congress&any=&exact=data+mining&without=&begindate=&enddate=&advanced=&searchfield=title&collection=limited&submitted=Search).

Kaiser Frederick (10 October 1997), 'Congressional Oversight', CRS Report 97-936 GOV.
Martin Kate (2004), 'United States of America' in *Transparency and Accountability of Police forces, Security Services and Intelligence Agencies*, Geneva Centre for the Democratic Control of Armed Forces and the Centre for European Security Studies, Sofia.

McDonough Denis, Rudman Mara and Peter Rundlet (June 2006), 'Congressional Oversight of Intelligence is Broken', Center for American Progress, available at (http://www.americanprogress.org/issues/2006/09/no_mere_oversight.pdf).

Mullen Patrick R. (2006), 'Dissertation on Congressional Reporting: A Management Process to Build a Legislative-Centered Public Administration', Dissertation, Virginia Polytechnic Institute and State University, available at (http://scholar.lib.vt.edu/theses/available/etd-04202006-104259/).

National Commission on Terrorist Attacks Upon the United States (2004), 'Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition', Government Printing Office, Washington DC, available at http://www.gpoaccess.gov/911/index.html.

Office of the Director of National Intelligence (15 February 2008), 'Data-mining report required to Congress: Data Mining Report as defined by Congress under Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007', available at (http://www.dni.gov/reports/data_mining_report_feb08. pdf).

Office of the Inspectors General (10 July 2009), 'Report on the President's Surveillance Program', available at (http://www.justice.gov/oig/special/s0907. pdf).

Richelson Jeffrey T. (2007), *The US Intelligence Community*, Westview Press, Boulder CO.

Senate Select Committee on Intelligence (17 March 2011), 'Report of the Senate Select Committee on Intelligence, 2009–2011', available at (http://intelligence.senate.gov/pdfs/1123.pdf).

US Code, Title 28 Section 533, 'Investigative and other officials; appointment'.

US Code, Title 31 Section 712, 'Investigating the use of public money'.

US Code, Title 31 Section 716, 'Availability of information and inspection of records'.

US Code, Title 50 Section 413, 'General Congressional oversight provisions'.

US Constitution, Article I, Sections 8, 9 and Article II, Section 2.

United States, Public Law 108–458 (17 December 2004), *The Intelligence and Terrorism Prevention Act of 2004*.

United States, Public Law 110–53 (3 August 2007), *The Implementing Recommendations of the 9/11 Commission Act of 2007*.

United States House of Representatives, 'House Rules', available at (http://clerk.house.gov/committee_info/commfaq.aspx).

United States Senate, 'Senate Rules', available at (http://www.senate.gov/general/common/generic/committee_faq.htm#committee_assignment).

Walker David M. (February 2008), 'GAO Can Assist the Congress and the Intelligence Community on Management Reform Initiatives', Testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, US Senate,

available at (http://www.fas.org/irp/congress/2008_hr/_022908walker.pdf), quoted in Aftergood 2008a.

White House, 'Privacy and Civil Liberties Oversight Board', Bush Administration website, available at (http://georgewbush-whitehouse.archives.gov/_privacyboard/).

ANNEX B: THEMATIC STUDIES ON OVERSIGHT OF THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE (AFSJ) BODIES[1009]

I. Parliamentary Scrutiny of Justice and Home Affairs Agencies by Bruno De Witte & Jorrit J. Rijpma

II. Europol and Eurojust by Alexandra De Moor & Gert Vermeulen

III. The European Union's Area of Freedom, Security and Justice Architecture after the Lisbon Treaty by Steve Peers

[1009] The opinions expressed in the annexed studies are the responsibility of their respective authors, and do not necessarily reflect the views of the Geneva Centre for the Democratic Control of Armed Forces, or the European University Institute.

ANNEX B: THEMATIC STUDIES

I. PARLIAMENTARY SCRUTINY OF JUSTICE AND HOME AFFAIRS AGENCIES

BRUNO DE WITTE AND JORRIT J. RIJPMA

1. INTRODUCTION

With the entry into force of the Lisbon Treaty, the Area of Freedom, Security and Justice (AFSJ) has taken the last step towards becoming an area of EU competence as any other. The removal of the pillar structure and the extension of the ordinary legislative procedure to all matters pertaining to justice and home affairs (JHA) have granted the European Parliament important new powers. Still, the AFSJ retains two of its characteristic features. First, the competences grouped under Title V of the TFEU touch upon the core of Member States' sovereign powers: migration, family and criminal law. Even more importantly, EU action in this area may impact on fundamental rights. Both factors call for sound democratic oversight.

A characteristic of the AFSJ has been its focus on practical cooperation arrangements rather than, or in addition to, harmonising national legislation. This has resulted in the establishment of 'light' institutional governance structures, such as agencies, whose task is to facilitate, coordinate and strengthen the cooperation between national authorities.[1010] Agencies have been given a degree of autonomy from the institutions and Member States in order to shield the exercise of 'technical' tasks from the political institutions, both European and national.[1011]

The two most prominent agencies in the AFSJ are Europol and Eurojust. Both originate under the former third pillar of the EU.[1012] The Lisbon Treaty has provided them with a legal basis in the TFEU. Although classified by the Commission as 'operational' agencies, a more correct description would be 'coordination' agencies. They coordinate joint law enforcement operations carried out by Member States' authorities, yet they do not have autonomous executive powers. Their intergovernmental background, structure and strong links to the Council—rather than the Commission—set them apart from the regulatory agencies established under the former Community pillar.[1013] At the same time, one can observe a gradual alignment with other EU agencies.[1014]

Europol and Eurojust are complemented by a number of other JHA agencies: the European agency for the coordination of operational cooperation at the external borders of the EU (Frontex), the European Police College (CEPOL) and the European Asylum Support Office (EASO).[1015] A proposal for the establishment of an agency for the operational management

[1010] Monar 2006, p. 19.
[1011] Groenleer 2009.
[1012] Council Act drawing up the Convention based on Article K.3 of the Treaty on European Union…, replaced by Council Decision 2009/371/JHA ('Europol Decision'); Council Decision 2002/187 ('Eurojust Decision').
[1013] Chiti 2009, p. 1398.
[1014] Rijpma 2010.
[1015] Council Regulation (EC) No 2007/2004 ('Frontex Regulation'); Council Decision 2005/681/JHA (CEPOL); Regulation (EU) No 439/2010 (EASO). One could also include the European Union Agency for Fundamental Rights

of large-scale IT systems in the AFSJ (SIS, VIS and EURODAC) is pending.[1016] Whilst the CEPOL, EASO and the future IT Agency are not involved in the coordination of law enforcement activities, part of Frontex's tasks is exactly that and it may therefore be considered an 'operational' or 'coordination' agency.[1017]

This study will look at the accountability mechanisms available to the European Parliament to control the work and functioning of Frontex, Europol and Eurojust. The findings for Frontex can, *mutatis mutandis*, be applied to the remaining JHA agencies as the latter follow the more or less standard structure for EU 'regulatory' agencies. The study will evaluate the legal and practical arrangements that have been put in place to provide the Parliament with the information it requires to carry out its supervisory tasks. Finally, the role of the Council's Standing Committee on Internal Security Committee (COSI) and the importance of parliamentary scrutiny of this body will be highlighted.

2. POLITICAL ACCOUNTABILITY

2.1 Management Board

Primary democratic control over agencies is exercised by the Member States and the Commission through their representatives in the administrative board, normally called the Management Board. Amongst the most important powers of the Management Board are the yearly adoption of the work programme, the general report and the budget. It may exercise disciplinary control over the Executive (or Administrative) Director and his deputy. The organisational structure of Eurojust is somewhat different in view of its judicial tasks. Its governing board, the College, consists of national members who have their regular place of work at the agency's seat in The Hague.[1018] The European Parliament does not have a representative on the Management Board. This is generally considered undesirable as it would confuse the legislative and controlling function of the Parliament with that of the Executive.[1019]

The Management Board members that represent Member States are responsible to their respective governments, which in turn are controlled by national parliaments. The members appointed by the Commission answer to the Commission, which in turn is controlled by Parliament. More generally, the influence of the Commission over agencies is considerable because of its representation on the Management Boards, its role in drafting the EU budget, its resources and frequent contacts with the agency's administration.[1020] However, the semi-autonomous status of agencies makes it hard to hold the Commission directly accountable for their actions. Therefore, Parliament's power to censure the Commission does not seem to constitute an effective or even appropriate means of control on EU agencies. A comparable problem can be observed in the Member States as regards ministerial responsibility for independent agencies.[1021]

(FRA), set up by Council Regulation (EC) No 168/2007, although its scope of activity extends beyond the AFSJ domain.
[1016] COM (2010) 93 final.
[1017] Rijpma (forthcoming 2012).
[1018] Article 2(2)(a), Eurojust Decision.
[1019] COM (2002) 718, p. 9; COM (2010) 776, p. 16.
[1020] Busuioc (September 2009).
[1021] Maggetti 2010.

2.2 Agency Director

The Executive (or Administrative) Director is the key official of an EU agency, being its legal representative and responsible for its management. S/he prepares and implements the agency's work plans and budget.[1022] The European Parliament does not have a role in the appointment procedure of agencies' directors. In view of the important role of the Agency Director, involvement of the European Parliament could be a useful tool for ex-ante democratic control. The Commission seemed to endorse this view when in 2002 it proposed to make formal appointment of candidates for the post of Director dependent on a hearing before Parliament.[1023] However, in its 2010 Communication on Europol, it argued against involvement of Council or Parliament as this could render the appointment a political issue.[1024] Still, it would seem that the appointment is inevitably a political matter, even where the appointing body is the Management Board.

In fact, hearings in EP committees could be held prior to the appointment of an agency's Executive Director without the need to amend the founding acts of those agencies. The question is which consequences should be attached to such hearings. The recognition of a veto right for Parliament would probably require legislative amendment. At the time of the adoption of the Europol Decision, Parliament was unsuccessful in obtaining the right to hear candidates and provide the Management Board with an order of preference. One could also contemplate an arrangement that is currently being tested as regards the European External Action Service (EEAS), under which the Committee on Foreign Affairs, Fundamental Rights and Common Security and Defence Policy (AFET) may invite newly appointed Heads of Delegation for an informal 'exchange of views' before taking up their posts, but only after their appointment.[1025]

Agency Director				**Commissioners**
JHA Agency	**Europol**	**Eurojust**	**Frontex**	
Appointment	Art. 38(1), Council, QMV, on proposal MB	Art. 29, College, 2/3rds majority, Com participates in selection procedure	Art. 26(2), MB, 2/3rds majority, on proposal Com	Art. 17(7) TFEU, EP RoP (Rule 106), European Council, QMV, after consent EP
Dismissal	Art. 38(7), Council, QMV, after opinion MB	Art. 29(4), College, 2/3rds majority	Art. 26(2), MB, 2/3rds majority	Art. 17(8) TFEU, EP RoP (Rule 107), 2/3rds majority of votes cast, representing majority of MEPs
Term of Office	4 yrs renewable once	5 yrs, renewable once	5 yrs, renewable once	5 years, renewable

Fig. 1: Agency Directors compared with Commissioners

[1022] The role of Eurojust's Administrative Director is somewhat more limited as the College forms a permanent body actively involved in the day–to-day activity of the Agency.
[1023] COM (2002) 718, p. 11.
[1024] COM (2010) 776, p. 16.
[1025] High Representative of the Union for Foreign Affairs and Security Policy (20 July 2010). Note that the procedure for appointment of Heads of Delegation is still in an experimental phase and, therefore, does not yet offer a clear model that could serve as a precedent for agency directors.

2.3 The European Parliament's Instruments

Despite the semi-autonomous status, MEPs make important use of their power to ask questions to the Commission and the Council regarding JHA agencies. The most important committee for the political monitoring of these agencies' activities is the Committee for Civil Liberties, Justice and Home Affairs (LIBE). Within LIBE, a number of MEPs have developed an expertise on specific files and agencies. Interestingly, most questions have been addressed to the Commission, which seems to reflect the increasing importance of this institution in the AFSJ and the level of control it is believed to exercise over JHA agencies.[1026]

Parliament may invite the directors of JHA agencies for questioning. For Europol, this option has been phrased as an obligation for the Executive Director ('shall appear').[1027] The Frontex Regulation merely states that the Council and Parliament 'may invite' the Executive Director.[1028] The Eurojust Decision is silent on the matter. However, 'accountability practices' have developed and even in the absence of any obligation to do so the director of Europol, the President of the College of Eurojust as well as Frontex's Director have appeared in hearings before the Parliament.[1029]

Parliamentary Committees may issue own-initiative reports.[1030] LIBE has frequently prepared such own-initiative reports on JHA related issues, including on the role of different JHA agencies. For instance, 2008 and 2009 reports discussed the role of Frontex.[1031] Currently, own-initiative reports are being prepared on organised crime in Europe and on the European Internal Security Strategy, which also take into account the role of Europol and Eurojust.[1032] Own-initiative reports have mainly been used to evaluate and influence policy directions and not so much as a means of direct control over JHA agencies, although they could be used for the latter purpose as well. However, such reports remain one-off events and do not provide for the 'comprehensive, constant and clear' monitoring of EU policies which Parliament felt to be lacking in the area of criminal justice.[1033] In its 2009 recommendation, it called for the establishment of 'an objective, impartial, transparent, comprehensive, horizontal and continuous monitoring and evaluation system of the implementation of EU policies and legal instruments in this area', which should include both a technical and a political dimension.[1034]

In case of serious structural problems, Parliament could consider the setting up of a Committee of Inquiry, also as a means of pressuring the Management Board to exercise its powers of control.[1035] Such committees are temporary and may be established on the request of one-quarter of Parliament's Members in the case of alleged infringements of EU law or maladministration in the application of EU law by, inter alia, EU bodies. This seems

[1026] Previous term: 229 questions in the Parliament's registry refer to Europol (81), Eurojust (34) or Frontex (114), of which 145 directed to Commission and 84 to Council. Current term (registry last consulted 10 March 2011): 163 questions referring to Europol (65), Eurojust (13) and Frontex (86), of which 124 directed to the Commission and 39 to the Council.
[1027] Article 48, Europol Decision.
[1028] Article 25(3), Frontex Regulation.
[1029] Busuioc 2010, p. 209.
[1030] Rule 45 of Parliament's Rules of Procedure (RoP).
[1031] European Parliament 11 November 2008; European Parliament 6 April 2009.
[1032] Rapporteur Rita Borsellino (S-D) and Rapporteur Sonia Alfano (ALDE).
[1033] European Parliament recommendation of 7 May 2009. See also: De Capitani (2009), pp. 51–72.
[1034] Ibid.
[1035] Article 226 TFEU, RoP 176. See also the Decision of the European Parliament, the Council and the Commission of 19 April 1995….

to be a heavy measure and past Committees of Inquiry have been set up to investigate issues of major concern such as the BSE crises, climate change and the social, economic and financial crisis. At the same time, they lack formal powers to summon witnesses and hear them under oath.[1036]

2.4 Reporting and Evaluation Obligations

Democratic oversight is facilitated through a number of reporting and evaluation obligations laid down in the founding instruments of Europol, Eurojust and Frontex.[1037] Each year, agencies are obliged to adopt a work programme and prepare a general report on the previous year. The general reports, with the exception of that of Europol, are made public and translated into all official languages. Frontex and Eurojust make their work programmes available on their website.

All founding acts provide for a periodical evaluation of the agency's functioning over a period of 4–5 years. These external and independent evaluations may provide valuable input for improvements and possible legislative amendments. The reports of the evaluation are either forwarded to Parliament or made public.

The adoption of the Europol Decision made an important improvement to Parliament's position which, under the Europol Convention, only received a specially adopted version of the annual report. In its 2010 Communication on procedures for the democratic scrutiny of Europol, the Commission proposed a debate in LIBE on Europol's multiannual strategy and annual work program.[1038] If this were to be done by all agencies, it would allow Parliament to have greater influence on the setting of JHA agencies' priorities.

The Commission also advocates a more pro-active communication strategy. Europol should, for instance, systematically inform Parliament of its operational achievements and the results of its bi-annual 'user survey'.[1039] Similar measures could also enhance the transparency of other JHA agencies. Frontex, for instance, now only reports on its joint operations in overall terms in its general report, whilst the individual evaluation reports of single operations is often not publicly available.

2.5 Oversight of Data Collection

Frontex, the only JHA agency originally set up as a Community body, is subject to Regulation (EC) No 45/2001, which provides for supervisory powers of the European Data Protection Supervisor (EDPS) and the appointment of a data protection officer within the Agency. Europol and Eurojust have their own data protection regime incorporated in their founding act. Both have a data protection officer and a Joint Supervisory Body (JSB) composed of representatives of the Member States' national supervisory bodies, which fulfils tasks comparable to that of the EDPS.

Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters does not apply to these agencies.[1040] Moreover, Article 28 states that the Framework Decision leaves specific data

[1036] See: Shackleton 2002 (the powers of committees of inquiry have not changed since then).
[1037] Reporting obligations as regards the budgetary procedure will be discussed in Section 3.
[1038] COM (2010), p. 15.
[1039] COM (2010), p. 16.
[1040] Framework Decision 2008/977/JHA.

protection rules adopted prior to the Framework Decision unaffected. A general overhaul of the data protection regime is foreseen in the Commission's Communication of 2010 on data protection, in which the Commission states the objective of establishing a comprehensive and coherent system in the EU and vis-à-vis third countries. This would 'entail the need to consider a revision of the current rules on data protection in the area of police cooperation and judicial cooperation in criminal matters'.[1041]

It has been argued that the 'specific nature and sensitivity of the processing operations in the fields of police and justice' calls for tailor-made rules, potentially leaving co-existing supervisory systems in place.[1042] Indeed, any reform should take account of the experience and expertise of existing supervisory bodies. However, a single legal framework seems preferable in terms of transparency, legal certainty and cost-efficiency.[1043] It would form a strong signal that JHA policies no longer are governed by intergovernmental exceptionalism but by generally applicable EU standards.

2.6 Oversight of 'External Relations'

JHA agencies have the power to conclude agreements or so-called working arrangements with their counterparts in third countries and with international organisations within their respective field of competence.[1044] Europol and Eurojust may only conclude the agreements after approval by the Council, which in the case of Eurojust has to act by qualified majority. Parliament is not informed and does not play any role, formal or informal, in the conclusion of such agreements. In view of Parliament's increased role in the AFSJ after Lisbon, including its external dimension, this would require urgent attention and correction.

With the exception of Frontex, which for the time being does not have the power to process personal data, agreements concluded by the JHA agencies may cover the exchange of personal information.[1045] In such a case, the Joint Supervisory Body of the agency must give its opinion and will have an important role in ensuring an adequate level of data protection in the implementation of the agreement.

In the case of Frontex, it is problematic that the Agency often cooperates with third countries on the basis of bilateral international agreements or non-binding memoranda of understanding between an individual Member State and the third country in question. Often the non-binding legal nature of these bilateral agreements means that they are not published. Moreover, access to these documents by the public has been denied.

In addition, there is the need for the EP to monitor the role assigned to JHA agencies in 'real' international agreements of the EU. For instance, the SWIFT Agreement on bank data transfers states that Europol will verify and approve requests for data from the US.[1046] MEPs, national parliamentarians and national data protection authorities have already voiced their concern over the secrecy surrounding the implementation of this agreement. The German Federal Commissioner for Data Protection and Freedom of Information has denounced in strong terms the lack of effective auditing of the Agreement. [1047] Similarly,

[1041] COM (2010) 609.
[1042] Alonso Blas 2010, p. 250.
[1043] De Hert and Bellanova March 2009.
[1044] Article 23, Europol Decision; Article 26a, Eurojust Decision; Articles 13–14, Frontex Regulation.
[1045] The pending Commission Proposal amending the Frontex Regulation (COM (2010) 61) does foresee granting Frontex a limited mandate to process personal data, p. 4.
[1046] Article 4(3-5), Agreement between the EU and the USA on the processing and transfer of Financial Messaging Data….
[1047] Council Document 6266/11.

MEPs have voiced loud discontent over the classification of all documents concerning the Agreement as 'top-secret'.[1048] Here there is an obvious role for the JSB to ensure Europol offers an adequate level of data protection.[1049] The problem of the lack of access to confidential information will be discussed further in Section 5.

2.7 Cooperation with National Parliaments

Articles 85 and 88 of the TFEU provide that the founding acts of Eurojust and Europol should be recast as regulations. These should include provisions on their evaluation by the European Parliament and national parliaments. Both the importance of national parliaments as a source of legitimacy and the nature of JHA competences call for joint supervision of JHA policies and agencies.[1050] In 2010, the Commission published its Communication on procedures for the democratic scrutiny of Europol.[1051] According to the Stockholm Programme's Action Plan a similar Communication for Eurojust will follow in 2011.[1052]

In its 2010 Communication, the Commission considered that most of Parliament's concerns as regards its role in scrutinising Europol had been addressed by the 2009 Europol decision. Outstanding issues related primarily to the role of national parliaments' involvement in the democratic scrutiny of Europol. National parliaments have experienced difficulty in scrutinising Europol's work through the national representatives on the Management Board, in finding information and in coordinating their efforts, internally amongst national parliaments and with the European Parliament.[1053] This is likely to apply also to Eurojust and Frontex.

The absence of a well-structured framework does not mean that national parliaments have showed a lack of interest in the scrutiny of JHA policies and agencies. Roughly two out of three national parliaments have exercised some form of monitoring of Eurojust and Europol.[1054] Importantly, the UK House of Lords has published reports on all three JHA agencies under discussion.[1055] National parliaments and the European Parliament exchange information through the Interparliamentary EU Exchange Information Network (IPEX), a website for the electronic exchange of information.[1056] There are informal contacts between national and European parliamentarians and within European political families also on JHA issues. In addition, there have been a number of hearings, joint committee meetings and joint parliamentary meetings held on the role of Europol and Eurojust. As early as 2001, recommendations for a 'Parlopol' Committee were made, but it was not established as a formal parliamentary committee.[1057] In 2010, the Conference of the Speakers of the Parliaments of the EU held in Brussels endorsed the proposal for the setting up of a European Intelligence Review Agencies Knowledge Network (EIRAN), implemented through a website.[1058]

Finally, the Conference of national parliaments' European Affairs Committees (COSAC) must be mentioned. The AFJS and the political monitoring of Europol and evaluation of

[1048] *EU Observer* 16 March 2011.
[1049] See Europol's JSB report of 1 March 2011, which establishes serious faults in the overview of the agreement.
[1050] See also: Mitsilegas 2007.
[1051] COM (2010) 776.
[1052] COM (2010) 171. The Council Presidency noted that Europol could set a precedent for other EU agencies (Council Document 6847/11, p. 3).
[1053] See also: Ruiz de Garibay 2010.
[1054] COSAC 31 May–1 June 2010, pp. 24 and 26.
[1055] House of Lords Select Committee on the EU 2004, March 2008 and November 2008.
[1056] See (www.ipex.eu).
[1057] European Parliament 7 September 2006, p. 5.
[1058] Declaration of Brussels….

Eurojust's activities have become regular items on the COSAC agenda.[1059] A majority of COSAC's members have supported the idea of COSAC debates on Europol and Eurojust to be preceded by a hearing of the directors of the respective agencies and experts.[1060]

The potential for COSAC in the political monitoring of JHA agencies finds its expression in Article 10 of Treaty Protocol No 1 on the role of national parliaments. COSAC is to promote the exchange of information and best practice between national Parliaments and the European Parliament, including their special committees, and may organise interparliamentary conferences on specific topics. The Commission, in its 2010 Communication, proposed the setting up of a permanent joint or interparliamentary forum in which both national and European members of parliament are represented. It furthermore suggested that such a forum could establish a sub-group to liaise directly with Europol. Interestingly, it did not explicitly refer to COSAC.[1061]

The idea for increased inter-parliamentary cooperation must be applauded. However, a concern that was voiced at the strategic seminar organised by Eurojust and the Belgian Presidency should be repeated here. Increased parliamentary scrutiny should not result in additional administrative burdens on JHA agencies. Evaluation should take into account the specific nature of the tasks of these agencies and the purpose, criteria and scope of any form of scrutiny should be well-established in advance. The Council has questioned the added value of the interparliamentary forum.[1062] However, if such a forum would take the form of a permanent interparliamentary committee, it could very well enable more structural political supervision of Europol and Eurojust. Preferably, such a committee would also scrutinise other JHA agencies, allowing for a common approach towards JHA agency supervision. If such a forum is to be prevented from becoming a talking shop, it would have to be able to count on sufficient administrative support and consistency in its membership and frequency of meetings. Importantly, the EP and the national parliaments would have to react to the forum's conclusions and recommendations.

2.8 Conclusion

Busuioc has found that the European Parliament's political oversight of agencies is often incident-driven, focusing on a limited number of politically salient issues.[1063] An analysis of parliamentary questions on Frontex, Eurojust and Europol in the current and previous term seems to confirm this observation for JHA agencies. Busuioc has argued that such 'fire-alarm' oversight may be preferable for a high-level political forum, as full-time supervision would be too burdensome.[1064] Although indeed LIBE would lack the resources for full-time supervision, its members would certainly have the expertise. A more long-term reflection on JHA related policies can be found in LIBE's own-initiative reports, which provide the Parliament's outlook on the future directions of these policies. The establishment of an inter-parliamentary forum with members from both LIBE and its national counterparts would constitute a more structural means of parliamentary scrutiny.

There are diverging views as to the intensity of parliamentary scrutiny of JHA agencies. The Commission and Council advocate supervision that is limited to an overall assessment of the JHA agencies' performance. It can be argued that Parliament is not to enter into the

[1059] COSAC 31 May–1 June 2010, p. 8.
[1060] COSAC 25–26 October 2010, p. 8.
[1061] COM (2010) 776, p. 15.
[1062] Council Document 6847/11.
[1063] Busuioc 2010, p. 209.
[1064] Ibid.

assessment of specific joint operations coordinated by JHA agencies. These activities are not carried out by JHA agencies themselves but by national authorities under national law. For this reason, they are also outside the jurisdiction of the Court of Justice of the European Union (CJEU).[1065] The Commission and Council correctly note that the level of parliamentary control over Europol is already higher now than that exercised by national parliaments on their national police services.[1066] At the same time, knowledge of agencies' specific operational activities, or rather the coordination thereof, may be necessary to be able to successfully evaluate the agencies' overall functioning, and also because it is in the context of joint operational activity that concerns may arise regarding the safeguarding of fundamental rights.

Currently, Parliament is merely informed of JHA agencies' work plans and does not have a direct say over the setting of priorities, other than through its budgetary powers. On the one hand, this does justice to the semi-independent status of agencies and the idea that the setting of objectives should be based on non-political considerations based on independent expert analysis. On the other hand, the conclusions drawn from technical assessments—the risk management—are very much a political balancing act. Yet, the prioritisation of JHA agencies' work is determined by their Management Boards, the Commission and the Council. As noted by Mitsilegas in relation to the EU's Internal Security Strategy, 'scrutiny which is confined to the examination of EU legislative proposals and calling EU officials to give evidence may not provide the most effective way of parliamentary control […] if not combined with scrutiny at the level of strategy and operations'.[1067] Parliamentary debates on the JHA agencies' multi-annual and annual work programmes could form a first step in involving Parliament.

3. FINANCIAL ACCOUNTABILITY

The financial accountability of JHA agencies is twofold. First, there is a political financial accountability towards the Parliament as regards the setting of the agencies' budgets and the discharge. Secondly, the EU's financial regulations, as well as internal and external audits, ensure that the budget is implemented in accordance with the basic principles of sound accounting.

3.1 Adoption of the Budget

Until the adoption of the Europol Decision in 2004, Europol was funded through national contributions. Today, a subsidy from the general EU budget forms the main source of income for all JHA agencies, including Europol. Parliament has a final say on all expenditure on the general budget, including the amount of funds made available to the JHA agencies. Through this 'power of the purse', it can exercise considerable influence over agencies. In 2008, for instance, the Parliament increased Frontex's funds but put thirty per cent of the administrative budget in reserve only to be released when the Parliament was satisfied that the agency had improved its performance and accountability.[1068]

Each year the Management Board of the agency adopts a draft estimate, including a draft establishment plan, together with a draft work programme. This is forwarded to the

[1065] Article 276 TFEU.
[1066] As noted by both Commission (COM (2010) 776, p. 14) and Council (Document 6847/11, p. 2).
[1067] Mitsilegas 2011, p. 80.
[1068] House of Lords Select Committee on the EU 5 March 2008, p. 28. See European Parliament Resolution of 13 December 2007….

Commission by 31 March, which in turn forwards it to the Council and Parliament. On the basis of this estimate, the Commission enters the amounts necessary into the draft budgets. The EP's Committee on Budgets (BUDG) will produce a report on all sections of the draft budget, including Justice and Home Affairs.[1069] LIBE will give its input for this report in an opinion. In addition, MEPs, political groups or Committees as a whole can table amendments that will be voted upon in the Committee on Budgets. The Management Board adopts the agency's budget, but this only becomes final after adoption of the general EU budget and, where necessary, it will be adjusted.

3.2 Implementation

The Financial Regulation that lays down the rules for the establishment and implementation of the general Community budget refers expressly to agencies.[1070] Although Europol and Eurojust were not initially set up as Community bodies, their founding instruments make the 'Community' Financial Regulation applicable. On the basis of Article 185(1) of the Financial Regulation, the Commission has adopted a Framework Financial Regulation for bodies set up by the Communities, having legal personality and receiving grants charged to the Community budget.[1071]

3.3 Discharge Procedure

By 1 March following each financial year, the agency's accounting officer communicates the provisional accounts to the Commission's accounting officer together with a report on the agency's budgetary and financial management. The Commission's accounting officer forwards the Agency's provisional accounts to the Court of Auditors, together with its own report on the budgetary and financial management. This report is also forwarded to the Parliament and the Council. Upon receipt of the observations of the Court of Auditors, the Agency's Executive Director draws up the final accounts and forwards these to the Management Board for an opinion.

By 1 July of the following year, the Executive Director sends the final accounts to the Commission, Council, Parliament and the Court of Auditors. These are public. By 30 September, s/he also sends a reply to the observations of the Court of Auditors to the Court of Auditors itself and the Management Board.

LIBE will provide the Committee on Budgetary Control (CONT) with an opinion on the discharge with respect to the implementation of the specific agencies, as well as the implementation of the general budget of the EU. In these opinions, LIBE will make suggestions for CONT to incorporate in its motion for a Resolution. CONT also publishes a yearly overall report on the performance, financial management and control of EU agencies.

In its report for the discharge of 2009, CONT complimented Eurojust on its initiative to include Key Performance Indicators in its 2010 plans and recommended this as best practice for the other agencies, allowing stakeholders to better evaluate agencies' performance. It furthermore encouraged agencies to establish multiannual work programmes.[1072] After a negative opinion of CONT in 2010, Parliament refused discharge

[1069] See, e.g., European Parliament 8 March 2010.
[1070] Article 54, Council Regulation (EC, Euratom) 1605/2002 ('Financial Regulation').
[1071] Commission Regulation (EC, Euratom) No 2343/2002.
[1072] European Parliament 7 February 2011.

for the implementation of the European Police College (CEPOL) 2008 budget. The agency's funding was frozen and a new management put in place. Discharge for the implementation of CEPOL's 2009 budget was also delayed on the advice of CONT, which deemed the reporting 'insufficient to allow a clear understanding of implementation of concrete actions'.[1073]

In case of a positive opinion, Parliament will give a discharge to the Executive Director with respect to the implementation of the budget upon recommendation from the Council before 30 April (Frontex and Europol) or 15 May (Eurojust) of the discharge year + 2.

3.4 Conclusion

The Union's general financial rules and regulations constitute an important instrument for the transparent and sound financial management of the agencies' budgets. Still, the Commission Communication on the future of Regulatory Agencies rightly notes that the small size of agencies compared to institutions would seem to justify 'appropriate adaptations'.[1074] Indeed, there is a concern that multiple audits and financial controls may lead to cumbersome proceedings, distracting the agencies from their core tasks. LIBE provides important input for the reports of BUDG and CONT and the latter committee has proven willing to act in case of serious mismanagement, advising against discharge for the implementation of CEPOL's budget of 2008.

4. JUDICIAL ACCOUNTABILITY

The possibility for the European Parliament to hold JHA agencies accountable before the CJEU is limited. The CJEU has long held that, in accordance with Article 263 of the TFEU, the Court can only review the legality of measures intended to produce legal effects vis-à-vis third parties,[1075] which will seldom be the case. Moreover, no person on the staff of JHA agencies is endowed with autonomous law enforcement powers, let alone powers of coercion. For Europol, this is explicitly stated in Article 88 of the TFEU. There has been some discussion as to the extent to which Eurojust could be given the power under Article 85(1)(c) of the TFEU to order or initiate an investigation. It is submitted that Article 85(1) must be read restrictively on the basis of Article 85(2) of the TFEU, which states that formal acts of judicial procedure shall be carried out by the competent national officials.[1076]

Operational activity at the EU level remains limited to the coordination of operational activities of national law enforcement agencies by EU bodies and institutions, which—since it does not entail decision making—escapes review before the CJEU. Therefore, the extension of the Court's jurisdiction by the Lisbon Treaty to review the acts of bodies, offices and agencies of the Union does not change anything in relation to JHA agencies' coordinating activities.[1077]

[1073] European Parliament Press Release 11 April 2011.
[1074] COM (2008) 135 final, p. 6.
[1075] The Court has consistently held that 'an action for annulment is available in the case of all measures adopted by the institutions, whatever their nature or form, which are intended to have legal effects'. See: CJEU Case 22/70, *Commission v Council*, para. 42; CJEU Case C-57/59, *France v Commission*, para. 7.
[1076] A discussion of the possible future establishment of a European Public Prosecutor on the basis of Article 86 TFEU goes beyond the scope of this study.
[1077] Article 263 TFEU. The new treaty article does confirm, however, that agencies' decisions in the field of, e.g., public procurement, would be liable to review before the CJEU.

5. ACCESS TO INFORMATION

Despite the numerous information and evaluation obligations of JHA agencies, in practice the access by MEPs and their staff to information emanating from the JHA agencies, as well as information relating to the AFSJ policy field in general, has proven problematic. There is a tendency for JHA agencies and the other institutions to invoke the specific nature of JHA agencies' tasks in order to withhold access to information that would help the Parliament to exercise its supervisory powers. The classification of all documents relating to the implementation of the SWIFT Agreement, referred to above, is a case in point. MEPs have also voiced strong disapproval over the lack of information and evaluation of the EU's Counter-Terrorism Policy and Internal Security Strategy.[1078]

5.1 Access to documents

The founding acts of both Eurojust and Europol refer to the need for confidentiality of the information held by the agency.[1079] These acts also oblige the governing bodies to adopt a decision on access to documents, taking into account the limits and principles of Regulation (EC) No 1049/2001 on access to documents.[1080] The Frontex regulation contains an obligation of transparency, making Regulation (EC) No 1049/2001 applicable in full to the Agency. In the course of the current procedure for the revision of the Access to Documents Regulation, LIBE Rapporteur Michael Cashman (PES) has proposed an amendment to the Commission's draft, which would bring all EU agencies within the scope of the Regulation.[1081]

Article 4 of Regulation (EC) No 1049/2001 contains important exceptions, in particular for reasons of public security, defence and military matters, and international relations. These exceptions are likely to cover sensitive documents, classified as such by the institution or agency under their respective security regulations and covered by Article 9 of the Regulation.[1082] There are four secrecy levels: restricted, confidential, secret and top secret. Without the consent of the originator, these sensitive documents are not released.[1083] Article 9(7) obliges the Commission and the Council to inform Parliament on sensitive documents in accordance with arrangements agreed between the institutions. The fact that some of the major cases decided by the CJEU on access to documents that were brought by MEPs shows that this provision does not work well in practice.[1084] The Cashman report proposes amendments which would grant Parliament access to classified documents through a special oversight committee composed of seven MEPs appointed by the Conference of Presidents. These members would have to comply with a specific clearance procedure and solemnly swear not to reveal in any way the content of the information accessed. [1085]

[1078] European Parliament Working Document of 14 February 2011…, p. 4.
[1079] Articles 40–41, Europol Decision; Article 25, Eurojust Decision.
[1080] Article 45, Europol Decision; Article 39, Eurojust Decision.
[1081] Amendment 1, Report on the proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (recast) (A6-0077/2009), 19 February 2009, Rapporteur Michael Cashman (PES).
[1082] These are normally based on the Council's Security Regulations: Council Decision 2001/264/EC.
[1083] See: CJEU Case C-266/05 P, paras. 95–97.
[1084] See: CJEU Case C-353/99 P and Cases C-39/05 P and C-52/05 P.
[1085] Amendment 33, Cashman Report, *supra* note 1081.

5.2 Access to information in the CFSP

A 2002 Interinstitutional agreement between the Parliament and Council applies to the access by Parliament of information classified as top secret, secret or confidential in the field of the Common Foreign and Security Policy (CFSP).[1086] Under this agreement, read in conjunction with the 2010 Declaration by the High Representative on Political Accountability, Parliament's President or the AFET Committee may request information from the Presidency of the Council or the High Representative.

In case of sensitive information, documents will be made available for inspection at the Council's premises. Where possible, the information is made available to the President of Parliament who has a choice between three options: granting access to the Chair or members of the AFET Committee, a discussion in the AFET Committee meeting *in camera,* or communication of documents from which information has been expunged. The High Representative can provide access to other documents in the CFSP area on a need-to-know basis to other MEPs, who, for classified documents, are duly security cleared by their home Member State's competent authority in accordance with applicable security rules. This is done at the request of the AFET Chair and, if needed, the President of the Parliament.

The 2002 Agreement specifically mentions that it may serve as an example for other areas. The AFSJ is particularly concerned by this precedent. In the AFSJ, the situation has potentially improved with the extension of the ordinary legislative procedure to matters of JHA, making Parliament a co-legislator. Prior to the entry into force of the Lisbon Treaty, ad hoc agreements between Parliament and the Council provided for access to sensitive documents, if necessary, in *huis clos* sessions in the margins of LIBE.[1087] There is no general agreement on the exchange of sensitive information between the Council and Parliament. Closed meetings have taken place for instance to grant Members of LIBE access to documents regarding the negotiations on international agreements for the exchange of PNR data.

5.3 The 2010 Framework Agreement

The Framework Agreement between the Commission and Parliament, newly concluded in 2010, contains an Annex II dealing in detail with the exchange of sensitive information. As a general rule, the Commission will provide Parliament at its request with all information necessary in order for it to exercise its prerogatives and competences but confidential information from a state, an institution or an international organisation will only be forwarded with the originator's consent. This is likely to apply also to documents stemming from the JHA agencies, as Article 9(3) of Regulation (EC) No 1049/2001 refers to 'the originator' in general. Access to information that is classified as confidential, secret or top secret can only be given to Parliament officials or employees working for political groups for whom it is strictly necessary, who have been designated in advanced and who have received a security clearance by their home Member State's competent authority in accordance with applicable security rules. MEPs who have not received such clearance will be granted access only to confidential information on the basis of arrangements adopted by common accord, including signature of a solemn declaration of non-disclosure. MEPs with a personal security clearance may have access to documents classified as secret.

[1086] Interinstitutional Agreement of 20 November 2002….
[1087] Council Document 7542/06, p. 2.

The actual consultation of documents takes place in a secure reading room if the information is classified as confidential. Other sensitive information may be divulged by holding a meeting *in camera*, attended only by the members of the Parliament's Bureau, the members of the Conference of Presidents or full members and substitute members of the competent parliamentary committee and those employees working for political groups, who have been designated and security cleared in advance. Documents may be numbered and collected after the meeting, and the minutes of the meeting shall not report any discussion of the item. Although the Council has publicly voiced its disagreement with these rules,[1088] they seem to strike a fair balance between maintaining adequate confidentiality and enabling MEPs to exercise their supervisory functions. The system will now have to be tested in practice. An evaluation is foreseen for the end of 2011.

Unlike the agreement with the Commission, the Parliament has currently no framework for the exchange of sensitive information between the Parliament and the JHA agencies. JHA agencies do exchange classified information amongst themselves on the basis of an agreement that considers their security regulations as equivalent. This is also the case for the exchange of sensitive information between the JHA agencies on the one hand and the Council and Commission on the other.[1089] Members of LIBE have in the past been granted access to sensitive documents on an ad hoc basis, largely following the procedure for *in camera* meetings described above. There are, however, no specific structural arrangements in place. Of course, individual MEPs may put forward a request for documents under Regulation (EC) No 1049/2001 but this is obviously a cumbersome procedure. If the experience with access to documents under the Framework Agreement between the Commission and Parliament proves positive, it could well serve as an example for the exchange of information between Parliament and JHA agencies.

The principle of sincere cooperation applies to the relation between Member States and institutions, as well as between institutions, and works both ways. It has been described by the CJEU as an overarching principle which finds specific expression in Article 4(3) of the TEU.[1090] This principle could be invoked by Parliament also against the JHA agencies in order to gain access to sensitive information. A stronger obligation on the JHA agencies to provide sensitive information to Parliament will force it to critically assess whether there is an actual need for classification of documents. Again, this may help to foster a culture of transparency in these agencies and do justice to the mainstreaming of JHA policies after the entry into force of the Lisbon Treaty.

6. THE ROLE OF THE COUNCIL'S COSI

Article 71 of the TFEU provides for the setting up of a Standing Committee on Internal Security (COSI) within the Council. COSI should promote and strengthen operational cooperation on internal security and 'facilitate' the coordination of the activities of Member States' competent authorities. COSI was established by a Council decision of November 2009, although already prior to its entry into force various bodies and working groups worked together towards its establishment.[1091] Its membership consists of high-level

[1088] Council Document 15018/10. See also the Council Legal Service's Legal Opinion: Council Document 12964/1/10.
[1089] Council Document 5524/10.
[1090] CJEU Case 230/81, para. 37.
[1091] Council Document 16515/09.

officials from Member States' Interior Ministries.[1092] The EU's JHA agencies and other bodies, such as the SitCen, may be invited to attend as observers.[1093]

COSI does not have a legislative role. It is also not involved in conducting operations, something which is explicitly left to the Member States. Despite these limitations, COSI has the potential to become an important actor. It has primary responsibility for the EU's internal security strategy, which covers the whole AFSJ.[1094] At the first bi-monthly COSI meeting in June 2010, the 'Member states identified five key objectives: a partly operational and partly strategic role; coordinating the various agencies in the EU; assuming the functions of the police chiefs' task force; assessing the effectiveness of existing legislative instruments; and providing the Council with regular reports on internal security.'[1095]

COSI is likely to have an indirect yet substantial impact on the EU's priority-setting in the AFSJ and by implication on national police activities.[1096] In this manner, the Council has retained important influence over operational cooperation in JHA. Moreover, the JHA agencies have increased their importance through their preparatory work for the Internal Security Strategy.[1097]

Again, there is a lack of involvement of Parliamentary actors in a priority setting. The Council decision merely states that the European Parliament and national Parliaments will remain informed of the proceedings of COSI. This seems an insufficiently strong obligation in order for Parliament to successfully scrutinise the work of COSI. Already in its resolution of 25 November 2009, it called for 'the creation of the evaluation system to give Parliament and national parliaments access to information related to the policies and activities of the internal security committee'. It is indeed important that initiatives for greater involvement of parliamentary actors in the work of JHA agencies are not undermined by a shift of agency activity towards COSI. The proposed joint or inter-parliamentary forum proposed by the Commission for the scrutiny of Europol's powers should therefore extend its remit to the activities of COSI.

7. CONCLUSION

This paper has laid out and evaluated the instruments available to the European Parliament for the democratic oversight of JHA agencies. Whilst there are many formal and informal arrangements which allow Parliament to effectively scrutinise JHA agencies, some important deficiencies have been observed. The entry into force of the Lisbon Treaty now brings the AFSJ squarely within the Treaties' single legal framework. As regards Europol and Eurojust, the Treaty explicitly requires increased control of these agencies by both the European Parliament and national parliaments. It is now up to the EU Commission to present proposals to bring about the necessary legal changes to reflect this new situation. Parliament should not merely be part of the legislative work in the AFSJ but should also be able to actively scrutinise the governance in this policy area.

[1092] This is, however, not explicitly stated in the COSI decision. In the past, differing membership in the European Police Chiefs Task Force (operational staff, officials from different ministries at different levels) has had a stifling effect on its functioning: Van Buuren 2010, pp. 332–333.
[1093] The Joint Situation Centre (SITCEN) forms part of the EEAS but contributes to police cooperation through the provision of threat assessments and counterterrorism intelligence.
[1094] European Council 2010, point 4.1.
[1095] Justice and Home Affairs Post-Council Statement 5 March 2010, Column 121WS.
[1096] Hillebrand 2010, p. 41.
[1097] Ibid., p. 39.

There are a number of very concrete areas in which Parliament should be given greater involvement in the functioning of JHA agencies: the nomination of their Director, their activity in external relations, and the setting of their priorities. In addition, Parliament and JHA agencies should aim to cooperate with each other in a spirit of mutual trust and cooperation. Real and timely access to information, with due regard for the sensitive nature of JHA agencies' activities, is indispensable. The rules on access to documents held by the Commission contained in the 2010 Framework Agreement could serve as an example. Moreover, it would contribute to transparency if all JHA agencies were covered by a single overarching legal framework for access to documents, as well as for data protection.

Although European parliamentary scrutiny of JHA agencies seems to exceed the level of control by national parliaments on national law enforcement agencies, this does not in itself form an argument against strong democratic oversight. The fact that this remains a relatively young and politically sensitive policy area, with a huge transformative potential and possible impact on fundamental rights pleads for an intensive concerted control by European Parliament and national parliaments. This control could take the form of a joint or interparliamentary forum. Such a forum should not merely oversee the JHA agencies but also examine broader institutional arrangements for the coordination of operational cooperation, in particular COSI.

REFERENCES

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, 13 July 2010, OJ 2010, L195/5.

Alonso Blas D. (2010), 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom', *ERA Forum*, Vol. 11, pp. 233–250.

Busuioc M. (September 2009), 'Accountability, Control and Independence: The Case of European Agencies', *European Law Journal*, Vol. 15, No 5, pp. 599–615.

Busuioc M. (2010), *The Accountability of European Agencies: Legal Provisions and Ongoing Practices*, Eburon, Delft, 2010.

Chiti E. (2009), 'An important part of the EU's institutional machinery: Features, problems and perspectives of European agencies', *Common Market Law Review*, Vol. 46, No 5, pp. 1395–1442.

CJEU, Opinion of AG Poiares Maduro in Case C-380/05, *Centro Europa 7* [2008] ECR I-349, delivered on 12 September 2007.

CJEU, Joined Cases C-39/05 P and C-52/05 P*, Sweden and Turco v Council* [2008] ECR I-4723.

CJEU, Case C-266/05 P *Sison v Council* [2007] ECR I-1233.

CJEU, Case C-353/99 P, *Hautala* v Council [2001] *ECR* I-9565.

CJEU, Case C-57/59, *France v Commission* [1997] ECR I-1627.

CJEU, Case 230/81, *Luxembourg v European Parliament* [1983] ECR 255.

CJEU, Case 22/70, *Commission v Council* [1971] ECR 263.

COM (2010), 776 final, Commission Communication on the procedures for the scrutiny of Europol's activities by the European Parliament, together with national Parliaments, 17 December 2010.

COM (2010), 609 final, Commission Communication on a comprehensive approach on personal data protection in the European Union, 4 November 2010.

COM (2010), 171 final, Commission Communication Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme, 20 April 2010.

COM (2010), 93 final, Commission Proposal for a Regulation of the European Parliament and the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 19 March 2010.

COM (2010), 61 final, Commission Proposal for a Regulation of the European Parliament and the Council amending the Frontex Regulation, 24 February 2010.

COM (2008), 135 final, Commission Communication on 'European Agencies - The Way forward', 11 March 2008.

COM (2002), 718 final, Commission Communication on the operating framework for the European regulatory agencies, 11 December 2002.

Commission Regulation (EC, Euratom) No 2343/2002 on the framework Financial Regulation for the bodies referred to in Article 185 of the general Financial Regulation, OJ 2002, L357/72.

COSAC (25–26 October 2010), 'Fourteenth Bi-annual Report: Developments in European Union Procedures and Practices Relevant to Parliamentary Scrutiny', Brussels.

COSAC (31 May–1 June 2010), 'Thirteenth Bi-annual Report: Developments in European Union Procedures and Practices Relevant to Parliamentary Scrutiny', Madrid.

Council Act drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office ('Europol Convention'), OJ 1995, C316/1.

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ 2009, L121/37 ('Europol Decision').

Council Decision 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA, OJ 2005, L256/63.

Council Decision 2002/187 of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2002, L63/1 ('Eurojust Decision').

Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations, OJ 2001, L101/1.

Council Decision on setting up the Standing Committee on operational cooperation on internal security.

Council Document 6847/11 (22 February 2011), Outcome of proceedings CATS, on 10 & 11 February 2011.

Council Document 6266/11 of 8 February 2011, Europol's role in the framework of the EU-US TFTP Agreement and state of play of operational and strategic agreements of Europol (specific focus: the agreement on exchange of personal data and related information that Europol has with the US)—EU information policy on the TFTP Agreement.

Council Document 15018/10 (18 October 2010), Framework Agreement on relations between the European Parliament and the Commission.

Council Document 17625/10 (2010), 'Eurojust and the Lisbon Treaty: Towards more effective actions', Conclusions of the strategic seminar organised by Eurojust and the Belgian Presidency, Bruges, 20–22 September 2010.

Council Document 12964/1/10 (17 September 2010), Opinion of the Legal Service, Draft Framework Agreement between the European Parliament and the Commission.

Council Document 5524/10 (19 January 2010), Annex II, Draft Declaration by the Council and the Commission on the protection and handling of EU classified information (EUCI) by EU agencies, bodies or offices.

Council Document 16515/09 (27 November 2009).

Council Document 7542/06 of 20 March 2006, Draft Interinstitutional Agreement concerning access by the European Parliament to classified information of the Council [and of the Commission] in the field of Freedom, Security and Justice.

Council Framework Decision of 13 June 2002 on joint investigation teams, OJ 2002, L162/1.

Council Regulation (EC) No 168/2007, OJ 2007, L53/1.

Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ 2004, L 349/1 ('Frontex Regulation').

Council Regulation (EC, Euratom) 1605/2002 on the Financial Regulation applicable to the General Budget of the European Communities, OJ 2002, L248/1.

Curtin D. (2006), 'European Legal Integration: Paradise Lost?' in Smits, J. et al., eds., *European Integration and Law*, Intersentia, Antwerp.

De Capitani E. (2009), 'The Possible Role of the European Parliament in evaluating EU judicial cooperation in criminal matters' in: Dane, M. and A. Klip, eds., *An additional*

evaluation mechanism in the field of EU judicial cooperation in criminal matters to strengthen mutual trust, Tilburg, Celsus Legal Publishers, 51–72.

Decision No 574/2007/EC establishing the External Borders Fund for the period 2007 to 2013 as part of the General programme 'Solidarity and Management of Migration Flows', OJ 2007, L144/22.

Decision of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry, OJ 1995, L113/2.

Declaration of Brussels by the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States (30 September–1 October 2010).

De Hert P. and R. Bellanova (March 2009), 'Data Protection in the Area of Freedom, Security and Justice: A system still to be fully developed?', Study requested by LIBE.

EU Observer (16 March 2011), 'MEPs decry "breach of trust" in EU-US data deal'.

European Council (2010), 'The Stockholm Programme: An open and secure Europe serving and protecting the citizens', (OJ 2010, C115/1).

European Parliament (7 February 2011), 'Draft Report on the 2009 discharge: performance, financial management and control of EU agencies', Rapporteur Georgios Stavrakakis (S-D).

European Parliament (8 March 2010), 'Report on Priorities for the 2011 budget – Section III – Commission (A7-9999/2010)', Rapporteur Sidonia Elzbieta Jedrzejewska (EPP).

European Parliament (6 April 2009), 'Report on a Common Immigration Policy for Europe: Principles, actions and tools', Rapporteur Simon Bussutil (PPE).

European Parliament (11 November 2008), 'Report on the evaluation and future development of the FRONTEX Agency and of the European Border Surveillance System (EUROSUR)', A6-0437/2008, Rapporteur Javier Moreno Sanchez (PSE).

European Parliament (7 September 2006), Meeting Document: 'What Future for Europol? Increasing Europol's Accountability and Improving Europol's Operational Capacity', Brussels.

European Parliament (2002), 'Final Report of the European Convention Working Group X on Freedom, Security and Justice', CONV 426/02.

European Parliament Press Release (11 April 2011), 'EU Police College and Medicines Agency management not good enough'.

European Parliament Recommendation of 7 May 2009 to the Council on development of an EU criminal justice area.

European Parliament Resolution of 13 December 2007 on the draft general budget of the European Union for the financial year 2008 as modified by the Council (P6_TA(2007)0616).

European Parliament Working Document of 14 February 2011 on the European Union's internal security strategy Committee on Civil Liberties, Justice and Home Affairs, Rapporteur Rita Borsellino (S-D).

Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008, L350/6.

Groenleer M. (2009), *The Autonomy of European Union Agencies: A Comparative Study of Institutional Development*, Eburon, Delft.

High Representative of the Union for Foreign Affairs and Security Policy 20 July 2010), Declaration on Political Accountability at the Adoption of a Council Decision establishing the organisation and functioning of the EEAS, Brussels.

Hillebrand C. (December 2010), 'Written Evidence for the House of Lords EU Sub-Committee F (Home Affairs) on The EU Internal Security Strategy'.

House of Lords Select Committee on the EU (12 November 2008), 'EUROPOL: coordinating the fight against serious and organized crime', HL Paper 183, Session 2007–08, 29th Report.

House of Lords Select Committee on the EU (5 March 2008), 'FRONTEX: the EU external borders agency', HL Paper 60, Session 2007-08, 9th Report.

House of Lords Select Committee on the EU (21 July 2004), 'Judicial Cooperation in the EU: the role of Eurojust', HL Paper 138, Session 2003-04, 23rd Report.

Interinstitutional Agreement of 20 November 2002 between the European Parliament and the Council concerning access by the European Parliament to sensitive information of the Council in the field of security and defence policy, point 3.3, OJ 2002, C298/1.

Justice and Home Affairs Post-Council Statement (5 March 2010), Parliamentary Under-Secretary of State for the Home Department (Meg Hillier), Hansard, Column 121WS.

Maggetti M. (2010), 'Legitimacy and Accountability of Independent Regulatory Agencies: A Critical Review', *Living Reviews in Democracy*, No 2.

Mitsilegas V. (5 January 2011), 'Written Evidence for the House of Lords EU Sub-Committee F (Home Affairs) on the EU Internal Security Strategy.

Mitsilegas V. (2007), 'Interparliamentary Co-operation in EU Justice and Home Afffairs', paper prepared for the conference 'Fifty Years of Interparliamentary Cooperation', Stiftung Wissenschaft und Politik, Berlin, 13 June 2007.

Monar J. (2006), *Specific Factors, Typology and Development Trends in Modes of Governance in the EU JHA Domain*, New Gov Project, Strasbourg.

Regulation (EC) No 45/2001 of 30 May 2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L8/1.

Regulation (EU) No 439/2010 of 19 May 2010 establishing a European Asylum Support Office, OJ 2010, L132/11.

Rijpma, J. (2010), 'Justice and Home Affairs Agencies: governing the Area of Freedom, Security and Justice after Lisbon', paper presented at the ECPR fifth Pan-European Conference, Porto, 24–25 June 2010.

Rijpma, J. (forthcoming 2012), 'Hybrid agencification in the Area of Freedom, Security and Justice and its inherent tensions: the case of Frontex' in Busuioc, M., Groenleer, M. and J. Trondal, eds., *The Agency Phenomenon in the European Union: Emergence, Institutionalisation, and Everyday Decision Making*, Manchester University Press, Manchester.

Ruiz de Garibay D. (2010), 'Interparliamentary Cooperation in the EU: A case study of Justice and Home Affairs', paper presented at the 60th Political Studies Association Annual Conference 'Sixty Years of Political Studies: Achievements and Futures', Edinburgh, 29 March–1 April 2010.

Shackleton M. (2002), 'The European Parliament's New Committees of Inquiry: Tiger or Paper Tiger?', *Journal of Common Market Studies*, Vol. 36, No 1, pp. 115–130.

Van Buuren J. (June 2010), 'Spin in het Europese politieweb: het Comité', *Internationale Spectator*, Vol. 64, No. 6, pp. 332–335.

ANNEX B: THEMATIC STUDIES

II. EUROPOL AND EUROJUST

ALEXANDRA DE MOOR & GERT VERMEULEN

1. INTRODUCING EUROPOL AND EUROJUST

An examination of the oversight mechanisms for Europol and Eurojust has to begin with an examination of these agencies. In the first part of this study, Europol and Eurojust are introduced as two police and judicial cooperation in criminal matters agencies. Their changing legal basis, competence and tasks are assessed, with a particular focus on the Lisbon Treaty. The relationship between Europol and Eurojust is also examined, as it is by no means an accountability relationship between an actor (Europol) and a forum (Eurojust).

1.1 Europol

Based in The Hague (NL), the European Police Office (Europol) is the EU law enforcement agency that handles criminal intelligence. Its objective is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.

1.1.1 Legal basis

Europol commenced full activities on 1 July 1999 after ratification of the 1995 Europol Convention (OJ C 316, 27.11.1995), which was amended by three Protocols: the 2000 Money Laundering Protocol (OJ C 358, 13.12.2000), the 2002 Joint Investigation Teams Protocol (OJ C 312, 16.12.2002) and the 2003 Danish Protocol (OJ C 2, 6.1.2004). The Europol Decision was adopted on 6 April 2009 (OJ L 121, 15.5.2009). As decisions are more easily adaptable than conventions, Member States hoped to increase Europol's flexibility. On 1 January 2010, Europol became a formal agency of the European Union (EU).[1098] Under the Lisbon Treaty (OJ C 306, 17.12.2007), Europol will find its legal basis as stated in Article 88 of the Treaty on the Functioning of the European Union (TFEU): the European Parliament and the Council shall determine Europol's structure, operation, field of action and tasks by means of regulations, which also lay down the procedures for scrutiny of Europol's activities by the European Parliament, together with national Parliaments. While the Commission, in its Action Plan Implementing the Stockholm Programme (COM (2010) 171 of 20.4.2010), only foresees the Proposal for a Europol Regulation for 2013, the European Parliament called for a proposal to be submitted six months after the entry into force of the Lisbon Treaty (OJ C 41E, 19.2.2009).

1.1.2 Competence

A visible trend in Europol's competence is the shift from specific crimes towards more general crime.[1099] Drug trafficking provided the main rationale for Europol in the pre-Convention era. In the Convention era, organised crime became the primary rationale for

[1098] See De Moor & Vermeulen 2010a.
[1099] See De Moor & Vermeulen 2010b.

Europol. The organisation was made competent to support law enforcement action against a list of crimes (see Annex Europol Convention), where an organised criminal structure was involved and two or more Member States were affected (Article 2 of the Europol Convention). In the Europol Decision, the organised criminal structure is no longer a limiting element. This makes serious crime the dominant theme. Article 88 of the TFEU is an affirmation as now it also mentions 'serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy'.

1.1.3 Tasks

Europol's core task has always been to support the competent national authorities in their criminal intelligence work. National units and liaison officers liaise between Europol and national police forces, immigration and customs authorities. For its supply of information, Europol depends on the Member States. It is tragic that 80% of the information exchanged by national liaison officers stationed at Europol is exchanged without actually going through Europol, and hence without being stored in Europol's information systems.[1100] The Europol Information System (IS) is a central EU repository for serious organised crime. The Analysis Work Files (AWFs) offer more sensitive information, with limited access only, and allow Europol to provide analysis for ongoing investigations and operations in the Member States. The Europol Decision continues to stress Europol's information-related tasks. Article 88 of the TFEU also gives prominence to 'the collection, storage, processing, analysis and exchange of information (…)'.

Europol staff lack executive powers: they cannot carry guns, conduct home searches or tap wires, nor can they question, arrest or detain suspects. However, the Member States have over time endowed Europol with powers that enable it to do more than collect and analyse information. Since March 2007, Europol has the mandate to participate in 'joint investigation teams' (JITs), albeit in a support capacity.[1101] A JIT can be described as a team consisting of representatives of law enforcement and other authorities of different states jointly investigating cases of international or cross-border crime. Within the limits provided for by national law, Europol officials are allowed to assist in all activities and exchange information with all the members. However, they are not allowed to take part in any coercive measures. Europol's semi-operational tasks undergo no significant changes in the Europol Decision. The Lisbon Treaty is more ambitious in its wording. There is but one restriction: 'The application of coercive measures shall be the exclusive responsibility of the competent national authorities' (Article 88 (3) of the TFEU). A development of this kind is thus excluded.

A further extension of Europol's operational tasks will make it all the more necessary to have counterbalancing forms of accountability and control, as both are 'intrinsically interlinked'.[1102] This has given rise to a 'chicken and egg' debate[1103]—whether improved forms of control should come before more operational powers for Europol, or should be introduced afterwards to avoid undermining the effectiveness of the organisation by burdening it with too heavy accountability procedures. The second part of this study elaborates further on the question of Europol's accountability and control.

[1100] House of Lords 2008, p. 22.
[1101] See De Moor 2009.
[1102] Bruggeman 2006, p. 64.
[1103] Anderson & Apap 2002, p. 65.

1.2 Eurojust

The EU's Judicial Cooperation Unit (Eurojust) is also based in The Hague (NL). In addition to stimulating the coordination and improving the cooperation between the competent authorities of the Member States in investigations and prosecutions, Eurojust shall otherwise support these authorities in making their investigations and prosecutions more efficient.

1.2.1 Legal basis

Eurojust was established by the Decision of 28 February 2002 (OJ L 63, 6.3.2002), which was amended in 2003 (OJ L 245, 29.9.2003) and 2008 (OJ L 138, 4.6.2009). Under the Lisbon Treaty, Eurojust will find its legal basis as stated in Article 85 of the TFEU: the European Parliament and the Council shall determine Eurojust's structure, operation, field of action and tasks by means of regulations, which also determine arrangements for involving the European Parliament and national Parliaments in the evaluation of Eurojust's activities. The Commission, in its Action Plan Implementing the Stockholm Programme, foresees the Proposal for a Eurojust Regulation for 2012. It is difficult to understand the different timetables for Europol (2013) and Eurojust (2012), notably for settling the procedures for parliamentary oversight. As suggested in the second part of this study, these procedures should be very similar.

1.2.2 Competence

Eurojust has always had a general competence for serious crime, particularly when it is organised. Eurojust is thus competent for the same crimes as Europol. Upon request of a national prosecutor, Eurojust can provide assistance in case of any other type of offence. Limitations to Eurojust's competence include the requirement that an investigation or prosecution shall concern two or more Member States (Articles 3 and 4 of the Eurojust Decision). Article 85 of the TFEU also refers to 'serious crime affecting two or more Member States, *or requiring a prosecution on common bases*'. The latter phrase is an important change in formulation, suggesting that Eurojust could initiate coordination in areas where a common criminal policy strategy is needed.

1.2.3 Tasks

It is important to consider Eurojust's 'double nature' for the analysis of its tasks.[1104] Under the current legal framework, these are only tasks of a coordinating, recommending and supporting nature. They differ according to whether Eurojust acts through one of its 27 national members (judges, prosecutors or police officers of equivalent competence) or as a College, consisting of all national members (Articles 6 and 7 of the Eurojust Decision).

The 2008 Eurojust Decision introduced a number of significant changes, in particular with regard to the powers of Eurojust national members in their capacity as competent national authorities acting in accordance with national law—as opposed to acting on behalf of Eurojust. The original Eurojust Decision had set very low minimum standards. Consequently, the powers of national members varied considerably. Once the new provisions are implemented (before June 2011), all national members of Eurojust should be granted certain minimum powers (Article 9b to 9e of the Eurojust Decision). National members are also formally entitled to participate in JITs concerning their own Member

[1104] Vlastnik 2008, p. 37.

State, either as a national competent authority or on behalf of Eurojust (Article 9f of the Eurojust Decision).

An area where the remit of Eurojust is extended considerably is the collection, processing and exchange of personal data, including the establishment of a Case Management System (CMS) (Article 16 of the Eurojust Decision). The CMS is as an EU-wide judicial database containing information on all investigations and prosecutions reported to Eurojust.[1105] A Eurojust national coordination system is also established (Article 12 of the Eurojust Decision), thereby closing the gap between The Hague and the national capitals.[1106]

The 2008 amendment refrains from introducing changes with regard to the character of Eurojust's requests to national authorities to initiate investigations and prosecutions. Although currently non-binding, in practice they can have a great influence on the way cases are dealt with. Therefore, the impact of Eurojust's activities on the position of the citizens, in particular with regard to the protection of fundamental (defense) rights, should be kept in mind. Eurojust is also empowered to process personal data, which leads to the issue of data protection. The second part of this study elaborates further on the question of Eurojust's accountability and control.

Concerning Eurojust's tasks, the Lisbon Treaty clearly goes further than the current legal framework, allowing for granting Eurojust certain binding powers with regard to the national authorities. Article 85 of the TFEU offers concrete possibilities to transform Eurojust from a simple mediator at a horizontal cooperation level to a player with binding operational powers at a vertical integration level. Nevertheless, the changes remain limited because, unlike Article 86 of the TFEU, the centre of gravity for investigations and prosecutions would not be transferred at the EU level. Article 86 of the TFEU paves the way for the establishment, by means of regulations, of a European Public Prosecutor's Office (EPP). The creation of Eurojust had always been intimately connected to the EPP, which has its origins in the *Corpus Iuris* Project.[1107] The EPP resurfaced in the—stillborn—Constitutional Treaty (2004) (OJ C 310, 16.12.2004) and in the Lisbon Treaty.

Although the EPP is to be established by unanimity, there is a possibility for at least nine Member States to use enhanced cooperation. It may only concern 'offences against the Union's financial interests'. An extension with 'serious crime having a cross-border dimension' again requires unanimity. As the competence of the EPP, at least in the beginning, will be limited, Eurojust will remain in its (possibly changed) structure. Article 86 of the TFEU provides that the EPP will be created '*from* Eurojust'. There are different scenarios as to how both bodies could function alongside one another.[1108] The EPP could become a 28th national member and sit in the College every time the protection of the financial interests of the Union is discussed. An alternative is that the College of Eurojust itself would become the EPP.

The European Commission will prepare the establishment of the EPP, starting with a Communication in 2013. This exercise demands a real impact assessment, in the light of how Eurojust works and how judicial cooperation in the protection of the financial interests of the Union works.

[1105] Bures, 2010, 240.
[1106] Nilsson 2010, p. 75.
[1107] See Van den Wyngaert 2004.
[1108] See Nilsson 2010, p. 78; CEU 17625/10 of 8.12.2010, p. 22.

1.3 THE RELATIONSHIP BETWEEN EUROPOL AND EUROJUST

One of the basic visions for Eurojust involved granting it the role of Europol's supervisor. This view stressed that the rule of law requires police to be subject to judicial oversight, and that in most Member States police investigations in criminal matters are under judicial or prosecutorial supervision and control. The creation of Eurojust, however, did not provide in a power to exercise supervision and control of Europol's activities.[1109] The situation in the EU anno 2011 is not equivalent to the relations between the police and the judiciary in the Member States. However, the relationship between Europol and Eurojust may change fundamentally in the future if an EPP is established. Depending on the place of the various European criminal justice agencies in the future institutional architecture of the EU, the issue of supervision of Europol may have to be revisited.

The present relationship between Europol and Eurojust is based on the principle of complementarity. The two agencies concluded a cooperation agreement in 2004, which was revised in 2009. The negotiations of the 2004 Agreement were difficult as some members of the Europol Management Board were reluctant to agree to any wording that would imply supremacy for Eurojust of Europol.[1110]

The practical relations between the two agencies have been rather complicated. In the area of Eurojust's access to AWFs, significant progress was made only in the past couple of years. The 2003 Danish Protocol created the possibility for Europol to invite third experts to be associated with the activities of an analysis group. Eurojust eventually became associated with the first AWFs in June 2007.[1111] Europol promotes Eurojust's participation in AWFs, but the final decision lies with the Member States. In 2008, a secure communication link was established to facilitate the exchange of information (including personal data) between Europol and Eurojust.[1112] Cooperation recently received a new boost, triggered by the 2009 Agreement, as well as by the 2009 Swedish Presidency's request to CEPOL, Eurojust, Europol and Frontex to improve their cooperation. The latter resulted in a jointly drafted Report (CEU 8387/10 of 9.4.2010) and a Scorecard to track the implementation (CEU 5676/11 of 25.1.2011). A staff exchange programme, starting in 2011, has been agreed between Europol and Eurojust. Both agencies have improved their cooperation regarding the promotion of JITs. Europol and Eurojust have also agreed on a table of equivalence to exchange classified information above the level of 'restricted'.

2. THE ACCOUNTABILITY AND CONTROL OF EUROPOL AND EUROJUST

Governance, control, accountability, oversight, scrutiny, evaluation… are very popular terms often used interchangeably. The meaning of these concepts is by no means agreed. Rather than feeding semantic discussions, this paper uses a pragmatic operationalisation of accountability and control. As opposed to direct control, accountability amounts to information, explanation and justification ex post facto. Accountability is a non-intrusive dimension of control in the sense that it does not amount to direct interference in the agent's zone of discretion or a limitation of the agent's statutory autonomy as granted by

[1109] Gless, Grote & Heine 2004, pp. 37–38.
[1110] House of Lords 2004, p. 29.
[1111] Eurojust 2008.
[1112] Eurojust 2009.

the mandate.[1113] Thus, accountability is in essence retrospective, whereas control mainly concerns forward-looking mechanisms. Nevertheless, systems of control often include accountability mechanisms. This implies that accountability is part of the broader concept of control. Others, however, see control as one element of an overarching concept of accountability.[1114]

This study draws on Bovens' conceptual framework and advocates a narrow concept of accountability defined as 'a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgment, and the actor may face consequences'.[1115] A general distinction between internal and external accountability is maintained.[1116] There are different mechanisms through which accountability is achieved (managerial, political, legal, administrative and democratic). This analysis takes into account every single forum—both European and national—which oversees the functioning of Europol and Eurojust. The implications of the Lisbon Treaty are again considered, in particular in relation to parliamentary oversight, and some concrete recommendations are made.

According to Fijnaut,[1117] 'Europol is perhaps the most controlled police agency in Europe'. Although this is exaggerated, the office is certainly subject to extensive controls, at least on paper. Nevertheless, the control of Europol has remained a source of concern in academia and civil society.[1118] To a lesser extent, this also holds true for Eurojust.

2.1 Internal mechanisms of accountability and control

2.1.1 Management boards

Management boards are referred to by different names across EU agencies. For Europol, it is the Management Board. For Eurojust, it is the College.

2.1.1.1 Europol Management Board

The Europol Management Board (Article 37 of the Europol Decision) is to meet at least twice a year but de facto meets six times a year. It is composed of 27 national (police and/or ministerial) representatives and one representative of the Commission, each having one vote and acting by a two-thirds majority. The composition of the Management Board is not public, whereas this is common for other agencies (including Eurojust). The Management Board is mandated to oversee the Director's performance. Similarly, it is provided that the Director is accountable to the Management Board. The Europol Director (Article 38 of the Europol Decision), who is responsible for the day-to-day management of Europol, gives a written and oral report at every Management Board meeting. Moreover, in addition to the annual report, he submits a yearly internal evaluation report on the performance of Europol. Most EU agencies are required to commission an independent audit every few years. Now that Europol has been transformed into an agency, it is also subject to external evaluation (Article 37(11) of the Europol Decision). The evaluation report, commissioned by the Management Board, is forwarded to the European Parliament, the Council and the Commission.

[1113] Busuioc 2009.
[1114] Venice Commission 2007, p. 16.
[1115] Bovens 2006, p. 9; Bovens 2007, p. 452.
[1116] cf. den Boer 2001, p. 32.
[1117] Fijnaut 2004, p. 255.
[1118] e.g., Gless 2002; Hayes 2002; Wagner 2004 and 2006.

The quality of the accountability process is seriously impaired by the size of the Board, which allows little time for interventions and in-depth discussion.[1119] Moreover, the Management Board gets almost completely sidetracked into administrative and technical details, as opposed to considering the status of AWFs or the agency's strategy. Given the strategic and operational output of Europol, this casts doubts on the extent to which the Management Board is successful in holding the agency accountable.[1120] The Europol Decision now specifically demands that the Management Board adopt a strategy for Europol and that the Chairperson ensures a specific focus on strategic issues.

2.1.1.2 Eurojust College

The Eurojust College (Article 28 of the Eurojust Decision) is 'a collective organ of European character deciding in principle by majority vote'.[1121] As the 27 College members are also the drivers of operational work, they meet twice a week. Eurojust is assisted by a Secretariat, which is headed by the Administrative Director (Article 29 of the Eurojust Decision). The Director is responsible for the day-to-day administration of Eurojust and for budget and staff matters. This is different from most other EU agencies, where the director is not only in charge of the administrative but also the operational side of the organisation.[1122] The dual mandate of the College as the operational arm of the Member States and the management board of an EU agency affects internal coherence. Ideally, the College would only be involved in strategic aspects. However, representatives with smaller operational caseloads have involved themselves deeply in the management of the Eurojust administration.[1123]

The 2008 Eurojust Decision introduced an evaluation clause (Article 41a of the Eurojust Decision). The evaluation report, commissioned by the College, is again forwarded to the European Parliament, the Council and the Commission. Unlike the Europol evaluation report, it is also made public.

2.1.1.3 Data Protection Officer

The function of a Data Protection Officer (DPO) had been successfully introduced with Community institutions and bodies by Regulation (EC) No 45/2001 (OJ L 8, 12.1.2001), before its creation at Europol and Eurojust. However, the Europol and Eurojust DPOs are not part of the existing network of DPOs.

2.1.1.4 Europol

The formal establishment of a Europol DPO has enhanced data protection at Europol (Article 28 of the Europol Decision). The function was already being exercised, however, but without legal basis. The DPO is a member of the Europol staff but acts independently. The DPO has the principal task to ensure the lawfulness and compliance of Europol's processing of personal data, also relating to Europol staff. To this end, the DPO cooperates with the Europol Joint Supervisory Body (JSB).

[1119] Busuioc 2010a, p. 95.
[1120] Busuioc, Curtin & Groenleer 2010, p. 27.
[1121] Vlastnik 2008, p. 37.
[1122] Groenleer 2009, p. 314.
[1123] Ramboll, Euréval & Matrix 2009, p. 172.

2.1.1.5 Eurojust

A Eurojust DPO (Article 17 of the Eurojust Decision) started work already in November 2003. Although a member of the Eurojust staff, the DPO has an independent role in ensuring the lawfulness and compliance of Eurojust's processing of personal data. The DPO also cooperates with the Eurojust Joint Supervisory Body (JSB).

2.2 External mechanisms of accountability and control

2.2.1 EU institutions

Both Europol and Eurojust are primarily creatures of the Council. To varying degrees, the Commission, the Court of Justice and the Parliament also embody the accountability and control of Europol and Eurojust.

2.2.2 Council

2.2.2.1 Europol

The Justice and Home Affairs (JHA) Council[1124] is responsible for the political steering of Europol, although the overall supervision resides under the Article 36 Committee (CATS), which is in fact *under* the Council.[1125] The Council has a number of responsibilities towards Europol.[1126] The Council, and on its behalf the Management Board, lays down strategic priorities for Europol, taking particular account of Europol's strategic analyses and threat assessments. These priorities have not always been clear. Europol's annual work programme has been described as an 'aggregate of wish lists'.[1127]

The Council disposes of several sanctioning instruments. The Council appoints the Director and the Deputy Directors of Europol. The Europol Decision introduces a direct link between performance and reappointment but it remains to be seen how this will be implemented in practice. No dismissals have ever been undertaken by the Council. This would amount to a highly sensitive, political issue, likely to come at high costs for the agency as a whole. A strong reluctance to resort to formal sanctions has been voiced in other European agencies as well.[1128] A more implicit sanctioning instrument of the Council is the possibility to amend Europol's legal basis.[1129] With the Europol Decision, this process becomes less cumbersome and the Council can make amendments through the adoption of new decisions. Last but not least, Europol's financing is made subject to an agreement by the European Parliament and the Council, co-acting as Europol's new budgetary authority.

The Council also exercises control over Europol's agreements with third States and organisations.[1130] The Director can only start negotiations with third States and organisations with the authorisation of the Council. Moreover, the draft agreement can only be concluded once the Council has given its approval and, as far as it concerns the exchange of personal data, only after receiving the opinion of the JSB. This is an instance

[1124] In its JHA configuration, this EU institution is made up of the Justice and Interior Ministers of the Member States.
[1125] den Boer, Hillebrand & Nölke 2008, p. 11.
[1126] See Art. 4 (2); Art. 10 (4) *in fine*; Art. 14 (1) *in fine*, Art. 23 (2); Art. 26 (1); Art. 34 (6) and (7); Art. 37 (9) (h) and (10); Art. 38 (1) and (7); Art. 40 (1); Art. 42 Europol Decision.
[1127] Groenleer 2009, p. 295.
[1128] Busuioc 2010b, pp. 87–91 and 129–131.
[1129] Curtin 2005, p. 101.
[1130] See Heimans 2008.

of control—as opposed to accountability—for the Council not only retrospectively demands explanations from Europol but remains in the driver's seat during the whole process. Europol's room for manoeuvre is still significant. Moreover, the control exercised by the Council is by no means a substitute for oversight by a democratic, directly elected European Parliament, which leads to the conclusion that there is a serious accountability deficit in Europol's external relations.[1131]

2.2.2.3 Eurojust

Eurojust is directly accountable to the JHA Council, to which it is required to provide regular reports (Article 32 of the Eurojust Decision). In addition to an annual report, the President should submit any report or any information on the operation of Eurojust required by the Council. The examination of the Eurojust annual report results in direct Council follow-up. The Council reacts with conclusions, which contain an assessment of the performance during the previous year as well as future directions. The picture for Europol is different. The general report on Europol's activities is merely submitted to the Council 'for endorsement' (Article 37(10)(c) of the Europol Decision). To this extent, the accountability process is more comprehensive and better developed from an institutional learning perspective in the case of Eurojust than it is for Europol.[1132] Compared to Europol, however, the Council lacks sanctioning powers in relation to the Eurojust President and the Administrative Director.

The role of the Council in Eurojust's external relations is minimal. Although agreements with third States and organisations can only be concluded after consultation with the Eurojust JSB and after the approval by the Council, Eurojust merely has to inform the Council of any plans it has for entering into such negotiations (Art. 26a Eurojust Decision). Eurojust has considerably more leeway than Europol. This is further exacerbated by the lack of any democratic oversight, which leads to the conclusion that there is a massive accountability deficit.

2.2.3 Commission

2.2.3.1 Europol[1133]

The Member States had always been reluctant to grant the Commission a role with regard to Europol. It used to have one observer seat on the Europol Management Board, without voting rights (Article 28(4) of the Europol Convention). With Europol's change of status the Commission became a full voting member. It is also for the Commission to propose the agency's annual budget,[1134] which is then subject to approval by the two arms of the EU's budgetary authority, the Council and the Parliament.

Reportedly, the presence of the Commission in the Management Board with voting rights has given rise to concerns among Member State representatives that 'Europol will become a Commission organ' through attempts of the Commission to over-influence decision making.[1135] However, there is no indication of the Commission playing a misbalanced role. Moreover, a drastic shift in the balance of power in the Management Board is unlikely given

[1131] Peers 2005, p. 268.
[1132] Busuioc 2010a, p. 109.
[1133] The European Commission's Directorate-General for Home Affairs (created on 1 July 2010 from a division of DG Justice, Freedom and Security) is the parent DG for Europol.
[1134] See in great detail Art. 42 and 43 Europol Decision.
[1135] Busuioc, Curtin & Groenleer 2010, p. 23.

the mandate of Europol and the fact that the main 'clients' of Europol are national law enforcement authorities, not the Commission or other EU institutions.[1136]

2.2.3.2 Eurojust[1137]

The Commission is to be fully associated with the work of Eurojust (Article 11 of the Eurojust Decision). Even though during the negotiations of the Eurojust Decision the Commission tried to obtain a seat, the Member States considered that the Commission should not be part of the College given the operational nature of much of the College's work.[1138] The fact that the operations of Eurojust remain apolitical is seen as important to safeguard its legitimacy and acceptability among Member States.[1139] The Commission has affirmed that it does not want to be involved in concrete investigations, 'but we definitely need to follow very closely what the needs and the loopholes in criminal prosecutions at the European level are so we can exert our right of initiative to pass over those difficulties'.[1140]

By fixing the Eurojust budget, the Commission can minimally influence the agency's activities. Eurojust is also funded through the EU budget, although salaries of the national members are still borne by their Member State of origin, revealing the intergovernmental features of Eurojust. Eurojust staff are EU staff, subject to EU Staff Regulations.

2.2.4 Court of Justice

2.2.4.1 Europol

Judicial control over Europol is fragmented, since the Court of Justice shares its minimal responsibilities with the national courts. It is the primary duty of the national courts to decide on cases brought before them by the national prosecution authorities. A judgment on the activities of Europol and its staff is barred by the Protocol on the Privileges and Immunities of the EU, which is annexed to the Lisbon Treaty. A narrow field of accountability remains, as there is an exception for Europol's participation in JITs (OJ C 70, 19.3.2010). Another possibility for (indirect) national supervision is through the rules of evidence: national courts which are, for example, confronted with illegally gathered Europol data may exclude these pieces of evidence.[1141]

Under the Lisbon Treaty the entire field of JHA comes under the general jurisdiction of the Court of Justice of the European Union (Article 251-281 of the TFEU). There is, however, a five-year transitional period, during which the picture remains as follows: the Court of Justice has jurisdiction to give preliminary rulings on the validity and interpretation of the Europol Decision, where the Member State concerned has made a declaration (facultative jurisdiction). It should be noted that no national court has ever sent questions to the Court of Justice. Europol's new legal basis, a decision instead of a convention, also gives the Court of Justice jurisdiction in relation to annulment actions. Moreover, Europol's transformation into an EU agency and the consequent application of EU Staff Regulations to

[1136] Ibid.
[1137] The European Commission's Directorate-General for Justice and Fundamental Rights is the parent DG for Eurojust.
[1138] Groenleer 2009, p. 314.
[1139] Ramboll, Euréval & Matrix 2009, p. 171.
[1140] Quoting JHA Commissioner Vitorino at the *Interparliamentary conference on democratic control on Europol* on 8 June 2001 (X., 2001, p. 148).
[1141] Gless 2002, p. 44.

Europol staff (Article 39 of the Europol Decision) increases judicial control. In fact, several staff cases against Europol have been brought before the Court since 2002.[1142]

The principal mechanism to guarantee judicial accountability of agencies is a review of the legality of the agencies' acts. Under the Lisbon Treaty, the Court of Justice is explicitly granted jurisdiction over agencies' acts, including those of Europol and Eurojust, on par with those of the European Parliament, the Council, the Commission, the European Council and the European Central Bank.[1143] It remains to be seen how the jurisprudence will address this.

In any case, the Lisbon Treaty still excludes the jurisdiction of the Court when it comes to reviewing the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State (Article 276 of the TFEU). The Court of Justice may also not address possible infringements of fundamental rights by Europol.[1144] In this regard the future accession (cf. Article 6 of the Treaty on European Union) of the EU to the European Convention for the protection of Human Rights and Fundamental Freedoms (ECHR) is important, as it would dispel remaining doubts about the right of citizens to bring possible violations of human rights by the EU to the European Court of Human Rights in Strasbourg.

2.2.4.2 Eurojust

As the national members of the Eurojust College are not EU staff, they remain subject to national law. This implies that the supervision over and the accountability of these national members will vary according to the national criminal justice system to which they belong. The different mechanisms of accountability with regard to the national prosecutors and judges in the Member States are way beyond the scope of this paper.

The Eurojust Decision contains no reference to the Court of Justice. Due to its legal basis, the Court has some jurisdiction in the terms of legality review (cf. Europol). The five-year transitional period also applies to the Eurojust Decision.

Here and now, violations of human rights under the horizontal cooperation model, as facilitated by Eurojust, may only give rise to applications against the Member States, not against the relevant EU agencies (e.g., Europol, Eurojust, OLAF). The EU's accession to the ECHR would make it directly accountable for acts emanating from one of its institutions.[1145]

2.2.5 Parliament

Parliamentary oversight of Europol and Eurojust is split between the European Parliament[1146] and the 27 National Parliaments. The main challenge is to find the right balance between a high level of democratic accountability and the need for confidentiality and discretion of police and judicial cooperation agencies working in a highly sensitive area.[1147] In the case of Europol, much has been made about the lack of parliamentary accountability. Although there has been less critique in relation to Eurojust, the problems—and the solutions—are very much alike.

[1142] Peers 2005, p. 260.
[1143] Busuioc, Curtin & Groenleer 2010, pp. 37–38.
[1144] Wagner 2006, p. 1237.
[1145] Van den Wyngaert 2004, P. 233.
[1146] The Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) is the main scrutiny body for Europol and Eurojust.
[1147] Bruggeman 2002, p. 268.

2.2.5.1 Europol

The Europol Decision and the Lisbon Treaty significantly improve the situation of the European Parliament. The European Parliament is confronted with real legislative powers. The reference to the 'ordinary legislative procedure' in Article 88 of the TFEU means that the former co-decision procedure shall apply. Experience with Community agencies shows that once the European Parliament gained co-decision powers, it introduced new procedures of parliamentary scrutiny.[1148] A similar development is likely in the case of Europol, particularly as the European Parliament has long attempted to extend its powers and has been unable to do so. The European Parliament issued a number of reports, asking for:

- Budgetary powers: involvement in the Europol budget procedure and Europol funding through the Community budget;
- Appointment powers: involvement in the appointment and dismissal of Europol's (Deputy) Director(s) and two European Parliament elected representatives to take part in the Management Board meetings;
- Information and consultation rights: an extension of the documents on which the European Parliament shall be consulted; and
- The strengthening of judicial control by the Court of Justice, and ultimately communitarisation (see in great detail COM (2010) 776, 17.12.2010, 7, footnote 16).

Another significant change introduced by the Europol Decision is precisely that Europol's budget has been 'communitarised' into the EU budget. The European Parliament's powers increase as a result as it becomes the budgetary authority for Europol, as well as its discharge authority, politically endorsing Europol's implementation of the budget. It remains to be seen how the European Parliament will make use of it. Furthermore, Article 48 of the Europol Decision provides that the Europol Director, the Chairperson of the Management Board and the Presidency of the Council are obliged—instead of permitted—to appear before the European Parliament at its request.

So while there have been some welcome developments, there is still room for improvement in a future Europol Regulation. The European Parliament should also have a proper say in Europol's agreements with third States and organisations. The extremely late and inadequate involvement of Parliament in the controversial agreements between Europol and the United States in 2001 and 2002 doesn't bear repeating. This concern is, however, absent from the recent Commission Communication (COM (2010) 776, 17.12.2010), which serves as a reflection document on the procedures for scrutiny of Europol's activities. The recommendations focus on the setting up of a permanent joint or interparliamentary forum. The Commission also stresses the importance of separating roles. Hence, the Commission would not recommend that the European Parliament designates members to the Management Board. The Commission is a voting member of the Management Board, which creates an imbalance between both EU institutions. Although the Europol Management Board is largely a strategic body, it also deals with operational matters (e.g., the status of AWFs). Even an observer status for the European Parliament is delicate in this respect. However, a compromise could be to have an agenda with and without representatives of the European Parliament. Equally, the Commission takes the view that the European Parliament should not have a say in the appointment of the Europol Director, to avoid

[1148] Busuioc, Curtin & Groenleer 2010, p. 31.

turning the appointment into a political issue. Of course, this appointment already is a largely politicised decision. A careful examination of the appointment powers of the EP in relation to other EU agencies[1149] could be very helpful.

2.2.5.2 Eurojust

The legislative role of the European Parliament in relation to Eurojust is very similar to what has just been outlined for Europol, with a shift from consultation towards co-decision. In addition, Eurojust was the first third pillar agency ever to be financed from the Community budget. The European Parliament was involved in budgetary control of Eurojust way before Europol. In terms of general parliamentary control, however, the influence of the European Parliament is fairly limited. There is no direct line of accountability between Eurojust and the European Parliament. Article 32 of the Eurojust Decision merely states that 'Each year the Presidency of the Council shall forward a report to the European Parliament on the work carried out by Eurojust and on the activities of the JSB'. There is no formal provision for hearings with the President of the College or the Administrative Director before the European Parliament. The European Parliament does not have access to the same reports as the Council, with the exception of the periodic external evaluation reports. Moreover, the external relations of Eurojust suffer from an accountability deficit in terms of democratic oversight. Europol clearly serves as the negative example here.

Article 85 of the TFEU opens up new prospects for enhanced democratic accountability through 'involving the European Parliament and national Parliaments in the evaluation of Eurojust's activities'. The wording of this provision leaves a lot of room for interpretation. What does 'Eurojust's activities' mean? It is important to bear in mind Eurojust's 'double nature'. Should the evaluation be limited to an overall assessment of the functioning of Eurojust, or should it also cover operational activities? There is no need for parliamentary scrutiny to involve oversight of individual operations, if only for security reasons. Parliamentarians should first and foremost look at the performance of the agency, comment on its strategies and ensure the European citizens that there is 'value for money'. It is desirable to mirror the procedures for scrutiny of Europol's activities as much as possible, as the analysis in the second part of this study shows that the lines of managerial, political, legal, administrative and democratic accountability are very alike for both agencies. At the Strategic Seminar on Eurojust and the Lisbon Treaty (September 2010) (CEU 17625/10, 8.12.2010), there were voices of concern about the possibility that Eurojust would be subject to multiple assessments, not only by the European Parliament. The conclusion was that the evaluation of Eurojust by different forums should be coordinated and implemented in such a way as not to be too cumbersome and time consuming. The EU political masters should take this into account.

2.2.6 EU bodies and agencies

The European Ombudsman and the European Data Protection Supervisor, two EU bodies, and the European Anti-Fraud Office, an EU agency, also qualify as accountability mechanisms, though only marginally.

2.2.6.1 European Ombudsman

The European Ombudsman (Article 288 of the TFEU and Article 43 of the Charter of Fundamental Rights of the EU) is an independent EU body, appointed by the European

[1149] See Busuioc 2010.

Parliament, which has the power to investigate cases of maladministration in EU agencies, including Europol and Eurojust. He increasingly safeguards the administrative accountability of these agencies.[1150] Poor or failed administration occurs if an institution fails to act in accordance with the law, fails to respect the principles of good administration or violates human rights. The European Ombudsman applies the European Code of Good Administrative Behaviour, which explains in more detail what the Charter's right to good administration (Article 41) means in practice. The Ombudsman usually conducts inquiries at the basis of complaints but can also launch inquiries on his own initiative. So far, the cases in relation to alleged maladministration by Europol (10 cases) and Eurojust (two cases) can be divided into two categories: public access to documents and recruitment and dismissal practices. Public access to documents is very important in terms of public accountability. Both Europol and Eurojust have established rules for public access to documents (cf. Article 45 of the Europol Decision and Article 39 of the Eurojust Decision). The European Ombudsman acts as an additional watchdog.

2.2.6.2 European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies.[1151] The EDPS' general objective is to ensure that the European institutions and bodies respect the right to privacy when they process personal data and develop new policies. A number of specific duties of the EDPS are laid down in Regulation (EC) No 45/2001. The three main fields of work are: supervision, consultation and cooperation. In relation to Europol and Eurojust, the EDPS has been active predominantly in the field of consultation and cooperation. The EDPS has, for example, delivered opinions on both the Europol and Eurojust Decisions. The EDPS also continues to cooperate with the Europol and Eurojust JSBs. Unlike other Community institutions and bodies, Europol and Eurojust are still subject to a specific, tailor-made system for the protection of personal data with external independent supervision.[1152] However, the 'agentification' of Europol leads to limited involvement of the EDPS relating to the Europol staff. Europol applies the provisions of Regulation (EC) No 45/2001 to the processing of personal data relating to Europol staff (Article 39(6) of the Europol Decision). This includes monitoring by the Europol DPO and the EDPS. The Eurojust Decision remains silent on this matter.

2.2.6.3 European Anti-Fraud Office (OLAF)

Europol's accountability has been given a brand new, administrative aspect as yet another consequence of its 'agentification'. In the prevention of fraud, the European Anti-Fraud Office (OLAF) can carry out so-called internal investigations, i.e., within EU structures. The rules laid down by Regulation (EC) No 1073/1999 concerning investigations conducted by OLAF (OJ L 136, 31.5.1999) have been made applicable to Europol (Article 49 of the Europol Decision). OLAF has the power to carry out administrative investigations within Europol and has the right to immediate and unannounced access to any information held by Europol, excluding operational data. It covers investigations by OLAF on fraud, corruption, money laundering and other irregularities affecting the financial interests of the European Community. From the very beginning, Article 38 of the Eurojust Decision made Regulation (EC) No 1073/1999 applicable to Eurojust. The College of Eurojust adopted the necessary implementing measures in 2004. Case related information generated in the context of

[1150] Andoura & Timmerman 2008, p. 15; Curtin 2005, p. 112.
[1151] See Hijmans 2006.
[1152] Hijmans & Scirocco 2009, p. 1523.

investigations and prosecutions is explicitly excluded from the scope of OLAF's internal investigations.

2.2.7 Other mechanisms

2.2.7.1 Joint Supervisory Bodies

Administrative accountability also addresses quasi-legal forums and independent supervisory authorities.[1153] This form of accountability bears particular importance with regard to data processing, which is a core activity of both Europol and Eurojust. The supervision mechanisms of the data processing by Europol and Eurojust are generally regarded as solid and sufficient to guarantee an adequate level of protection.

2.2.7.2 Europol Joint Supervisory Body

Europol handles large amounts of sensitive information about individuals and it is vital that Europol takes account of their fundamental rights. As a safeguard, the Europol Decision contains provisions relating to data protection, including the supervision by an independent Joint Supervisory Body (JSB) (Article 33 of the Europol Decision). The JSB is an intergovernmental structure, for it comprises two members of each of the national supervisory bodies.[1154] The exercise of quasi-judicial tasks by the JSB has been criticised because its members are not eligible judges and because their independence would be compromised by also advising Europol on other issues.[1155]

The JSB reviews the activities of Europol to ensure that the rights of the individual are not violated by the storage, processing and use of the data held by Europol. The JSB carries out regular inspections at Europol. In addition, the JSB is responsible for upholding the right of access, as well as the right to correction and deletion of data. If, after an attempt to exercise one of these rights, one is not satisfied with Europol's response, there is an appeal to the JSB (Articles 30–32 of the Europol Decision). The JSB is also responsible for considering whether Europol follows the principles of data protection in a number of specific areas (e.g., examining and commenting on the opening of AWFs; monitoring the transmission of personal data by Europol to Union institutions, bodies, offices and agencies, third States and organisations; and drawing up proposals for common solutions to existing problems).

For reasons of transparency, the JSB is required to draw up regular activity reports. These reports are forwarded to the European Parliament and to the Council. Current practice is that the JSB issues its activity report every two years. So far, four activity reports have been presented to the EU institutions and to the public. The Europol JSB website also features inspection reports and opinions (for example, on agreements with third States and organisations).

The JSB is complemented by National Supervisory Bodies (NSBs), with the task to monitor, independently and in accordance with national law, the permissibility of the input, the retrieval and any communication to Europol of personal data by the Member State concerned. For that purpose, the NSB has access to the data input by the Member State in Europol's information systems. The NSB is one of the two authorities from which citizens

[1153] Puntscher Riekmann 2008, p. 27.
[1154] den Boer & Bruggeman 2007, p. 81.
[1155] Wagner 2006, pp. 1233–1234.

may request a check on data concerning themselves (see Article 33 of the Europol Decision).

2.2.7.3 Eurojust Joint Supervisory Body

Given the very sensitive nature of the information processed by Eurojust (data on persons who are subject to an investigation or prosecution, victims, witnesses and convicted people), it is crucial to ensure that the rights of the data subjects are properly protected. The Eurojust Decision contains several provisions with regard to data protection, including the supervision of data processing by Eurojust.

The Eurojust Joint Supervisory Body (JSB) is an independent external supervisor (Article 23 of the Eurojust Decision). It is composed of three members who are elected by the plenary meeting of Member States' appointees (judges or persons with an equal level of independence). The JSB monitors Eurojust's activities involving the processing of personal data and ensures that they are carried out in accordance with the Eurojust Decision.

The JSB is a redress instance for the Eurojust DPO in cases of non-compliance with the Eurojust Decision, which the College has not resolved within a reasonable time (Article 17(4) of the Eurojust Decision). The JSB also examines appeals, if the applicant is not satisfied with Eurojust's decision (Articles 19(8) and 20(2) of the Eurojust Decision). Furthermore, the JSB carries out controls. There is a yearly study visit, as well as regular on-the-spot inspections. If the JSB considers that a decision taken by Eurojust or the processing of data by it is not compatible with the Eurojust Decision, the matter is referred to Eurojust, which shall accept the decision of the JSB. The JSB also provides its obligatory opinion concerning the provisions on data protection in agreements or working arrangements with EU bodies or cooperation agreements with third States (Articles 26 and 26a of the Eurojust Decision).

The JSB submits an annual report to the Council (Article 23(12) of the Eurojust Decision), which is also made public on the Eurojust JSB website.

2.2.7.4 National Parliaments

The national Parliaments of the EU Member States have a mission to monitor the activities of Europol and Eurojust. This is because Europol is increasingly involved in the criminal procedures of the Member States—albeit in a support capacity. For Eurojust, which can act through national members, this is even more so.

The national parliaments enjoyed certain rights associated with the ratification of the Europol Convention and its amending Protocols (Article 34(3) of the Europol Convention). With the Europol and Eurojust Decisions, these powers have now gone. What remains is the general right to hold JHA Ministers to account for the activities of Europol and Eurojust. Whether national Parliaments have information, consultation or control powers is a purely national matter. Consequently, current practices in parliamentary scrutiny of Europol and Eurojust differ considerably.[1156]

With the Lisbon Treaty, the national Parliaments have everything to gain as they shall be involved—together with the European Parliament—in the scrutiny of Europol's activities and in the evaluation of Eurojust's activities. In addition, both are able to contribute to the

[1156] COSAC 2009, pp. 10–15.

shaping of the Europol and Eurojust Regulations. Thanks to the Protocols on the Role of National Parliaments and the Application of the Principles of Subsidiarity and Proportionality, which are both annexed to the Lisbon Treaty, Europol- and Eurojust-related measures are subject to the scrutiny of the national Parliaments.[1157]

To be effective, parliamentary control cannot just be the sum of 27 fragmented and diversified national parliamentary controls. Therefore, parliamentary control of JHA agencies is an area in which interparliamentary cooperation between the national Parliaments and the European Parliament is likely to have real added value.

Empowering the national parliaments together with the European Parliament is an old idea. 'Parlopol', a joint committee of members of the European Parliament and national Parliaments to oversee Europol, was first suggested at the Interparliamentary conference on democratic control on Europol (June 2001) and taken over by the Commission Communication on Democratic Control over Europol (COM (2002) 95 final). The Lisbon Treaty provides a fresh opportunity to put the idea into practice. The Commission made it tangible in its recent Communication:[1158] 'An interparliamentary forum could consist of both the national Parliaments' and the EP's committees responsible for police matters. This joint body could meet at regular intervals and invite the Director of Europol to discuss questions relating to the agency's work. It could establish a special subgroup, for instance, to liaise directly with Europol. The Commission recommends that the Chairman of the Management Board should also be invited to appear before this body'.

The proposal to establish a joint parliamentary committee is also applicable in the context of Eurojust. It would only make sense if it were the same forum overseeing the activities of both Europol and Eurojust, and perhaps also extending to the other JHA agencies. The Commission has foreseen a Communication on the arrangements for involving the European Parliament and national Parliaments in the evaluation of Eurojust's activities for 2011. It remains to be seen whether it will mirror the 2010 Communication on Europol.

Whatever procedure is adopted, it has to be kept simple. To have a forum in which every Chamber of every Parliament is represented would result in a body of over 100 members. That is unrealistic or, to quote Lord Peter Bowness (UK) at the Interparliamentary Committee Meeting devoted to the evaluation of Europol, Eurojust, Frontex and Schengen (October 2010): 'We don't want a good idea to be buried in bureaucracy'. Using the existing structures as much as possible clearly is the preferable option. We don't need yet another body to oversee Europol and Eurojust. The fundamental choice is where the centre of gravity should lie, with the European Parliament or at the national-interparliamentary level (COSAC).[1159] There are sound arguments for unifying parliamentary control at the EU level, without prejudice to national parliamentary procedures.

[1157] De Capitani 2010, p. 23; Wolff 2009, pp. 3–4.
[1158] European Commission 2010, p. 15.
[1159] See Ruiz de Garibay 2010.

REFERENCES

Anderson M. and J. Apap (2002), *Striking a balance between freedom, security and justice in an enlarged European Union*, Brussels, Centre for European Policy Studies.

Andoura S. and P. Timmerman (October 2008), *Governance of the EU: The Reform Debate on European Agencies Reignited*, EPIN Working Paper N° 19, available at (http://www.ceps.eu/files/book/1736.pdf).

Apap J. (7 September 2006), 'What Future for Europol? Increasing Europol's Accountability and Improving Europol's Operational Capacity', Brussels, available at (http://www.europarl.europa.eu/meetdocs/2004_2009/documents/nt/630/630339/630339en.pdf).

Bovens H. (2006), 'Analysing and Assessing Public Accountability: A Conceptual Framework', *European Governance Papers (EUROGOV)*, N° C-06-01, available at (http://www.connex-network.org/eurogov/pdf/egp-connex-C-06-01.pdf).

Bovens H. (2007), 'Analysing and Assessing Accountability: A Conceptual Framework', *European Law Journal*, Vol. 4, pp. 447–468.

Bruggeman W. (2006), 'What are the options for improving democratic control of Europol and for providing it with adequate operational capabilities', *Studia Diplomatica*, Vol. 1, pp. 163–181.

Bruggeman W. (2002), 'Policing and accountability in a dynamic European context', *Policing and Society*, Vol. 4, pp. 259–273.

Bures, O. (2010), 'Eurojust's Fledgling Counterterrorism Role', *Journal of Contemporary European Research*, Vol. 6, Issue 2, pp. 236-256.

Busuioc M. (2010), 'European Agencies: Pockets of Accountability' in Bovens, M., Curtin, D. and P. 't Hart, eds., *The Real World of EU Accountability: What Deficit?*, Oxford University Press, Oxford, pp. 87–116.

Busuioc M. (2010), *The Accountability of European Agencies: Legal Provisions and Ongoing Practices*, Eburon, Delft.

Busuioc M. (2009), 'Accountability, Control and Independence: The case of European Agencies', *European Law Journal*, Vol. 5, pp. 599–615.

Busuioc M., Curtin D. & M. Groenleer (2010), 'Living Europol: Between Autonomy and Accountability', Paper prepared for the ECPR fifth Pan-European Conference on EU Politics, Porto (Portugal), 24–26 June 2010, available at (www.jhubc.it/ecpr-porto/virtualpaperroom/058.pdf).

COSAC Secretariat (May 2009), *Eleventh Bi-annual Report: Developments in European Union Procedures and Practices Relevant to Parliamentary Scrutiny*, available at (http://www.cosac.eu/en/documents/biannual/).

Council Act of 27 November 2003 drawing up, on the basis of Article 43 (1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol amending that Convention (OJ C 2, 6.1.2004).

Council Act of 28 November 2002 drawing up a Protocol amending the Convention on the establishment of a European Police Office (Europol Convention) and the Protocol on the privileges and immunities of Europol, the members of its organs, the deputy directors and the employees of Europol (OJ C 312, 16.12.2002).

Council Act of 30 November 2000 drawing up on the basis of Article 43 (1) of the Convention on the establishment of a European Police Office (Europol Convention) of a Protocol amending Article 2 and the Annex to that Convention (OJ C 358, 13.12.2000).

Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) (OJ C 316, 27.11.1995).

Council Decision of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009).

Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 138, 4.6.2009).

Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 245, 29.9.2003).

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002).

Council of the European Union (25 January 2011), *Draft Scorecard: Implementation of the JHA Agencies Report* (Document 5676/11).

Council of the European Union (8 December 2010), *Eurojust and the Lisbon Treaty: Towards more effective action—Conclusions of the strategic seminar organised by Eurojust and the Belgian Presidency* (Document 17625/10).

Council of the European Union (9 April 2010), *Final report on the cooperation between JHA agencies* (Document 8387/10).

Council Resolution of 26 February 2010 on a Model Agreement for setting up a Joint Investigation Team (JIT) (OJ C 70, 19.3.2010).

Curtin D. (2005), 'Delegation to EU Non-majoritarian Agencies and Emerging Practices of Public Accountability' in Geradin, D., Muñoz, R. and N. Petit, eds., *Regulation through Agencies in the EU: A New Paradigm of European Governance*, Edgar, Cheltenham, pp. 88–119.

De Capitani E. (2010), 'The Democratic Accountability of the EU's Area of Freedom, Security and Justice Ten Years On' in Guild, E., Carrera, S. and A. Eggenschwiller, eds., *The*

Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme, CEPS, Brussels, 23–30.

De Moor A. (2009), 'The role of Europol in joint investigation teams. A foretaste of an executive European Police Office?' in Cools, M. et al., eds., *Governance of Security Research Paper Series*, Maklu, Antwerpen, pp. 329–358.

De Moor A. & G. Vermeulen (2010a), 'The Europol Council Decision: Transforming Europol into an Agency of the European Union', *Common Market Law Review*, Vol. 4, pp. 1089–1121.

De Moor A. & G. Vermeulen (2010b), 'Shaping the competence of Europol. An FBI perspective' in Cools, M. et al., eds., *Governance of Security Research Paper Series*, Maklu, Antwerpen, pp. 63–99.

den Boer M. (2001), 'Towards a European Framework for Police Accountability: the Case of Europol' in X., *From Europol to Parlopol: Interparliamentary conference on democratic control of Europol*, Boom, Amsterdam, pp. 26–41.

den Boer M. & W. Bruggeman (2007), 'Shifting gear: Europol in the contemporary policing era', *Politique européenne*, Vol. 3, pp. 77–91.

den Boer M., Hillebrand C. and A. Nolke (2008), 'Legitimacy under Pressure: The European Web of Counter-Terrorism Networks', *Journal of Common Market Studies*, Vol. 1, pp. 101–124.

Eurojust (February 2009), *Eurojust Annual Report 2008*, available at (http://www.eurojust.europa.eu/press_releases/annual_reports/2008/Annual_Report_2008_EN.pdf).

Eurojust (January 2008), *Eurojust Annual Report 2007*, available at (http://www.eurojust.europa.eu/press_releases/annual_reports/2007/Annual_Report_2007_EN.pdf).

European Commission (17 December 2010), Communication from the Commission to the European Parliament and the Council on the procedures for the scrutiny of Europol's activities by the European Parliament, together with national Parliaments (COM (2010) 776 of 17.12.2010).

European Commission (20 April 2010), Action Plan Implementing the Stockholm Programme (COM (2010) 171 of 20.4.2010).

European Parliament legislative resolution of 17 January 2008 on the proposal for a Council Decision establishing the European Police Office (OJ C41E, 19.2.2009).

Fijnaut C. (2004), 'Police Co-operation and the Area of Freedom, Security and Justice' in N. Walker, ed., *Europe's Area of Freedom, Security and Justice*, Oxford University Press, Oxford, pp. 241–282.

Gless S. (2002), 'What kind of judicial control do the new protagonists need? The accountability of the European Police Office (Europol)' in De Kerckhove, G. and A. Weyembergh, eds., *L'espace pénal européen: enjeux et perspectives*, Editions de l'Université de Bruxelles, Brussels, pp. 31–45.

Gless S., Grote R. & G. Heine (30 April 2004), *Justitielle Einbindung und Kontrolle von Europol durch Eurojust*, Gutachten erstattet im Auftrag des Bundesministeriums der Justiz, available at (http://www.bmj.de/media/archive/ 399.pdf).

Groenleer M. (2009), *The Autonomy of European Union Agencies. A Comparative Study of Institutional Development*, Eburon, Delft.

Hayes B. (2002), *The activities and development of Europol—towards an unaccountable FBI in Europe*, Statewatch, available at (www.statewatch.org/ news/2002/feb/eufbi.pdf).

Heimans D. (2008), 'The External Relations of Europol—Political, Legal and Operational Considerations' in Martenczuk, B. & S. van Thiel, eds., *Justice, Liberty, Security: New Challenges for EU External Relations*, VUB Press, Brussels, pp. 367–392.

Hijmans H. (2006), 'The European Data Protection Supervisor: The institutions of the EC controlled by an independent authority', *Common Market Law Review*, Vol. 5, pp. 1313–1342.

Hijmans H. & A. Scirocco (2009), 'Shortcomings in EU data protection in the second and third pillars. Can the Lisbon Treaty be expected to help?', *Common Market Law Review*, Vol. 5, pp. 1485–1525.

House of Lords, European Union Committee (2008), *Europol: coordinating the fight against serious and organised crime*, London, available at (http://www. publications.parliament.uk/pa/ld200708/ldselect/ldeucom/183/183.pdf).

House of Lords, European Union Committee (2004), *Judicial Cooperation in the EU: the role of* Eurojust, London, available at (http://www.publications. parliament.uk/pa/ld200304/ldselect/ldeucom/138/138.pdf).

Joint Action of 10 March 1995 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning the Europol Drugs Unit (OJ L 62, 20.3.1995).

Nilsson H. (2010), 'Judicial cooperation in the EU: Eurojust and the European Public Prosecutor' in Guild, E., Carrera, S. and A. Eggenschwiller, eds., *The Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme*, CEPS, Brussels, pp. 73–78.

Peers S. (2005), 'Governance and the Third Pillar: The Accountability of Europol' in Curtin, D. and R. Wessel, eds., *Good Governance and the European Union. Reflections on concepts, institutions and substance*, Intersentia, Antwerpen, pp. 253–276.

Puntscher Riekman S. (2008), 'Security, Freedom and Accountability' in Guild, E. and F. Geyer, eds., *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, pp. 19–34.

Ramboll Euréval & Matrix (December 2009), Evaluation of the EU decentralised agencies in 2009: Final Report Volume III – Agency level findings, available at (http://ec.europa.eu/dgs/secretariat_general/evaluation/docs/decentralised_agencies_2009_part3_en.pdf).

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001).

Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF) (OJ L 136, 31.5.1999).

Ruiz de Garibay D. (2010), *Interparliamentary Cooperation in the EU: A case study of Justice and Home Affairs*, Paper 60th Political Studies Association Annual Conference, Edinburgh, 29 March–1 April 2010, available at (http://www.psa.ac.uk/journals/pdf/5/2010/1634_1490.pdf).

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007).

Treaty establishing a Constitution for Europe (OJ C 310 of 16.12.2004).

Van den Wyngaert C. (2004), 'Eurojust and the European Public Prosecutor in the *Corpus Iuris* Model: Water and Fire?' in N. Walker, ed., *Europe's Area of Freedom, Security and Justice*, Oxford University Press, Oxford, pp. 201–239.

Venice Commission (11 June 2007), *Report on the democratic oversight of the security services*, (CDL-AD(2007)016).

Vlastnik J. (2008), 'Eurojust: A Cornerstone of the Federal Criminal Justice System in the EU?' in Guild, E. and F. Geyer, eds., *Security versus Justice: Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, pp. 35–49.

Wagner W. (2004), *Stop, Europol! Problems of European Police-Cooperation for Parliamentary Control and Civil Rights*, HSFK-Report No 15, available at (http://www.hsfk.de/downloads/report1504.pdf).

Wagner W. (2006), 'Guarding the guards: The European Convention and the communitization of police co-operation', *Journal of European Public Policy*, pp. 1230–1246.

Wolff S. (30 September 2009), 'From The Hague to Stockholm: the Future of EU's Internal Security Architecture and Police Cooperation', Overview Paper, Clingendael European Studies Programme Round Table Seminar, available at (http://www.clingendael.nl/publications/2009/20090930_cesp_paper_swolff_police_cooperation.pdf).

ANNEX B: THEMATIC STUDIES

III. THE EUROPEAN UNION'S AREA OF FREEDOM, SECURITY AND JUSTICE ARCHITECTURE AFTER THE LISBON TREATY

STEVE PEERS

1. INTRODUCTION

This paper provides information and analysis on the 'new intelligence architecture' of the European Union after the Lisbon Treaty, particularly with regard to Europol, Eurojust, Frontex and the European External Action Service (EEAS). It looks at the overall legal framework of these bodies and the specific issues that arise from their intelligence activities, including the regime relating to classified documents, relations with third countries and their accountability to national parliaments, and the European Parliament (EP).

2. LEGAL FRAMEWORK AND CURRENT POWERS OF EUROPOL, EUROJUST, FRONTEX AND THE INTELLIGENCE COMPONENTS OF THE EEAS

2.1 Mandate, functions and powers of each body

2.1.1 Europol

On 1 January 2010, the basic legal acts governing Europol (the previous Convention and Protocols) were replaced by a third-pillar Council Decision (the 'Europol Decision') adopted in 2009.[1160] A parallel Regulation specifies that Europol staff do not have immunity when they participate in joint investigation teams.[1161] The Europol Decision is supplemented by a number of implementing measures.[1162] The Decision differs from the prior Convention and Protocols not only with regard to its legal form and effect but also the application of the EU budget and staff rules, and the modest extension of Europol's tasks (for instance, to establish information systems).

Europol's chief organ is a Management Board, made up of one representative from each Member State with one from the Commission, and taking most decisions by a two-thirds vote,[1163] although day-to-day management is in the hands of a Director and Deputy Directors.[1164] The Board must report annually to the Council on both the previous year's

[1160] OJ 2009 L 121/27.
[1161] Reg. 371/2009; OJ 2009 L 121/1.
[1162] Rules of procedure of the Joint Supervisory Board (OJ 2010 C 45/2); Management Board decision on appointment of the Director and Deputy Directors (OJ 2009 L 348/3); Management Board decision on conditions for data processing (OJ 2009 L 348/1); Council decision on confidentiality rules (OJ 2009 L 332/17); Management Board decision on the rules for analysis work files (OJ 2009 L 325/14); Council decision on the States which Europol can sign treaties with (OJ 2009 L 325/12); and Council decision on Europol's relations with external partners (OJ 2009 L 325/6).
[1163] Article 37 of the Decision.
[1164] Article 38 of the Decision.

activities and plans for the upcoming year, and the Council forwards these reports to the European Parliament.[1165]

Europol's main tasks are to: 'collect, store, process, analyse and exchange information and intelligence'; inform national authorities of information about criminal activities; aid national investigations; ask national authorities to begin or coordinate investigations; provide intelligence and support as regards major events; and draw up threat assessments and strategic analyses.[1166] These tasks include analysis of internet information. Europol has the additional tasks of developing knowledge of investigative procedures, advising on investigations and providing strategic intelligence.[1167]

Europol has competence over 'organised crime, terrorism and other forms of serious crime' listed in the Annex to the Europol Decision, as long as those crimes '[affect] two or more Member States in such a way as to require a common approach by the Member States owing to the scale, significance and consequences of the offences'.[1168] It also has competence over specified 'related criminal offences'.[1169] Europol is also the supervisory body when it comes to transfers of financial data to the US.[1170] It has been given or will be given access to the data in a number of EU information systems:[1171] the Schengen Information System (SIS);[1172] the second generation Schengen Information System (SIS II);[1173] the Visa Information System (VIS);[1174] the Customs Information System (CIS);[1175] and possibly Eurodac, the database of fingerprint data of asylum seekers and irregular border crossers.[1176] There are relatively strict rules on the use of data by Europol, including time limits for the storage of data and provisions on data protection rights of individuals, involving a data protection officer and a Joint Supervisory Body.[1177]

[1165] Art. 37(10) of the Decision.
[1166] Article 5(1) of the Decision.
[1167] Article 5(2) and (3) of the Decision.
[1168] Article 4(1) of the Decision. The Annex lists a further twenty-four crimes, with definitions of four of them.
[1169] Article 4(3) of the Decision.
[1170] Article 4 of the 'Swift' treaty on the terrorist finance tracking programme, or TFTP (OJ 2010 OJ L 195/1).
[1171] See Article 21 of the Decision.
[1172] See Article 101A of the Schengen Convention, as inserted by a Decision (OJ 2005 L 68/44), which was applied from 1 Oct. 2006 (OJ 2006 L 256/18). Europol was given access to the data concerning extradition or arrest warrant requests, persons and objects to be placed under surveillance and objects to be seized or used as evidence in criminal proceedings. Europol is not able to enter or delete data in the SIS. The use of the information, including its transfer to a third State, is subject to the consent of the Member State concerned. Europol may request further information from a Member State. It is striking that Europol's annual reports do not contain any information on Europol's use of the SIS in practice.
[1173] See Article 41 of the Decision establishing SIS II (OJ 2007 L 205/63), which applies the same rules as in the Schengen Convention (as amended). At present, SIS II is scheduled to become operational in the first quarter of 2013.
[1174] The VIS was established by Reg. 767/2008 (OJ 2008 L 218/60) and access to the VIS by Europol and national law enforcement agencies is set out in a related Decision (OJ 2008 L 218/129). Europol will have access to VIS data for the purposes of a specific analysis and for general or strategic analyses (Article 7, VIS Decision). The VIS will consist of extensive information on applicants for Schengen visas and is scheduled to become operational as regards the first region from June 2011.
[1175] The CIS was established by a Convention (OJ 1995 C 316/33) and several Protocols, which were replaced by a Decision (OJ 2009 L 323/20), which will apply from 27 May 2011 (Articles 33–36 of the Decision). Europol will get access to CIS data once that Decision applies; its access will be regulated by rules similar to those governing its access to SIS and SIS II data (Article 11 of the Decision). CIS contains many different types of data, including eleven items of information on persons for use in 'preventing, investigating and prosecuting serious contraventions of national [customs] laws' as defined in the Decision, and for the purposes of 'sighting and reporting, discreet surveillance, specific checks and strategic or operational analysis' (Articles 1–5 of the Decision).
[1176] Eurodac was established by Reg. 2725/2000 (OJ 2000 L 316/1) and became operational in 2003 (OJ 2003 C 5/2). Currently, Europol has no access to the data concerned. The Commission proposed a Decision which would give Europol and national law enforcement bodies access to this data (COM (2009) 344, 10 Sep. 2009; see particularly Article 8) but this proposal lapsed with the entry into force of the Treaty of Lisbon. The Commission's subsequent revised proposal on Eurodac omitted to include access by Europol and national law enforcement agencies: COM (2010) 555, 11 Oct. 2010. However, the Commission has now agreed to table a proposal to this end (see press release of the JHA Council, 11–12 April 2011).
[1177] See the rules of procedure of this body: OJ 2010 C 182/3.

Europol can participate in joint investigation teams, request national authorities to begin investigations, establish information systems (in particular the Europol Information System) and open analysis work files.[1178] An example of Europol's contribution to intelligence gathering and analysis is TE-SAT, the annual report on terrorism in the EU, which is derived from the processing of national information.[1179]

As for the accountability of Europol, admittedly the agency does not have powers as extensive as those of national police authorities—for example, the power to arrest, question and detain suspects. Nevertheless, there is still a need for national and European parliamentary accountability regarding the powers Europol does exercise. Concerning data protection, such accountability would be supplementary to the oversight of Europol's Joint Supervisory Body, which is not an elected body; for example, the parliaments could question Europol as to whether or not it has implemented the recommendations of the Joint Supervisory Board. As regards Europol's tasks of support and coordination, parliaments could have a role questioning the effectiveness of these activities; they could also examine issues relating to Europol's accounts. While Europol's annual reports are somewhat informative, they inevitably reflect the position of the agency and some issues are not discussed in the reports (for instance, as noted above, the use which Europol makes of the Schengen Information System in practice). Although there are some national parliamentary reports on Europol, an additional collective accountability mechanism would disseminate the results of the parliamentary scrutiny process more widely. Finally, the position regarding judicial control of Europol is not clear at present, although it would perhaps be clearer once a post-Lisbon Regulation re-establishing Europol was adopted.

2.1.2 Eurojust

Eurojust was definitively established by a Council Decision in 2002, which was subsequently amended because of the financial rules governing Eurojust and then amended again more substantially in 2008, inter alia, in order to strengthen Member States' support for Eurojust (regarding the powers of national members), to give Eurojust a greater role settling conflicts of jurisdiction, to increase the flow of information to Eurojust, and to overhaul the external relations rules.[1180] Eurojust should be considered part of the EU's 'intelligence architecture'—assuming that this concept encompasses law enforcement intelligence—because it processes personal data derived from police intelligence, including in terrorism cases.

Eurojust is a 'body' of the EU made up of one member seconded by each Member State who may be a prosecutor, judge or police officer depending on the national legal system and whose place of work must be at Eurojust. Each member must be assisted by one deputy and one assistant, and may be assisted by more people. The deputy must be able to replace the national member.[1181] National Members must have, *inter alia*, access to the national registers on criminal records, arrested persons, investigations and DNA.[1182]

The activities of Eurojust are threefold: to coordinate national investigations and prosecutions; to improve cooperation between national authorities, in particular by

[1178] Articles 6–7 and 10–16 of the Decision.
[1179] The report is available here: (http://www.europol.europa.eu/index.asp?page=publications& language).
[1180] OJ 2002 L 63/1, as amended (OJ 2003 L 245/44 and OJ 2009 L 138/14). Member States have until 4 June 2011, if necessary, to amend their national law to comply with the latter amendments (Article 2 of the latter Decision).
[1181] Article 2, Eurojust Decision, as amended.
[1182] Articles 9–9f of the Decision, as amended.

facilitating judicial cooperation and mutual recognition; and to support in other ways the effectiveness of national investigations and prosecutions.[1183] Eurojust may also become involved in assisting investigations and prosecutions involving only one Member State and a non-Member State, once Eurojust has concluded an agreement with the relevant non-Member State or where there is an 'essential interest' in specific cases.[1184] It may also become involved in investigations involving only one Member State and the EU.[1185]

Eurojust's competence encompasses the crimes which Europol is competent to address, plus other offences committed in conjunction with any of the crimes over which it is competent.[1186] Eurojust may also assist in other investigations at the request of a Member State's authorities.[1187] It has established an 'on-call coordination centre' to deal with urgent requests.[1188] When it acts through its individual members, it can, inter alia, request Member States' authorities to begin investigations or prosecutions, to accept that one of them is in a better position to undertake a prosecution, to coordinate between authorities, to set up a joint investigation team, or to take special investigative measures.[1189]

Also, Member States must exchange extensive information with Eurojust.[1190] In particular, Member States must ensure that their national members are aware of: the setting up of a joint investigation, 'and of the results of the work' of such teams; of 'any case in which at least three Member States are directly involved and for which requests for or decisions on judicial cooperation, including regarding instruments giving effect to the principle of mutual recognition, have been transmitted to at least two Member States', where the offence in question is 'punishable in the requesting or issuing Member State by a custodial sentence or a detention order for a maximum period of at least five or six years, to be decided by the Member State concerned', if the offence in question is one of the following: '(i) trafficking in human beings; (ii) sexual exploitation of children and child pornography; (iii) drug trafficking; (iv) trafficking in firearms, their parts and components and ammunition; (v) corruption; (vi) fraud affecting the financial interests of the European Communities; (vii) counterfeiting of the euro; (viii) money laundering; (ix) attacks against information systems'.

Member States must also inform their national members of cases where: 'there are factual indications that a criminal organisation is involved'; 'there are indications that the case may have a serious cross-border dimension or repercussions at the European Union level or that it might affect Member States other than those directly involved'; 'conflicts of jurisdiction have arisen or are likely to arise'; 'controlled deliveries' (subject to certain conditions); and 'repeated difficulties or refusals regarding the execution of requests for, and decisions on, judicial cooperation', including also mutual recognition measures. The types of information concerned are listed in an Annex. There is an exception where supplying information would mean 'harming essential national security interests' or 'jeopardising the safety of individuals'. Eurojust must then provide 'competent national authorities with information and feedback on the results of the processing of information'.

As for access to EU databases, Eurojust was given access to the SIS by means of a measure adopted in 2005, which gave its national members and their assistants access to

[1183] Article 3(1) of the Decision, as amended.
[1184] Article 3(2) of the Decision, as amended.
[1185] Article 3(3) of the Decision, as amended.
[1186] Article 4(1) of the Decision, as amended.
[1187] Article 4(2) of the Decision, as amended.
[1188] Article 5a of the Decision, as inserted.
[1189] Article 6(1)(a) of the Decision, as amended.
[1190] Article 13 of the Decision, as amended.

the SIS alerts concerning extradition and persons who are wanted to assist with a judicial procedure.[1191] Eurojust access to the SIS has been operational since December 2007.[1192] In future, Eurojust will have access to SIS II[1193] and to the CIS.[1194] However, there are no plans to give Eurojust access to VIS or Eurodac data. In practice, in 2008 there were 229 SIS queries by Eurojust national desks. The Eurojust annual report for that year stated that operational information is checked in the SIS, and that information supplied to national authorities has facilitated the finding and arrest of some persons subject to a European Arrest Warrant. The SIS is also used to decide on which European Arrest Warrant to execute, where there are competing warrants. Finally, the report states that the SIS is useful as it permits a quick search to be carried out without having to make formal requests to other national members.[1195]

There are also detailed rules on data protection,[1196] including individual rights for data subjects, restrictions on the processing of personal data, the existence of a Joint Supervisory Body and a data protection officer.[1197]

The involvement of the EP and national parliaments in evaluating Eurojust's activities (as now provided for in Article 85 TFEU) could entail assessment of the effectiveness of Eurojust activities in practice and the adoption of recommendations for the agency to improve its functioning and to focus its operations on certain areas of law—much as the Council has been adopting conclusions on Eurojust's annual reports for some time.

2.1.3 Frontex

Frontex was established in 2004 by a Council Regulation,[1198] in place of an informal system of coordination of national border guards' operations managed by the Council Secretariat, which had developed ad hoc over the previous two years.[1199] The main tasks of Frontex, according to Article 2 of its founding Regulation, are to 'coordinate operational cooperation between Member States' regarding the management of external borders', to 'assist Member States on training of national border guards, including the establishment of common training standards', to 'carry out risk analyses', to 'follow up on the development of [relevant] research', to 'assist Member States in circumstances requiring increased technical and operational assistance at external borders', to 'provide Member States with the necessary support in organising joint return operations' and to 'deploy Rapid Border Intervention Teams'.[1200] In particular, the agency's tasks as regards risk analysis are to 'develop and apply a common integrated risk analysis model', to 'prepare both general and tailored risk analyses to be submitted to the Council and the Commission' and to

[1191] See Article 101B of the 2005 Decision amending the Convention, as applied from 1 Oct. 2006. The data can only be communicated to third States and third bodies with the consent of the Member State concerned.
[1192] See Eurojust's 2007 annual report, p. 11.
[1193] See Article 42 of the SIS II Decision, which will give Eurojust access to alerts concerning missing persons and objects to be seized or used as evidence in criminal proceedings, along with the categories of alerts which it can access at present.
[1194] As noted above, the original Conventions and Protocols establishing CIS will be replaced as from 27 May 2011, at which point Eurojust will have access to the data in CIS (Article 12 of the CIS Decision, OJ 2009 L 323/20). Access to CIS data will be permitted only for 'the national members of Eurojust, their deputies, assistants and specifically authorised staff'.
[1195] The 2009 and 2010 annual reports of Eurojust make no further reference to the agency's use of SIS in practice.
[1196] Articles 14–24 of the Decision, as amended.
[1197] See the rules of procedure of this body: OJ 2004 C 86/1.
[1198] Reg. 2007/2004 (OJ 2004 L 349/1), subsequently amended by Reg. 863/2007 (OJ 2007 L 199/30).
[1199] See further chapter 7 of Peers and Rogers 2006.
[1200] Article 2(1) of Reg. 2007/2004, as amended by Reg. 863/2007.

'incorporate the results of' its risk analysis model in its development of a training curriculum for border guards.[1201]

According to the proposed amendments to the Frontex Regulation tabled in February 2010,[1202] the Agency's tasks regarding risk analysis would be amended to include an 'evaluation of the capacity of Member States to face threats and pressure at the external borders'.[1203] Furthermore, there would be two new relevant tasks: to 'develop and operate information systems that enable swift and reliable exchanges of information regarding emerging risks at the external borders', and to 'provide the necessary assistance to the development and operation of a European border surveillance system and, as appropriate, to the development of a common information sharing environment, including interoperability of systems'.[1204] More specifically, the provisions relating to risk analysis would elaborate upon the task of evaluating Member States, and also require Member States to 'provide the Agency with all necessary information regarding the situation and possible threats at the external borders', for the purposes of risk assessment.[1205]

Currently, Frontex 'may take all necessary measures to facilitate the exchange of information relevant for its tasks with the Commission and the Member States';[1206] the 2010 proposal would supplement this with an obligation to 'develop and operate an information system capable of exchanging classified information with the Commission and the Member States', although this system 'shall not include the exchange of personal data'.[1207]

The EP's proposed amendments to the Commission's proposal would require the risk analyses of Frontex to be sent also to the EP, and would change some of the rules relating to the evaluation of Member States' capacity.[1208] As for the exchange of personal data, the Council's version of the text would insert two new provisions into the Regulation, first of all concerning the processing of personal data in the context of joint return operations and, secondly, concerning personal data collected during joint operations, pilot projects and the deployment of rapid border intervention teams.[1209]

In the first case, Frontex 'may process personal data of persons who are subject to such joint return operations' where it coordinates such operations. The data would have to be deleted ten days after collection at the latest, although Frontex could transfer that data to a carrier if a Member State had not done so. In the second case, Frontex could 'further process personal data collected by the Member States during such operational activities and transmitted to the Agency in order to contribute to the security of the external borders of the Member States of the European Union.' But such data could only cover 'persons who are suspected, by the relevant authorities of Member States, on reasonable grounds of involvement in cross-border criminal activities, in facilitation of illegal migration activities or in human trafficking activities' as defined in EU legislation concerning the facilitation of irregular entry. That personal data could only be used for risk analysis or for transmission to Europol or other EU law enforcement bodies. At that point, or at any rate within three months, the personal data would have to be deleted. The onward transmission of the data

[1201] Article 4, Reg. 2007/2004.
[1202] COM (2010) 61, 24 Feb. 2010.
[1203] Proposed amendment to Article 2(1)(c) of Reg. 2007/2004.
[1204] Proposed new Article 2(1)(h) and (i) of Reg. 2007/2004.
[1205] Proposed amendment to Article 4 of Reg. 2007/2004.
[1206] Article 11, Reg. 2007/2004.
[1207] Proposed amendment to Article 11 of Reg. 2007/2004.
[1208] EP's revised version of Article 4, in Council doc. 7961/11, 25 Mar. 2011.
[1209] Council's proposed new Articles 11b and 11c, in Council doc. 7961/11, 25 Mar. 2011.

to anyone else would be prohibited. In either case, the data processing would have to 'respect the principles of necessity and proportionality' and 'shall be strictly limited to' use for the relevant purposes. The EP's proposed amendments are broadly similar as regards the second type of processing of personal data but do not address the first type of processing.[1210]

As for the functioning and accountability of Frontex, a key institution is the Management Board, which appoints the Executive Director (proposed by the Commission) and adopts Frontex's annual general reports and work programmes.[1211] It is made up of one representative of each Member State and two representatives of the Commission.[1212] The Executive Director has the general power to manage Frontex and either the EP or the Council 'may invite' him or her 'to report on the carrying out of his/her tasks'.[1213] He or she has the general power to prepare the Agency's activities.

A particular parliamentary accountability gap regarding Frontex arises from the lack of detailed rules or arrangements on the reporting of Frontex operations. This includes (in future) the exchange of information by Frontex—and the important issue of the compatibility of Frontex actions with human rights obligations—in conjunction with the question of whether Frontex would be judicially accountable for its operational actions.

2.1.4 The EEAS

The EU's foreign policy intelligence unit, Sitcen, which was previously situated in the Council General Secretariat, was transferred to the EEAS in accordance with the Decision establishing the EEAS.[1214] There are no formal rules governing the establishment or operations of Sitcen. However, it is known that it is staffed by 'diplomats from the Policy Unit, secretariat personnel, and seconded intelligence analysts from the Member States' and works closely with the Intelligence Directorate of the EU Military Staff.[1215] It gathers information from open sources and compiles replies to requests for information sent out to national agencies, making its own assessments based on this information.

Sitcen is divided into three units: a Civilian intelligence Cell (CIC), which comprises civilian intelligence analysts working on political and counterterrorism assessment; a General Operations Unit (GOU), which provides operational support, research and non-intelligence analysis; and a Communications Unit (ComCen), which handles communications security issues and running the Council's communications centre. Since 2005, it has sought to develop an anti-terrorist capability.[1216]

2.1.5 The Standing Committee on Operational Security (COSI)

Article 71 TFEU, as inserted by the Treaty of Lisbon, provides for the creation of a standing committee on internal security (known as COSI) to 'facilitate coordination of the action of Member States' competent authorities'; representatives of the relevant EU bodies and

[1210] EP's proposed new Article 11aa, in Council doc. 7961/11, 25 Mar. 2011.
[1211] Article 20, Reg. 2007/2004.
[1212] Article 21, Reg. 2007/2004.
[1213] Article 26, Reg. 2007/2004. During the process to amend the founding legislation, the EP seeks to amend this provision to report 'in particular on the general report of the Agency for the previous year, the work programme for the coming year and the Agency's multi-annual plan.'
[1214] See the Annex to the EEAS Decision (OJ 2010 L 201/30).
[1215] See Fägersten 2008.
[1216] See *Hansard* (UK parliamentary reports), 27 June 2005, column 1249W.

agencies are involved in the proceedings of this committee. The EP and national Parliaments must be 'kept informed of the proceedings'.

This committee was established by a Council Decision adopted in 2010,[1217] which made it clear that COSI would not conduct operations but rather 'shall facilitate, promote and strengthen coordination of operational actions of the authorities of the Member States competent in the field of internal security' and 'shall also evaluate the general direction and efficiency of operational cooperation; it shall identify possible shortcomings or failures and adopt appropriate concrete recommendations to address them'. While COSI does not itself have an intelligence capability, it has an important role coordinating the operations of those bodies which do and should therefore be subject to sufficient oversight.

2.2 Major legal developments & impact of the TFEU

The EEAS was itself established recently pursuant to new provisions of the Treaties introduced by the Treaty of Lisbon thus its legal framework has not yet been amended. As for Frontex, the Treaty of Lisbon did not as such make amendments to its legal framework because Frontex was not (and still is not) specifically mentioned in the Treaties. However, as mentioned above, the legal framework of Frontex was amended in 2007 and will be amended further pursuant to the 2010 proposal to this end, which is likely to be agreed and adopted by summer 2011.

As for Eurojust and Europol, as mentioned above, the legal framework of Eurojust was altered by a Decision adopted in 2008. The original legal framework for Europol (a Convention adopted in 1995) was amended first by a series of Protocols (adopted in 2000, 2002 and 2003) and then by a Decision, adopted in 2009, which replaced the previous legal measures.

The framework relating to Europol and Eurojust was also altered by the Treaty of Lisbon, which amended the basic legal provisions in the Treaties that referred to these bodies. First of all, the previous legal provision relating to Eurojust (Article 31(2) TFEU) provided for the Council to 'encourage cooperation through Eurojust' by 'enabling' it to 'facilitate… coordination between… national prosecuting authorities', to promote its support for 'criminal investigations in cases of serious cross-border crime', taking account of Europol analyses, and to facilitate 'close cooperation between Eurojust and the European Judicial network'; for instance, to assist with executing letters rogatory and extradition requests.

Following the entry into force of the Treaty of Lisbon, Article 85 of the TFEU now provides that the agency's mission is 'to support and strengthen coordination and cooperation between national investigating and prosecuting authorities…, the basis of operations conducted and information supplied by the Member States' authorities and by Europol'. EU Regulations 'shall determine Eurojust's structure, operation, field of action and tasks, which 'may include' the 'initiation of criminal investigations' and proposals to national authorities to initiate prosecutions, the 'coordination of' such investigations and prosecutions and strengthening judicial cooperation, 'including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network'. However, 'formal acts of judicial procedure shall be carried out by the competent national officials' as regards the prosecutions concerned. Finally, the legislation establishing Eurojust must also 'determine arrangements for involving the European Parliament and national Parliaments in the evaluation of Eurojust's activities'.

[1217] OJ 2010 L 52/50.

As for Europol, the previous Article 30(2) of the TFEU stated that the Council had to 'promote cooperation through Europol' and had to adopt measures to: 'enable Europol to facilitate and support the preparation, and to encourage the coordination and carrying out, of specific investigative actions by the competent authorities of the Member States, including operational actions of joint teams comprising representatives of Europol in a support capacity' and to allow Europol 'to ask the competent authorities of the Member States to conduct and coordinate their investigations in specific cases and to develop specific expertise which may be put at the disposal of Member States to assist them in investigating cases of organised crime'. Article 88 of the TFEU now provides that Europol's mission is to 'support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime' and terrorism. As with Eurojust, EU Regulations will 'determine Europol's structure, operation, field of action and tasks', which may include 'the collection, storage, processing, analysis and exchange of information' and 'the coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States' competent authorities or in the context of joint investigative teams'. However, 'any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State or States whose territory is concerned' and 'coercive measures shall be the exclusive responsibility of the competent national authorities.' Finally, similarly to Eurojust, the EU legislation concerned must 'also lay down the procedures for scrutiny of Europol's activities by the European Parliament, together with national Parliaments'.

As compared to the previous Article 31(2) of the TFEU, Article 85 of the TFEU—the new legal base regarding measures concerning Eurojust—refers to the initiation of investigations and the proposal for initiation of prosecutions, as well as the resolution of conflicts of jurisdiction. It also refers specifically to the role of the EP and national parliaments, and provides for a reservation of national competence as regards 'formal acts of judicial procedure'. Furthermore, it is clear that the three tasks for Eurojust listed in Article 85(1) are not an exhaustive list of such tasks (see the words 'shall include'). However, the Treaty provisions concerning Eurojust can only take effect when the Eurojust Decision is amended or replaced by a Regulation, to be adopted pursuant to the ordinary legislative procedure. On this point, the Stockholm programme and the action plan on implementing the Stockholm programme call for a proposal on Eurojust in 2012.[1218]

As for Europol, compared to the previous Article 30(2) of the TFEU, there is an express exclusion from exercising 'coercive measures' and a requirement to act in liaison and agreement with each Member State as regards 'operational action'. More specifically, 'investigative and operational action' has to be carried out either 'jointly' with Member States or 'in the context of joint investigative teams'. The reference to specific rules concerning the EP and national parliamentary scrutiny of Europol is new.

Overall, Europol is no longer assigned a role supporting, facilitating and requesting action by national police forces but rather (implicitly) has a role in partnership with national forces. But the partnership is not fully equal since Europol cannot have the capacity to apply coercive measures. Moreover, the Treaty does not refer to any independent role for Europol to act fully by itself, although since the listed powers are non-exhaustive ('may include'), it would be possible to adopt rules to that effect—as long as Europol would not

[1218] See, respectively, OJ 2010 C 115 and COM (2010) 171, 20 Apr. 2010.

thereby carry out operational action independently, or exercise coercive powers, in light of the limits on its powers set out in Article 88(3).

For the future, the Commission plans to propose further legislation on Europol in 2013.[1219] Only at this point would the provisions on scrutiny by national parliaments and the EP referred to in Article 88 be invoked. In the meantime, the Commission has released a communication on this issue.[1220]

The different references to the role of the EP and national parliaments in Articles 85(1) and 88(2) of the TFEU (i.e., 'the *evaluation* of Eurojust's activities' as distinct from the '*scrutiny* of Europol's activities', emphasis added) are not explained in the *travaux* of the Convention, which drew up the text of the Constitutional Treaty. However, the difference might possibly be due to the principle that judicial bodies need more independence from political control.

As for Frontex, it can be presumed that the Treaty does not refer to similar oversight powers for the EP as regards Frontex simply because, as noted already, the Treaty does not explicitly refer to Frontex. This omission may be simply because when the Constitutional Treaty (the precursor to the Treaty of Lisbon) was originally drafted and signed in 2002–2004, Frontex was not yet established.[1221]

3. CLASSIFIED INFORMATION IN THE JUSTICE AND HOME AFFAIRS FIELD

The basic legal framework for accessing and processing classified information in the European Union is the security rules of the Commission and the Council.[1222] These sets of rules will soon be made rather more equivalent and they will also be accompanied by an agreement between Member States on the sharing of classified information within the framework of the EU. This is meant to 'constitute a more comprehensive and coherent general framework within the European Union for the protection of classified information originating in the Member States, in institutions of the European Union or in EU agencies, bodies or offices, or received from third States or international organisations.'[1223] There are also rules on the transfer of confidential information between the Commission and the EP in the EP/Commission framework agreement, which contains a specific Annex (Annex II) on this issue.[1224]

The standard classification of classified information within these rules is as follows: EU classified information (EUCI) is defined as 'any information and material, classified as "TRÈS SECRET UE/EU TOP SECRET", "SECRET UE", "CONFIDENTIEL UE" or "RESTREINT UE" or bearing equivalent national or international classification markings, an unauthorised disclosure of which could cause varying degrees of prejudice to Union interests, or to one or

[1219] COM (2010) 171, 20 Apr. 2010.
[1220] COM (2010) 776, 17 Dec. 2010.
[1221] Reg. 2007/2004 was adopted on 26 Oct. 2004 while the Treaty was signed on 29 Oct. 2004.
[1222] For the Council's rules, see OJ 2001, L 101/1. These rules will be replaced by Council doc. 6952/11, 28 Mar. 2011, online at: (http://www.statewatch.org/news/2011/mar/eu-council-security-rules-euci-6952-11.pdf). For a detailed study, see *Principles and procedures for dealing with European Union Classified Information in light of the Lisbon Treaty*, available at: (http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/pe425616_/pe425616_en.pdf).
[1223] See the declarations to be adopted when the new Council decision is adopted, in Council doc. 8054/11, 23 Mar. 2011, online at: (http://www.statewatch.org/news/2011/mar/eu-council-classified-information-8054-add1-11.pdf).The agreement by Member States is in Council doc. 13886/09, 6 Nov. 2009, online at: (http://www.statewatch.org/news/2011/mar/eu-euci-13886-09.pdf).
[1224] OJ 2010 L 304/1.

more Member States, whether such information originates within the Union or is received from Member States, third States or international organisations'.

The relevant categories are further defined as follows:

> (a) TRÈS SECRET UE/EU TOP SECRET: this classification shall be applied only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the Union or of one or more of its Member States.
> (b) SECRET UE: this classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of the Union or of one or more of its Member States.
> (c) CONFIDENTIEL UE: this classification shall be applied to information and material the unauthorised disclosure of which could harm the essential interests of the Union or of one or more of its Member States.
> (d) RESTREINT UE: this classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the Union or of one or more of its Member States.

Eurojust has been required to apply the Council security rules from 2009, following the adoption of the amendments to its founding Decision.[1225] The same is true of Europol, following the adoption of the 2009 Decision re-establishing that body.[1226] There are no specific rules on the sharing of classified information with the EP.

As for Frontex, a new provision in the proposed amendments to the founding Frontex Regulation would require Frontex to apply the Commission's security rules on classified information, as well as the Commission's security principles on non-classified sensitive information.[1227] There would be no special rule as regards the transfer of classified information to the EP, although this issue might be affected by the EP's amendments (discussed above) on the relationship between the Agency and the EP.

Finally, Article 10 of the EEAS decision provides that the High Representative will, inter alia, 'decide on the security rules for the EEAS', which will 'apply to all EEAS staff, and all staff in Union Delegations, regardless of their administrative status or origin'. Pending that decision, the EEAS had to apply the Council security rules as regards the protection of classified information, and the Commission's rules on 'other aspects of security'. It also has a 'department responsible for security matters', which is 'assisted by the relevant services of the Member States'. More generally, the High Representative has the power to 'take any measure necessary in order to implement security rules in the EEAS, in particular as regards the protection of classified information'. There is an inter-institutional agreement between the Council and the EP on the sharing of classified foreign policy and defence information[1228] but it does not apply to JHA matters.[1229]

[1225] Article 39a of the Decision, as inserted by the 2008 amendment.
[1226] Article 46 of the Decision.
[1227] Proposed new Article 11b of Reg. 2007/2004. This provision seems to be broadly acceptable to the Council and EP: see Art. 11d in Council doc. 7961/11, 25 Mar. 2011.
[1228] OJ 2002 C 298/1.
[1229] Point 6 in the preamble to the EEAS decision refers to the adoption of new rules on the issue but specifies that the 2002 agreement applies in the meantime. Point 4 of the High Representative's Declaration regarding the EEAS Decision (OJ 2010 C 210/1) specifies further: '[t]he HR can also provide access to other documents in the CFSP area on a need to know basis to other MEPs, who, for classified documents, are duly security cleared in accordance with applicable rules, where such access is required for the exercise of their institutional function on the request of the AFET Chair, and, if needed, the EP President. The HR will, in this context, review and where necessary propose to adjust the existing provisions on access for Members of European Parliament to classified

The concept of 'classified' information is not further defined in the relevant legislative texts, except as regards Europol, where the Decision includes a number of detailed rules to this effect.[1230] However, the cross-references to the Council and Commission rules presumably mean that the classification described above is applicable.

4. INFORMATION SHARING

In the case of Eurojust, the founding Decision has specific provisions on relations with the European Judicial Network, other EU bodies (Europol, OLAF, Frontex and the Council as regards foreign policy), and third States and bodies, including provisions on sending and receiving liaison officers and executing requests for judicial cooperation from third States.[1231] In practice, an agreement with Europol came into force in 2004 and was revised in 2009. A memorandum with OLAF was agreed in 2003, although the relationship with OLAF was considered unsatisfactory until a formal agreement was negotiated in 2008. Treaties with Norway, Iceland, Romania, the US, Croatia, Switzerland and several international bodies are in force,[1232] a treaty with the Former Yugoslav Republic of Macedonia has applied since 2010, and further treaties are planned with Russia, Ukraine, Moldova, other Western Balkan States, Liechtenstein, Cape Verde and Israel.

The Europol Decision sets out separate rules for information sharing with EU bodies, offices and agencies, third States and bodies, and private entities.[1233] In practice, Europol has: operational agreements with Australia, Canada, the US, Croatia, Iceland, Norway and Switzerland; strategic agreements with other Western Balkan States, Russia, Ukraine, Moldova and Colombia; operational agreements with Eurojust and Interpol; and strategic agreements with several EU bodies (including Frontex and Sitcen), as well as two UN bodies.[1234]

As for Frontex, Article 13 of the founding Regulation provides that it 'may cooperate with Europol' and other competent international organisations 'in the framework of working arrangements concluded with those bodies, in accordance with the relevant provisions of the Treaty and the provisions on the competence of those bodies'. Article 14 of that Regulation in turn provides that '[i]n matters covered by its activities and to the extent required for the fulfilment of its tasks', Frontex 'shall facilitate the operational cooperation between Member States and third countries, in the framework of the European Union external relations policy'. Again, it can do this by means of 'working arrangements' with the third countries concerned. At present, Frontex has arrangements with Western Balkan States, Russia, Ukraine, Belarus, Moldova, Georgia, the US, Canada and Cape Verde, along with the with the CIS Border Troop Commanders Council and the MARRI Regional Centre in the Western Balkans. It is negotiating arrangements with eight other States: Turkey, Libya, Morocco, Senegal, Mauritania, Egypt, Brazil and Nigeria. However, the texts of these

documents and information in the field of security and defence policy (2002 IIA ESDP). Pending this adjustment, the HR will decide on transitional measures that she deems necessary to grant duly designated and notified MEPs exercising an institutional function easier access to the above information.'

[1230] See Articles 22(2), 22(4), 23(2) to (8), 26(1)(b) and 41(4) of the Decision.

[1231] Articles 25a–27b of the Decision, as amended.

[1232] For the texts, see: (http://www.eurojust.europa.eu/official_documents/eju_agreements.htm).

[1233] Articles 22–26, Europol Decision. See also the Council decisions on the States which Europol can sign treaties with (OJ 2009 L 325/12) and on Europol's relations with external partners (OJ 2009 L 325/6).

[1234] For the treaties concerned, see: (http://www.europol.europa.eu/index.asp?page=agreements).

agreements are not online and little is known about their application in practice.[1235] There is an obvious accountability gap here, particularly from a human rights perspective.

The Commission's proposal to amend the founding Regulation would simply add references in Article 13 to the European Asylum Support Office and the EU's Fundamental Rights Agency. The Council's version of the proposal would specify that '[o]nward transmission or other communication of personal data processed by the Agency to other European Union agencies or bodies shall be subject to specific working agreements regarding the exchange of personal data and subject to the prior approval of the European Data Protection Supervisor'. The EP's version of the proposal would insert key provisions on accountability, requiring Frontex to inform the EP of such arrangements. It would also permit Frontex to invite other EU bodies and international organisations to participate in certain Frontex activities, including risk assessment, subject (in most cases) to the consent of the Member States concerned.

The Commission's proposals to amend Article 14 of the Regulation (as regards cooperation with third States) are more far reaching. They would first specify that such cooperation must take place 'in the framework of the European Union external relations policy, including with regard to human rights.' The EP version would add a specific reference to the European Neighbourhood Policy, would specify that no operation could take place 'under the jurisdiction of any third country', and would note that cooperation with third countries would have to 'promote European border management standards, also covering respect for fundamental rights and human dignity'.

Next, the proposal would permit Frontex to send liaison officers to third States, but only where 'border management practices respect minimum human rights standards', with priority for third States 'which on the basis of risk analysis constitute a country of origin or transit regarding illegal migration'. Frontex could also receive liaison officers posted by those States. The Frontex Management Board would adopt an annual list of priorities to this end. Furthermore, Member States would also have to include in their bilateral treaties with third States, 'where appropriate', 'provisions concerning the role and competencies of the Agency'. The Council's version of the proposal would make this provision optional for Member States, while the EP's version would require Frontex to inform the EP about such treaties, and about the deployment of liaison officers and its arrangements with third States. Finally, the Commission's original proposal would require the Commission's consent for Frontex's deployment of liaison officers and its arrangements with third States. The Council's version would delete this requirement. In the Council's version, Frontex's external relations would not as such be accountable to anyone, other than in the general context of Frontex accountability.

A significant development in the near future will be the likely development of an EU Terrorist Finance Tracking Programme (TFTP) to parallel the established US system, which is regulated by an EU/US agreement.[1236] The Commission is due to make proposals to this end by summer 2011. Questions will inevitably arise about the architecture of sharing the financial information concerned, along with further related information concerning terrorist operations, as between EU bodies and national law enforcement and intelligence agencies, and important data protection issues will also have to be addressed.

[1235] For instance, Frontex's 2009 annual report contains a one-page summary of external relations with third States.
[1236] OJ 2010 L 195.

5. FUTURE POWERS

As we have seen, the roles of Europol and Eurojust have yet to be developed pursuant to the Stockholm programme following the entry into force of the Treaty of Lisbon, and the proposed amendments to the Frontex legislation have yet to be agreed. However, the EEAS is now operational, including Sitcen and the amendments to the Frontex legislation will likely be agreed shortly and will certainly develop Frontex's intelligence role. Similar developments are likely in the foreseeable future as regards Europol and Eurojust.

The particular concerns that could arise with Frontex relate to the use of personal information for risk analysis, and the possible transfer and subsequent use of that information by national agencies. To what extent could inaccurate or misleading information about a particular individual be used without an adequate remedy in place? While the legislation establishing the EU's JHA databases contains systematic rules governing the exchange and processing of personal data, the more informal process envisaged by the proposed amendments to the Frontex legislation is not so detailed. It is therefore important to ensure that the mechanisms for accountability of Frontex to the EP include a focus on this particular issue, inter alia.

As for the EEAS, it is notable that the TFEU (as revised by the Lisbon Treaty) contains a specific rule on the processing of personal data by Member States within the framework of EU foreign policy (Article 39 of the TFEU):

> In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

No such measure has yet to be adopted. However, this exception only applies to Member States and Article 11(3) of the EEAS Decision specifies that '[t]he EEAS shall protect individuals with regard to the processing of their personal data in accordance with the rules laid down' in EU legislation, and that '[t]he High Representative shall decide on the implementing rules for the EEAS'. It remains to be seen what specific implementing rules are adopted. Nonetheless, the problem still remains that there is no specific mechanism in the EEAS Decision as regards the accountability of the EEAS intelligence capability to the EP. More generally, there is little information available concerning the functioning of Sitcen and, as noted above, there are no formal rules concerning its establishment.[1237] This omission necessarily hinders its accountability.

6. CONCLUSION

The EU is lacking a systematic framework governing the parliamentary oversight of intelligence activity. In particular, there are significant gaps in EP (and national parliamentary) access to classified information held by Europol and Eurojust, and such access as regards JHA documents held by the Council. The agreements concerning access

[1237] The Situation Centre is referred to in passing in the Decisions establishing the Political and Security Committee (OJ 2001 L 27/1) and the Military Staff (OJ 2001 L 27/7).

to classified information between the EP and the Commission, and between the EP and the Council on foreign policy documents, do not apply to national parliaments, although the latter agreement will shortly be replaced by arrangements on EEAS documents. In order to ensure accountability of the relevant EU bodies, these gaps have to be filled.

The EP is also lacking a systematic internal framework for the oversight of classified information. A key issue here is whether this framework should be developed by the EP autonomously, or whether it should be developed in conjunction with national parliaments collectively, given the latter's explicit role as regards oversight of Europol, Eurojust and COSI as set out in the Treaties. An alternative approach would be to devise two (perhaps similar) systems for oversight: an autonomous system for the EP alone where the Treaties do not require national parliaments' involvement (for example, Frontex and the EEAS), and a specific system regarding Europol, Eurojust and COSI where the Treaties do require such involvement. This suggestion begs the question, however, of whether the EP should seek to involve national parliaments in oversight activities even in cases where the Treaties do not require it.

In either case, the EP (with or without national parliaments) needs to adopt internal rules governing the sharing and analysis of this information in order to ensure that its access to this information can contribute to its assessment of EU policies and can be evaluated in the context of guaranteeing the accountability of the relevant bodies.

A particular topic for the EP (and national parliaments) to focus on is the potential overlap between EU bodies in general and with regard to particular areas of crime or incidents (certain terrorist attacks, for instance). Does this entail a duplication of resources or a useful synergy?

Finally, while examining the accountability of EU action in this area, parliaments will have to draw a distinction between the operation of the EU bodies generally (i.e., the effectiveness of their organisation and management) and supervision of individual operations, given the confidentiality issues that arise.

REFERENCES

Fägersten B. (2008), *European Intelligence Cooperation: Drivers, Interests and Institutions*, SIIA Papers No 6.

Hertzberger E. (2007), *Counter-Terrorist Intelligence cooperation in the EU*, UNICRI.

Hinarejos A. (2009), 'The Lisbon Treaty versus Standing Still: A View from the Third Pillar', 5 EUConst, 299.

House of Lords European Scrutiny Committee (2007–2008a), *EUROPOL: Coordinating the fight against serious and organised crime*, 29th report.

House of Lords European Scrutiny Committee (2007–2008b), *FRONTEX: the EU external borders agency*, 9th report.

Ladenburger C. (2008), 'Police and Criminal Law in the Treaty of Lisbon: A New Dimension for the Community Method', 4 EUConst, 20.

Mitsilegas V. (2009), *EU Criminal Law*, Hart Publishing, Oxford.

Müller-Wille B. (2004), *For our eyes only? Shaping an intelligence community within the EU*, WEU Security Studies Institute.

Peers S. (2005), 'Governance and the Third Pillar: The Accountability of Europol' in D. Curtin and R. Wessel, eds., *Good Governance and the European Union*, Intersentia.

Peers S. and N. Rogers (2006), *EU Immigration and Asylum Law: Text and Commentary*, 1st edition, Martinus Nijhoff.

Rijken C. (2001), 'Legal and Technical Aspects of Cooperation Between Europol, Third States and Interpol' in V. Kronenberger, ed., *The European Union and the International Legal Order: Discord or Harmony?*, Asser.

ANNEX C: QUESTIONNAIRE FOR OVERSIGHT INSTITUTIONS OF CIVILIAN SECURITY AND INTELLIGENCE AGENCIES IN EU MEMBER STATES

Methodological Note:

The questionnaire drafted by DCAF-EUI was addressed to all national parliaments in the European Union member states and, where applicable, specialised non-parliamentary oversight committees. The questionnaire aimed to gather more information from these entities on the oversight of security and intelligence agencies. From the information provided by the EU member states, common standards and good practices were identified.

The questionnaire was set up in two parts. The first part concerned parliaments as a whole. The second part related to specialised parliamentary committee(s) or, where applicable, specialised non-parliamentary oversight committees which are responsible for overseeing security and intelligence agencies.

Out of 27 Member States of the European Union, 13 have a bicameral parliament and 14 have a unicameral parliament. In total there are 40 national parliamentary chambers in the 27 Member States of the European Union.

While the national parliaments of Austria, Belgium, Czech Republic, France, Germany, Ireland, Italy, the Netherlands, and Romania have a bicameral system, they each sent a single set of responses to the questionnaire. This was done because in some member states the oversight of security and intelligence agencies is exercised by a Joint Committee, in which members of both Chambers are represented. This is the case in Italy, Romania, and the United Kingdom. Furthermore, in some member states one of the two Chambers has a paramount role in overseeing security and intelligence agencies, for instance the German *Bundestag,* Belgian *Senaat,* Dutch *Tweede Kamer,* Czech *Poslanecká sněmovna (Chamber of Deputies),* and the French *Assemblée Nationale*.

DCAF-EUI received responses from 28 national parliaments or chambers to the first part of the questionnaire, and 28 responses to the second part from specialised parliamentary committees and/or specialised non-parliamentary committees responsible for overseeing security and intelligence agencies.

QUESTIONNAIRE FOR OVERSIGHT INSTITUTIONS OF CIVILIAN SECURITY AND INTELLIGENCE AGENCIES IN EU MEMBER STATES

INTRODUCTION

This questionnaire forms part of a comparative study on the oversight of civilian security and intelligence agencies and relevant activities in all European Union member states and other major democracies. The study was commissioned by the European Parliament (DG Internal Policy) and is being undertaken jointly by the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the European University Institute (EUI);1238 it will be published by the European Parliament.

The study will examine the oversight of security and intelligence agencies at the national level with the aim of identifying models and practices that can inform the European Parliament's (EP's) approach to the establishment of parliamentary oversight of EU's internal security agencies, i.e. EUROPOL, EUROJUST, FRONTEX, and some intelligence components of the European External Action Service. The Lisbon Treaty has given the European Parliament a mandate to strengthen parliamentary oversight of these EU agencies – this study should be seen within this context.

This questionnaire aims to gather more information on common standards and good practices relating to the oversight of security and intelligence agencies by parliaments, as well as specialised institutions outside parliament. The European Parliament is particularly interested in the division of responsibilities for overseeing security and intelligence agencies; national parliaments' access to classified information in the security field; and the mandates, functioning and powers of specialized oversight committees both within parliament and outside. The questionnaire provides an opportunity for EU member states to demonstrate how security and intelligence agencies are overseen in their state, and thus to provide examples which will inform the European Parliament in strengthening its oversight of EU security agencies.

[1238] DCAF is an international foundation specialising in security sector governance and reform ; it is based in Geneva, Switzerland. The EUI is an international postgraduate and post-doctoral teaching and research institute established by European Union member states. It specialises in the fields of Economics, Law, History and Civilization, and the Political and Social Sciences. The EUI is based in Florence, Italy.

TERMINOLOGY

For the purposes of this questionnaire, "security and intelligence agencies" are broadly defined to include all civilian government agencies which perform any of the following activities in the area of national security: handling and processing of classified information; information sharing domestically and with foreign entities; processing and use of personal data; collection of information covertly and from open sources. We are primarily interested in domestic intelligence agencies, security police, special branch police services, border security services and joint analysis/fusion centers. The term "committee" is used throughout the questionnaire to denote the overseer(s) of security and intelligence agencies, whether they be parliamentary, or non-parliamentary entities.

STRUCTURE

PART I: QUESTIONS FOR NATIONAL PARLIAMENTS ON THE OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES

Section A: General questions on the oversight of security and intelligence agencies

Section B: Parliament and access to classified information in the area of national security

Section C: Managing Classified Information

PART II: QUESTIONS FOR SPECIALISED COMMITTEES RESPONSIBLE FOR OVERSEEING SECURITY AND INTELLIGENCE AGENCIES

Section A: Organisational Structure

Section B: Legal basis and Mandate

Section C: Investigations & Powers

Section D: Access to Classified Information

Section E: Protecting Classified Information

Section F: Reporting and Follow-Up

Section G: Challenges and Strengthening Oversight

INSTRUCTIONS

This questionnaire contains 43 questions.

Part I of this questionnaire is addressed to parliaments as a whole. It should take 20 minutes to complete

Part II should be answered by the parliamentary committee(s) or (where applicable) the specialised institution(s) outside parliament that are responsible for overseeing security and intelligence agencies in your state. This part may be completed by more than one committee if required. These questions should take approximately 30 minutes to complete.

If the main institution responsible for overseeing security and intelligence agencies is outside parliament, please complete Part I and then kindly provide us with the contact details of this institution, we will ask them to complete the questions in part two.

We kindly request that you write your answers to the open questions in English in the space provided or attach an additional sheet of paper if necessary.

PART I: QUESTIONS FOR NATIONAL PARLIAMENTS ON THE OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES

Your contact details:

Name: _____

Organisation: _____

Function: _____

Email: _____

Telephone: _____

(This information will only be used to contact you in case we have questions about your responses; the results of the survey will be processed anonymously)

Section A: General questions on the oversight of security and intelligence agencies

1. Which committee(s) of parliament and/or institutions outside of parliament oversee the following aspects of the security and intelligence agencies?

Please write the name (in the original language and in English) of the relevant committee(s) in each box. For parliamentary committees please indicate if it belongs to one chamber of parliament or is a joint committee. If the responsible oversight body differs depending on the security agency being overseen, please indicate this.

	Parliamentary committee(s)	**Institutions/committees outside parliament**
Budget & Expenditure		
Administration & Management		

Compliance with the law		
Policies		
Operations (future, ongoing and completed) *Delete as appropriate*		
Security agencies' relations with foreign governments and international organisations		
Complaints about the agencies		

2. Does parliament play a role in appointing senior staff of security and intelligence agencies?

□ No

□ Yes (please explain):_____

_____

_____

3. Does parliament play any of the following roles vis-à-vis external institutions which oversee security and intelligence agencies (such as information commissioners, ombudsman institutions, specialised intelligence oversight institutions)?

Please tick all boxes that apply

□ Appointing members

□ Approving budget

□ Requesting investigations or reports on given matters

□ Receiving and scrutinising reports

□ Other (please specify):_____

_____

Section B: Parliament and access to classified information in the area of national security

4. Please indicate the extent of parliament's access to the following four levels of classified information in the field of national security:

For each level of classified information, please select only one of the three options provided

a) Information classified as "Top Secret"

□ All members of parliament have access to all relevant information

□ Access is limited to one or more of the following categories of MPs *(please tick all which apply)*

□ Access is limited to the chairs of particular committees

(please specify): _____

□ Access is limited to members of particular committees

(please specify): _____

□ Access is limited party or group leaders in parliament

□ Access is limited to the president/speaker of parliament

□ Access is limited to ad hoc parliamentary committees inquiry

□ No members of parliament have access

b) Information classified as "Secret"

□ All members of parliament have access to all relevant information

□ Access is limited to one or more of the following categories of MPs (please tick all which apply)

□ Access is limited to the chairs of particular committees

(please specify): _____

□ Access is limited to members of particular committees

(please specify): _____

□ Access is limited party or group leaders in parliament

□ Access is limited to the president/speaker of parliament

□ Access is limited to ad hoc parliamentary committees inquiry

□ No members of parliament have access

c) Information classified as "Confidential"

□ All members of parliament have access to all relevant information

□ Access is limited to one or more of the following categories of MPs (please tick all which apply)

□ Access is limited to the chairs of particular committees

(please specify): _____

□ Access is limited to members of particular committees

(please specify): _____

□ Access is limited party or group leaders in parliament

□ Access is limited to the president/speaker of parliament

□ Access is limited to ad hoc parliamentary committees inquiry

□ No members of parliament have access

d) Information classified as "Restricted"

□ All members of parliament have access to all relevant information

□ Access is limited to one or more of the following categories of MPs (please tick all which apply)

□ Access is limited to the chairs of particular committees

(please specify): _____

□ Access is limited to members of particular committees

(please specify): _____

□ Access is limited party or group leaders in parliament

□ Access is limited to the president/speaker of parliament

□ Access is limited to ad hoc parliamentary committees inquiry

□ No members of parliament have access

5. Which of the following types of frequently classified information can be accessed by the categories of MPs indicated in your responses to question 4?

Please check all that apply

□ Information on ongoing operations of security and intelligence agencies

□ Information on past operations of security and intelligence agencies

□ Budgets for future spending by security and intelligence agencies

□ Information on past expenditure by security and intelligence agencies

□ Internal guidelines of security and intelligence agencies

□ Information shared domestically between security and intelligence agencies

□ Information shared between security and intelligence agencies and foreign governments and international organizations

□ Information on negotiations between the executive and foreign governments and international organisations in the area of internal and external security (e.g. the Passenger Name Records Agreement with the USA)

☐ International agreements between security /intelligence agencies and foreign entities

☐ Other (please specify): _____

_____

_____

6. Does your state's access to information or information security legislation make a distinction between parliament as an institution, MPs and the general public in terms of access to information?

☐ No

☐ Yes (please explain):_____

_____

_____

_____

7. Can the government and/or the security and intelligence agencies lawfully deny access to classified information which MPs could normally access in accordance with the terms you outlined in question 4?

☐ Yes ☐ No (go to question 9)

(b) If yes, on what grounds can access to classified information be denied?

_____

_____

_____

_____

_____

(c) Who can take the decision to deny access to classified information?

_____

_____

_____

8. Do any procedures exist for parliament to challenge a refusal to grant relevant MPs access to classified information?

☐ No

□ Yes (*Please explain)*

_____
_____
_____
_____

9. (a) Do staffers employed by parliament have access to classified information in the field of national security?

□ Yes □ No

(b) Do staffers employed by MPs/political parties have access to classified information in the field of national security?

□ Yes □ No

Section C: Managing Classified Information

10. (a) Are members of parliament vetted/required to obtain a security clearance before being granted access to classified information?

□ Yes □ No

(b) Are parliamentary staffers vetted/required to obtain a security clearance before being granted access to classified information?

□ Yes □ No

(c) If yes, who administers security clearances?

_____

(d). Which institution takes the final decision on whether security clearance is granted?

_____

_____

11. Are members of parliament required to sign a confidentiality agreement before being given access to classified information?

☐ Yes ☐ No

12. What action can be taken against members of parliament who make unauthorised disclosures of classified information?

☐ Criminal prosecution

☐ Disciplinary action according to parliament's internal procedures

☐ Other (please explain):_____

_____

_____

13. By which of the following means are members of parliament able to access to classified information?

(Please tick all boxes which apply)

☐ Information can be viewed in a secure reading room in parliament

☐ Information can be viewed on the premises of the executive

☐ Information can be viewed on the premises of the security and intelligence agencies

☐ Information can be viewed on secure computer system in parliament

☐ Information can be viewed in the context of committee meetings

☐ Other (please explain):_____

_____

_____

_____

PART II: QUESTIONS FOR SPECIALISED COMMITTEES RESPONSIBLE FOR OVERSEEING SECURITY AND INTELLIGENCE AGENCIES

Your contact details:

Name: _____

Organisation: _____

Function: _____

Email: _____

Telephone: _____

(This information will only be used to contact you in case we have questions about your responses; the results of the survey will be processed anonymously)

NAME OF COMMITTEE:_____

_____

_____

Section A: Organisational Structure

14. Which of the following models best describes your committee?

☐ A parliamentary committee

☐ An oversight body which is independent of parliament, the executive and the agencies that it oversees

☐ Other (*please specify*) _____

_____

_____

15. How many members and staffers does your institution have?

Members _____ **Staffers**_____

16. Who appoints the members of your committee?

(Please tick one box, or indicate if a combination of these actors is involved)

☐ The head of government/state

☐ The minister(s) responsible for the security and/or intelligence agencies

☐ Parliament

☐ Other (*please specify*):_____

_____

_____

17. Do any of the following rules apply to membership of your committee?

☐ Proportional representation

☐ Guaranteed representation of opposition or minority parties

☐ A requirement that members are not parliamentarians

☐ A requirement that members are not members of political parties

☐ A requirement that members are not current/former members of the intelligence/security agencies

☐ A requirement that members are members of the legal profession

☐ A requirement that the committee is chaired by a member of an opposition party

☐ Other *(please specify)*_____

_____

_____

18. (a) What is your approximate annual budget?

€_____

(b) Which body allocates the budget for your committee?

_____

Section B: Legal basis and Mandate

19. What is the legal basis for your committee?

(Please select one or more of the following options and list the relevant document(s))

☐ Constitution

☐ Statute:_____

☐ Executive decree:_____

☐ Ministerial directive:_____

☐ Parliamentary rules of procedure: _____

☐ Other (*please specify*):_____

20. Which security/intelligence agencies does your committee oversee?

(Please provide the names of these institutions)

_____
_____
_____
_____

21. Does your committee oversee the work of any joint analysis or fusion centre?

☐ Yes ☐ No

Please specify which bodies these are:_____
_____
_____

22. (a) Is your committee mandated to address complaints about security/intelligence agencies from members of the public?

☐ Yes ☐ No

(b) If no, which institution is responsible for this?_____

23. (a) Which of the following areas of the intelligence/security agencies' activities does your committee oversee?

Please select all that apply

☐ The policies of the agencies

☐ Completed operations/investigations of the agencies

☐ Ongoing operations/investigations of the agencies

☐ The administration and management of the agencies

☐ The budgets and expenditure of the agencies

☐ Other _____

_____

_____

(b). Which of the following criteria are used when overseeing the matters referred to in 23 (a)?

Please select all that apply

☐ Effectiveness

☐ Efficiency

☐ Compliance with national law

☐ Compliance with international law

☐ Other _____

_____

_____

24. Which of the following specific activities of the security/intelligence agencies does your committee oversee, and how does the committee oversee these activities?

Please tick all boxes which apply; if you do not oversee a particular function leave the box blank. For each of the activities you oversee please briefly explain this is done. For example, your committee may examine these activities through random sampling of information held by security agencies, by investigating complaints made about agencies, or by examining reports produced by the agencies.

□ Collection of information using special powers (such as the interception of communications)

□ Collection of information from open sources

□ Use of personal data (including the processing, storage, deletion and transfer of personal data)

□ Sharing of information between agencies on a domestic level (e.g. between security services and the police)

□ Sharing of information with foreign entities

□ Information sharing and cooperation agreements/memoranda of understanding signed with foreign governments and agencies

□ Analysis of information and production of reports (e.g. intelligence or threat estimates for policy-makers)

_____
_____
_____

□ Appointments of senior staff

_____
_____
_____

□ Appointments of agencies' oversight bodies within security and intelligence agencies (e.g. inspectors general within security agencies)

_____
_____
_____

□ Other_____
_____

Section C: Investigations & Powers

25. What can trigger an investigation by your committee into the activities of intelligence/security agencies?

Please select all options which apply

□ A decision by the committee itself (e.g. an own initiative investigation)

□ A request from the plenary of parliament

□ A request from the minister(s) responsible for security and/or intelligence agencies

□ A request from the head of state/government

□ A request from the judiciary

□ Complaints raised by members of the public

□ A request from the intelligence/security agencies themselves

□ Other (*please specify)*_____

_____

26. Which of the following powers or methods are available to your committee?

□ Periodic meetings with senior management of agencies (e.g. annual meetings)

□ Right to invite senior management to give testimony at other times

□ Right to receive and review annual reports of agencies

□ Right to invite external experts (e.g. academics) and members of civil society to give testimony

□ Right to invite members of the public the give testimony

Subpoena powers

- □ Subpoena intelligence/security officers to testify under oath before committee
- □ Subpoena members of the executive branch to testify under oath before committee
- □ Subpoena intelligence/security agencies to provide documents or other forms of evidence

□ Right to inspect the premises of intelligence/security agencies

□ Other (please specify):_____

_____

_____

Section D: Access to Classified Information

27. Do members/staffers of your committee have access to classified information?

Members

□ Yes □ No

Staffers

□ Yes □ No

28. Please indicate whether your committee has unlimited, restricted or no access to the categories of information listed in the table below.

Please check one box for each type of information and explain any restrictions

Type of information	**Unlimited Access**	**No Access**	**Restricted Access (please briefly explain restrictions)**
Security agencies' files and databases			
Information about future operations			
Information about ongoing operations			
Information about completed operations			
Internal regulations or guidelines			

Ministerial instructions/directives issued to the security & intelligence agencies			
Information on the budget and the projected expenditure of agencies			
Information on past expenditure			
Agreements with foreign governments, agencies, and international organisations			
Information received from other domestic agencies			
Information received from			

foreign governments and security agencies			
Information received from international organizations (e.g. the UN, EU or NATO)			
Other (*please specify*)			

29. (a) Are the intelligence/security agencies or the government legally entitled to refuse requests for information from your committee?

☐ Yes ☐ No

(b) Who can take the decision to refuse to provide the information to your committee?

☐ The minister(s) responsible for the security and/or intelligence agencies

☐ The head of state/government

☐ The head of the intelligence/security agencies

☐ Other *(please specify)*_____

_____

30. (a) Does a decision to deny the committee access to information need to be justified?

☐ No ☐ Yes

(b) If yes, which of the following justifications can be used to deny access to requests for information?

Please tick all boxes which apply

☐ The requested information relates to ongoing operations

☐ Disclosing the information to an oversight institution could jeopardize national security

☐ Disclosure of the information could reveal sources and methods used by intelligence/security agencies

☐ The requested information was provided by a third party (e.g. another state or international organisation)

☐ Disclosure would violate the privacy of individuals concerned

☐ Other (please explain)_____

_____

31. In the event that a request for information is denied, are there any procedures for challenging the decision taken by the executive and/or the intelligence/security agencies?

☐ No

☐ Yes *Please explain*_____

_____

_____

_____

32. What are the most significant restrictions on your committee's access to information and what impact, if any, do they have on your work?

_____

_____

_____

_____

_____

Section E: Protecting Classified Information

33. (a). Are members and staffers of your committee required to obtain security clearance and/or required to sign a non-disclosure agreement?

(*Select all that apply)*

Members

□ Security Clearance

□ Non-disclosure agreement

Staffers

□ Security Clearance

□ Non-disclosure agreement

34. Which of the following measures are used to protect classified information?

□ Meetings are held behind closed doors

□ Members and staffers are only permitted to access classified information on the premises of the intelligence and security agencies.

□ Secure reading room for committee members and staffers to view documents

□ Secure computer system for committee members and staffers

□ Other(s):_____

_____

_____

_____

35. What action can be taken against members/staffers of your committee who make unauthorized disclosures of classified information?

_____

_____

_____

Section F: Reporting and Follow-Up

36. Is your institution empowered to issue:

(*Please check all that apply)*

☐ Binding orders

☐ Recommendations

☐ Draft legislation or statutory amendments

☐ Other *(please indicate)*_____

_____

_____

37. Who does your committee report to?

(*If your institution reports to more than one body please indicate the principal one)*

☐ Head of state/government

☐ Parliament

☐ The minister(s) responsible for the security and/or intelligence agencies

☐ The intelligence/security agencies

☐ Complainants

☐ Other: (*please specify)*_____

38. Are your reports made public?

i). Periodic reports

☐ Yes

☐No

☐ Sometimes (*please explain*) _____

_____

ii). Reports on specific activities or events

□ Yes

□No

□ Sometimes (*please explain*) _____

_____

39. Are the institution's reports vetted and/or redacted by another institution before they are made public?

□ Yes □ No

If yes, which institution(s)?_____

40. Does your committee monitor the implementation of its recommendations?

□ Yes. □ No.

If yes, how is this done? _____

_____

_____

41. What action, if any, can you take if the intelligence/security agencies or the government fail to implement your order and/or recommendations:

(Please tick all boxes which apply)

□ Report non-implementation to parliament

□ Report non-implementation to the responsible minister(s)

□ Publicise a failure to implement recommendations

□ Seek to reduce an agency's budget in subsequent years

□ Seek a court order compelling compliance

□ Other (*please specify)*:_____

_____ _____

_____

Section G: Challenges and Strengthening Oversight

42. Please briefly outline two or three changes to your institution and/or its mandate which would strengthen its capacity to perform its functions.

1.

2.

3.

43. Please identify two or three strengths of your committee.

1.

2.

3.

Additional comments

Please feel free to add any additional comments which you deem to be relevant.

THANK YOU VERY MUCH FOR TAKING THE TIME TO COMPLETE THIS QUESTIONNAIRE

ANNEX D: MEMBERS OF THE PROJECT ADVISORY BOARD

Steven Aftergood is Project Director at the Federation of American Scientists, USA.

Monica den Boer is Academic Dean at the Police Academy of the Netherlands and Professor of Comparative Public Administration at the VU University of Amsterdam.

Iain Cameron is Professor of Public International Law at Uppsala University, Sweden.

Deirdre Curtin is Professor of European Law at the University of Amsterdam and Director of the Amsterdam Centre for European Law and Governance.

Peter De Smet is a member of the Belgian Standing Intelligence Agencies Review Committee.

Philippe Hayez is Adjunct Professor of Intelligence Policy at the Paris School of International Affairs (PSIA), Sciences Po, Paris.

Helga Hernes is the former Chair of the Norwegian Parliamentary Intelligence Oversight Committee (EOS-Utvalget) and is a Senior Advisor at the International Peace Research Institute (PRIO), Oslo.

A. H. (Bert) van Delden is Chair of the Review Committee for the Intelligence and Security Services, the Netherlands.

ANNEX E: AUTHORS OF THE ANNEXED BACKGROUND STUDIES

Iain Cameron is Professor of Public International Law at Uppsala University, Sweden.

Alexandra De Moor is Academic Assistant of Criminal Law and Internal member of the Institute for International Research on Criminal Policy (IRCP) at Ghent University, Belgium.

Hans De With is Chairman of the G 10 Commission of the German Bundestag.

Bruno De Witte is Professor of European law at Maastricht University, and part-time Professor at the Robert Schuman Centre of the European University Institute.

Federico Fabbrini is a PhD researcher in the Law Department at the European University Institute, Italy.

Gábor Földvary is Head of the Office of the State Secretary for Parliamentary Affairs of Defence, Hungary.

Craig Forcese is Vice Dean and Associate Professor in the Faculty of Law (Common Law Section) at the University of Ottawa, Canada.

Tommaso F. Giupponi is Professor of Constitutional Law at the Faculty of Law, University of Bologna, Italy.

Jorrit J. Rijpma is Assistant Professor of EU Law at the *Europa Instituut* of Leiden University.

Erhard Kathmann is Ministerial Counselor in the Administration of the German Bundestag.

Ian Leigh is Professor at the School of Law, Durham University, UK.

Charlotte Lepri is a Research Fellow at the *Institute de Relations Internationales et Stratégiques* (IRIS), France.

Kate Martin is Director of the Center for National Security Studies, Washington DC, USA.

Nicola McGarrity is a Lecturer and Director of the Terrorism and Law Project at the Gilbert + Tobin Centre of Public Law at the University of New South Wales, Sydney, Australia.

Steve Peers is Professor at the School of Law, University of Essex, UK.

Susana Sanchez Ferro is Lecturer in Constitutional Law, Universidad Autónoma de Madrid, Spain.

Wauter Van Laethem is Legal Advisor to the Belgian Standing Committee I on intelligence.

Nick Verhoeven is the Secretary of the Intelligence and Security Services Review Committee (CTIVD) in the Netherlands.

Gert Vermeulen is Professor of Criminal law and Director of the Institute for International Research on Criminal Policy (IRCP) at Ghent University, Belgium.

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

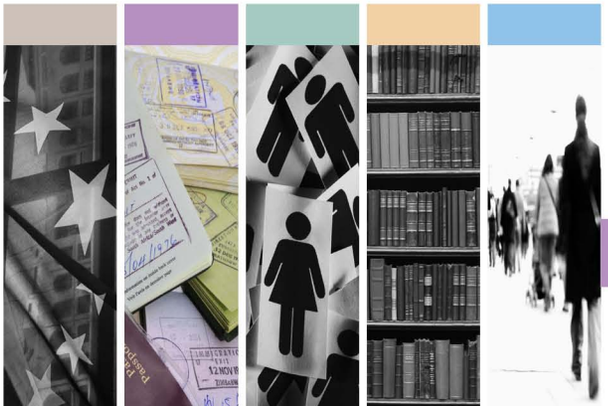
Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

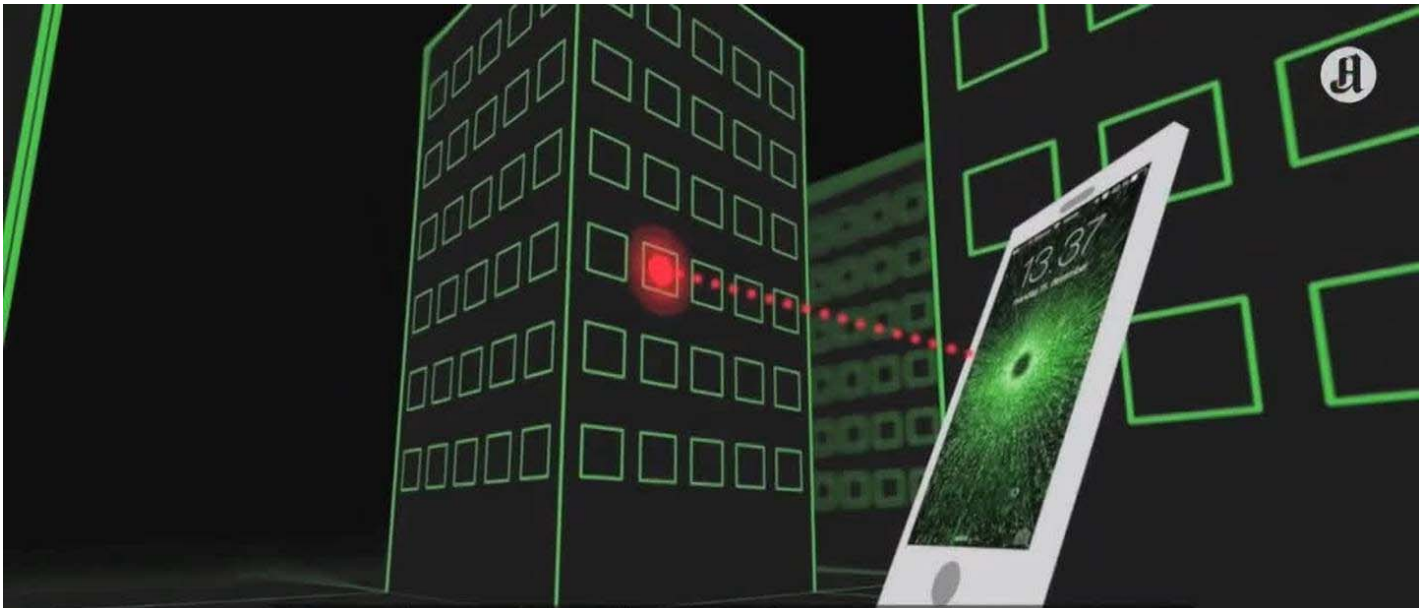


PARLIAMENTARY OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE EUROPEAN UNION

Secret surveillance of Norway's leaders detected

ANDREAS BAKKE FOSS | PER ANDERS JOHANSEN | FREDRIK HAGER-THORESEN

OPPDATERT: 16.DES. 2014 14:53 | PUBLISERT: 13.DES. 2014 13:29



This is how Aftenposten revealed the secret surveillance in Oslo

Members of parliament and the prime minister of Norway are being monitored by means of secret espionage equipment.

Norway's major secrets are being administered here, right in the centre of Oslo. A number of the most important state institutions are

situated within a radius of one kilometer: The Prime minister's office, the Ministry of defence, Stortinget (parliamen Norges Bank. Ministe of parliament, state of and other essential st nation's security, our totalling more than 6 working within this ar

The norwegian parliament - Stortinget - is situated in the centre of Oslo.
Monica Strømdahl

But passers-by are hardly aware of the following fact: In several locations someone has installed secret transmitters which most probably behave like fake mobile base stations. These so called IMSI-catchers can monitor all mobile activity in the vicinity.

The people who run this surveillance equipment may in principle monitor every person moving in and out of the parliament building, the goverment offices or other institutions in the area. They can

also select certain persons for eavesdropping and collecting data from their smartphones.

Aftenposten's mapping

This newspaper has undertaken the first ever tracking of active mobile surveillance equipment in Oslo. The measurements reveal that secret, fake base stations, so-called IMSI-catchers, are being operated in the immediate vicinity of several important buildings in the capital:

Around Stortinget:

- One in the area Lille Grensen between Karl Johans gate and Akersgata
- One in Nedre Vollgate

In Kvadraturen:

- One in the intersection Rådhusgata - Skippergata
- One in the area at Akershusstranda.

In Parkveien:

- On near the intersection Parkveien - Henrik Ibsens gate, close to the American embassy.
- One in the intersection Parkveien - Hegdehaugsveien

The fake base stations were active as late as last

Thursday.

A great number of findings

By means of one of the world's most advanced encrypted cell phones – the German-made CryptoPhone 500 – Aftenposten's journalists have - during two months this fall - monitored and disclosed a number of locations in the city with suspicious mobile activity. (See separate article on the methods we used below). Then we cooperated with the two security companies Aeger Group and CEPIA Technologies, both of which have very precise measuring equipment for locating fake base stations. During the past two weeks they made a number of measurements which indicate that the surveillance equipment «with a very high degree of probability» are being used actively in the centre of Oslo.

- If we had made such findings for a private company, they would have prompted a request for the autorities to begin an investigation, states Kyrre Sletsjøe, the manager of CEPIA Technologies. He has a long experience from Norway's intelligence services, and has assisted governments in several countries with similar examinations .

Saken fortsetter under annonsen.

In order to be able to determine with a hundred percent certainty what kind of equipment is being used, who the target is, and where its exact location is, Aftenposten and the security companies would have to undertake measurements inside the buildings. However, only the police are authorized for such action.

Very advanced and expensive

The fake base stations revealed during the monitoring have been in a so called «identification mode». The transmitters were switched on and were able to register all mobile phones within its reach.

The way this equipment functions indicates that very advanced systems are involved, with price tags between 500 000 kroner (approximately 85 000 dollars) and 2 million kroner (330 000 dollars). This kind of equipment cannot be legally sold to private persons in NATO member countries.

Jahn-Helge Flesvik, who is manager of the security company Aeger Group, participated in Aftenposten's mapping. He too has experience from the intelligence community.

He has no doubt whatsoever about the conclusion:

- Only organisations with strong resources are able to employ the kind of technical equipment involved here.

The entire Parkveien may be monitored

On a Friday morning several ministers have come together for lunch in the government's guesthouse Villa Parafina in the street Parkveien. Prime minister Erna Solberg (conservative) steps out of her black Mercedes and enters the building, just a few yards from her own residence.

In this neighbourhood, where among others the American and Israeli embassies are situated, our

CryptoPhone repeatedly registered highly suspicious activity. With a series of measurements during several days, the security companies detected two strategically placed IMSI-catchers which cover the blocks along Parkveien. Signals from the secret transmitters have a range of 1000 meters with unobstructed view, and a slightly shorter range in built-up areas.

Who is behind?

The big question is who operates the fake base stations in the centre of Oslo. And how long have they been in use?

Only the police, the Police Security Service (PST) and the National Security Authority (NSM) have the autority, according to the Criminal Procedure Act and the Police Law, to utilize such equipment. But no Norwegian official contacted by Aftenposten says the equipment belongs to them. Aftenposten has no reason to believe that the Norwegian government stands behind the transmitters.

- What I can say, is that the PST only to a very limited extent employs equipment that utilizes so called mobile regulated zones. And when we do, it will be part of precautionary measures or the investigation of a criminal offense. This is always

done on a legal basis, after a court order, says Signe Kathrine Aaling, police attorney at the Police Security Service.

Few people wish to speculate whether private companies, foreign intelligence or criminals have the resources to uphold such a large-scale espionage activity in Oslo's mobile network.

- What we see is a gathering of intelligence on Norwegian soil. Very few institutions in this country are authorized to use this kind of equipment, says Kyrre Sletsjøe in CEPIA Technology.

The Ministry of justice did not want to make an immediate comment on the matter. But only the morning after receiving the results of Aftenposten's investigations, did staff members from the National Security Authority appear on the streets of Oslo city, trying to trace the illegal base stations.

- **RELATED ARTICLE: Sources: We were pressured to weaken the mobile security in the 80's**

PST: Numerous players might be behind this

- Many people have an intention to access the mobile communicatons of others, says Arne

Christian Haugstøyl in the section for preventive action at PST. Aftenposten has disclosed, outside of Stortinget and several ministries, the presence of advanced espionage equipment that intercepts and monitors mobile phones.

- I think the findings are interesting, says section leader Haugstøyl at the PST. He says numerous players might be involved in this activity.

- Many people have the intention to access the mobile communication of others, and we know it is happening. It might be private players and it might be state players, he says. The PST confirms that the level of intelligence activity in and against Norway is high.

- I cannot say that the findings you made can be attributed to states' illegal intelligence activity, but on the other hand we can not exclude the possibility. We are aware that they have both an intention and the capacity to do so.

- Do you think foreign intelligence is involved?

- I can not, on the basis of these findings, state that it involves foreign intelligence, but I can say that we are aware of foreign intelligence services that have this kind of capacity. And in our preventive work,

we warn persons who administer Norwegian interests against discussing sensitive matters on the mobile phone.

- Will you be undertaking something on the basis of Aftenposten's informations?

- The PST are working continuously to prevent illegal intelligence activity. Most important for us is to convince Norwegians involved in managing Norway's interests, to reduce their own vulnerability. For instance avoid discussing sensitive matters on the mobile phone.

- Why is it so difficult for you to prevent this activity?

- This equipment involves no permanent installations, and there are no large antennas. It all fits in a suitcase. The PST sees no point in running around, trying to find the equipment itself. It is important for us to work with preventive measures and reduce the vulnerability, simply to make the Norwegian public understand that if you have a secret, you should not discuss it on an open line, says Haugstøyl.

NSM looks into the risk of espionage

The National Security Authority was informed last

Thursday about Aftenposten's detection of fake mobile base stations. The next day they started their own investigations near important buildings in the centre of Oslo.

- We take this very seriously, says Hans Christian Pretorius, who is head of department with the NSM.

- We started our own investigations immediately after receiving the information from Aftenposten, explains Pretorius.

It is not known who deployed the fake base stations (IMSI-catchers), the equipment used to monitor mobile communications. Pretorius confirmed that the security autority detected signals from IMSI-catchers in the centre of Oslo.

- We started out tracing the locations where Aftenposten had already been. We examine this particularly with a view to where there is a need to shield institutions – obviously government offices and other important buildings, says Pretorius. He adds that «our mission concerns objects that are vital for society».

Here you can send tips via an encrypted connection to our journalists.

Examined central buildings this Friday

- The results shown by Aftenposten's survey make us able to sharpen our own investigations. We did that on Friday, says Pretorius.

- Did you find IMSI-catchers, as Aftenposten did?

- We found things. We don't have all the data ready in order to find indications in precisely the same locations. But we did register signals from IMSI-catchers in the centre of town, says Pretorius. He adds that it is too early to say how many and where, or what types and capacity they have

Complicated disclosure

Pretorius says the findings are worrying.

- We do not know the intentions of those who are behind this, why the IMSI-catchers are here, and what they are collecting. But we are working to find that out right now, he says.

- It is important for us to secure our own communication. If weak points are being exploited, someone may have the opportunity to identify, listen in on conversations and find out persons' whereabouts. Of course this is unfortunate, he says.

According to the NSM, it may be extremely difficult to pinpoint the exact position of an IMSI-catcher. The equipment may be switched off at times, the signals are coming and going. In addition, these signals must be correlated to real base stations. This is demanding work, both as to technical equipment and time.

THIS IS HOW THE FAKE CELL TOWERS WORK

- The fake base stations - or cell towers - may monitor thousands of citizens in Oslo every day.
- They have the same size as a computer, cost between 10 000 and 12 million kroner (less than 2000 up to 2 million dollars). They make Oslo's mobile network very unsafe.
- The signals from the fake base station near the intersection Rådhusgata/Skippergata will blink for 20-30 seconds. Then they fade away.
- A few minutes later, the radiosignals are back. They are much too strong, and they come from somewhere they ought not come from.
- The alarm flashes on the advanced Falcon II-equipment belonging to the security-experts Aftenposten cooperates with. Once again we picked up the signals from an IMSI-catcher, a fake mobile base station.
- The Falcon II indicates that signals are coming from a surveillance point only 50 – 100 meters away, probably hidden in an office, a window, a

car or a small suitcase. Most probably it is placed a few hundred meters from the Prime minister's office (SMK), the Ministry of defence, the Norwegian Defence staff and Norges Bank, the Norwegian central bank.

IMSI-catchers

- Intelligence staff, police and military men refer to the fake base stations as «IMSI-catchers», «grabbers» or «stingrays».
- An IMSI-catcher tries to make itself as attractive as possible, in order to persuade your cell phone choose its signals instead of those coming from all the legal base stations in the vicinity. It offers strong signals and other data intended to cheat your mobile device.

And this makes them easy to detect, if you know what you are looking for, according to Kyrre Sletsjøe, the manager of CEPIA Technologies, the company which conducted the monitoring for Aftenposten.

Sophisticated equipment in Oslo

- One of the IMSI-catchers we registered is so technically advanced that it operates in dual bands, says Jahn-Helge Flesvik in the security company Aeger. This equipment can pick up and identify a mobile device in a very short time.

First step to a further surveillance

In the initial stage IMSI-catchers can only be used for collecting data from the sim-card. The most advanced gadgets may register several hundred numbers in just a few minutes.

Once your mobile phone has been detected by a fake base station, it will be aware that you find yourself close to the station, and it may control what your phone will be allowed to do.

Then the IMSI-catcher may enter an active mode in order to eavesdrop on certain conversations. In the next step, the IMSI-catcher will transmit the conversation to the real GSM-system. But the spies are sitting in between, where they are able hear every word.

In addition the fake base station may register SMS-messages and install spyware which enables someone to switch on the microphone. In that case, the mobile phone may be used for monitoring rooms or offices.

Even if Aftenposten's investigation is the first of its kind in Norway, security authorities, the police, criminals and spies have used the same equipment for at least 10 years. It is especially effective when hunting criminals and controlling mobile

communication in an area, in order to prevent detonation of remote-controlled bombs.

THE METHOD

This is how Aftenposten detected the fake base stations in Oslo.

- 1. From October 10 until November 21 Aftenposten used one of the world's most advanced encrypted mobile phones, the CryptoPhone, in order to identify suspicious mobile activity in the Oslo area.
- 2. This mobile was produced by the company GSMK and is distributed in Norway by Multisys. It can analyze communications in the baseband processor of your mobile phone, and it reacts when it discovers suspicious activity indicating the presence of fake base stations nearby.
- 3. Aftenposten made 50 000 measurements during 57 different expeditions, covering 100 kilometers in the streets in and around Oslo. The route was logged with location data.
- 4. Every indication was controlled for possible sources of error, for example signal strength, poor coverage, tunnels, bridges and imprecise GPS-positions. 122 incidents were, according to the CryptoPhone, «highly suspicious», indicating a fake base station nearby.
- 5. This material was submitted to the mobile companies Telenor and Netcom, the Police Security Service and the Norwegian Post and

Telecommunications Authority for comments. None of them could say whether they had information about fake base stations in Oslo. Telenor did not wish to meet with Aftenposten, they would only answer in an e-mail.

- 6. As a next step, this newspaper went into a cooperation with the Norwegian security firm Aeger Group, and the British-Norwegian-Czech company CEPIA Technology.
- 7. Both companies are being led by Norwegians with a long experience from military intelligence. They are hired by private institutions and state authorities to detect illegal surveillance.
- 8. Based on Aftenposten's informations, the security companies searched for signals at several locations in the Oslo-area in the weeks no. 49 and 50. They used highly sophisticated counterintelligence equipment.
- 9. This monitoring makes it possible to to identify with very high probability the location of IMSI-catchers, down to a distance of 50 meters. In order to pinpoint the precise location, however, one would need police authority to access offices and premises.

The story in Norwegian: Stortinget og statsministeren overvåkes

SISTE ARTIKLER OM

mobilspionasje:

THE GLOBE AND MAIL

RCMP fight to keep lid on high-tech investigation tool

COLIN FREEZE, MATTHEW BRAGA and LES PERREAUX
TORONTO and MONTREAL — The Globe and Mail
Published Sunday, Mar. 13, 2016 9:53PM EDT
Last updated Friday, Mar. 18, 2016 10:42AM EDT

Police in Canada are fighting to keep secret the specifics of advanced technology they've used to spy on mobile phones in a criminal investigation into organized crime.

Court documents filed in the Quebec Court of Appeal show government lawyers have acknowledged that the RCMP used an extraordinary communications-interception technique involving "mobile device identifier" equipment.

But the Crown will be fighting to keep details of the operation under wraps during a court hearing scheduled for March 30 in Montreal.

Chris Parsons, a researcher with the Citizen Lab at the University of Toronto's Munk School, said this case "wouldn't be the first time [these devices] have been used – but it would be the first time [authorities] have been caught out in court."

The public is bound to want to know more, Mr. Parsons said. "These are fundamentally devices of mass surveillance," he said.

"Authorities using them will also be collecting information about law-abiding Canadians."

Between 2010 and 2012, detectives in RCMP "Project Clemenza" used a high-tech device to eavesdrop on a group of reputed mafia members who were sending each other encrypted messages on BlackBerry phones. Police believed the suspects were out to settle scores during the power vacuum that had emerged after the jailing of mob boss Vito Rizzuto.

On Nov. 24, 2011, a New Yorker named Salvatore (Sal the Ironworker) Montagna was shot dead on the outskirts of Montreal. Fearing more bloodletting was imminent, an RCMP-led team divulged its ongoing operation to local police, so they could make arrests in that gangland slaying.

Defence lawyers suggest the machinery the RCMP used in the case works by mimicking a cellphone tower and can trick all mobile phones within a specific radius into giving up data to police.

That would make this equipment similar to dragnet devices – known as "Stingrays," "cell-site simulators" or "IMSI catchers"– that have become ubiquitous and controversial in the United States. The New York Police Department, for example, was recently forced to release documents showing it had secretly used similar tracking technology more than 1,000 times since 2008.

The Mounties will not comment about their investigative techniques. "Seeing that this matter is still before the courts, it would be inappropriate for the RCMP to comment," said Sergeant Harold Pfleiderer.

The Mounties' use of the equipment is documented – in broad strokes – in a Crown brief sent to the appeal court in December, as part of the organized-crime case.

Nearly five years after the murder, most of the seven accused conspirators in the murder still await trial, as lawyers and prosecutors argue how much of the RCMP's techniques should be disclosed to the defence.

Last November, Quebec Superior Court Judge Michael Stober ordered the Crown to acknowledge its use of RCMP "mobile device identifier" (MDI) technology, and added that the accused are entitled to know details about it.

Crown lawyers immediately appealed. "The information sought would tend to identify the RCMP's methods and give a way to circumvent them," says the Dec. 14 appeal brief. Arguing that the technology is shielded by "police investigative techniques privilege," the brief says any disclosure will "hinder the RCMP's capabilities to lead criminal investigations."

The filing shows the Crown is resisting the defence's bid for the "manufacturer, make, model" of the device in question, as well as its "practical range." The defence wants "confirmation the device is a cell-site simulator" and, also, to know whether federal authorities have studied the privacy, safety and technical impact of such surveillance.

The filings do not make clear how powerful the RCMP equipment was.

Some such devices can intercept voice conversations or text messages. Others merely collect what is known as "metadata" – or information relating to phone numbers, SIM cards, or handset identifiers – on all phones that show up in a given radius.

The Crown brief suggests the RCMP used the technique to lay the legal groundwork for warrants that could facilitate lawful eavesdropping against suspects who were proving hard to track.

The crux of the alleged murder-conspiracy centres on a circle of eight suspected mobsters, one of whom is now dead. Some were known to police at the time only by the aliases they used on their phones, such as "Gateau," "Aaaaaaacounts," "Shadow," and "JJ."

The brief says the Mounties used their device as a targeting method to figure out which specific BlackBerrys to target. "The fruits of the MDI were sometimes used as grounds to connect [BlackBerry] PIN numbers pursuant to … wiretap authorizations," the filing says.

There is no mention of verbal or typed conversations being collected by this equipment. The prosecution "will not use the MDI in its case," the brief says.

RCMP Project Clemenza has made headlines before, after the Mounties revealed they had figured out how to snoop on BlackBerry's supposedly secure messaging system. In 2014, the police force issued a press release claiming it had intercepted and read more than a million such messages as part of the wider investigation.

Now, defence lawyers are asking for details as to how exactly the Waterloo-based company may have helped police do that. Or, failing that, "how the RCMP came into possession of the BlackBerry global encryption key."

But this disclosure, too, has been resisted by the Crown.

Also on The Globe and Mail

go2INTERCEPT

GSM Interception ▪ IMSI Catcher and Voice Interception

Part of the product line go2SIGNALS

go2INTERCEPT passive:

GSM interception –
Passive, massive, of the air.

(page 3-4)

go2INTERCEPT active basic:

IMSI catcher –
Identify, control, locate, 2G, 3G.

(page 5-6)

go2INTERCEPT active extended:

IMSI catcher and voice interception –
Intercept, control, track, 2G, 3G.

(page 7-10)

go2INTERCEPT passive:
GSM interception –
Passive, massive, of the air.

The go2INTERCEPT passive off the air GSM interception unit is able to intercept the communications between the handset and the BTS.

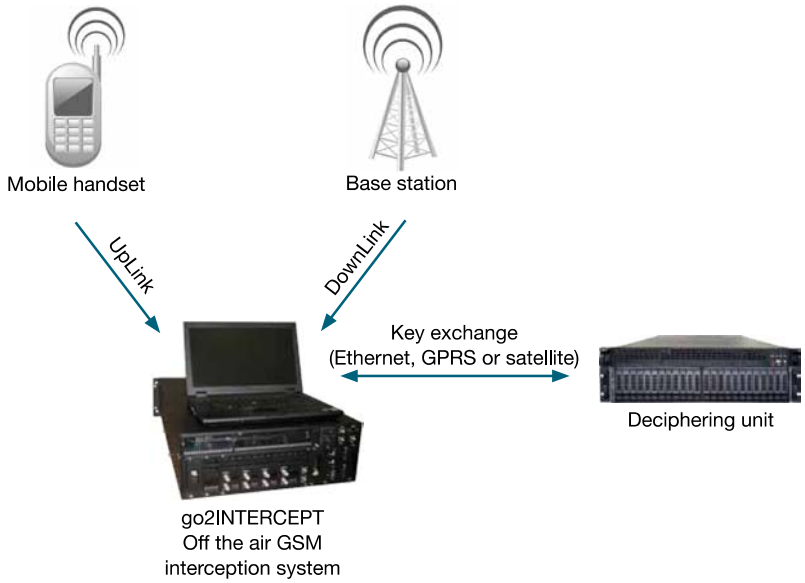
It is a wide band (processing the whole GSM bands) and passive solution, meaning that absolutely nothing is sent to intercept. It makes this solution completely undetectable by the targets or the operators unlike active interception solutions in the markets. Thanks to its dense FPGA architecture, this solution is able to intercept up to 60000 communications per hour, which enables this solution to be suited for massive application (border control for example), the go2INTERCEPT (passive) is able to demodulate and decipher in real time up to 320 duplex communication.

Two versions of go2INTERCEPT (passive) are available either in a 2U format for low cost application (up to 20 full duplex simulta-neous communication) or in a 3U format to get the full power of the systems.

The front end can be connected to the deciphering box (go2DECIPHER) through ethernet connection using either Vsat, 3G or cable links. In the case of a powerful deciphering box, multiple front ends can be connected.

Key features

- 3U 19” rack device
- 2G and 2,5G
- SMS, data and MMS supported
- From 10 to 320 simultaneous voice interceptions
- Up to 60000 intercepted communications per hour
- Simple Ethernet interconnection to the deciphering box
- Can be used as a tactical equipment in vehicles



Filtering abilities

Once the intercepted communications are stored in the data base, the user friendly GUI proposes many filtering abilities (operators,services, target ...):

- Provider selection
- Cell selection: power and quality criteria
- Service selection: GSM, GPRS, SMS, In/Out call
- Target selection: TMSI, IMSI, IMEI, MS-ISDN

Passive off the air GSM interception front end

- Passive and wide band solution
- All GSM bands (GSM450, GSM850, EGSM900, DCS1800, PCS1900)
- Full band analysis: Simultaneous acquisition of all channels
- No limit on frequency hopping and real time handover management
- Up to 64 cells can be under surveillance
- Automatic cell detection
- Store telephone conversations on the hard drive
- Ability to listen to conversations in real time
- Optional speaker identification thanks to biometric voiceprint technique

Control and test

- Remote and local control
- Ethernet connection to the deciphering unit
- BITE

Operational / physical / electrical specifications

Technical parameters	2U version	3U version
Connection to deciphering unit	Ethernet (RJ45)	Ethernet (RJ45)
Number of simultaneous calls	20	128, 256 or 320
AC power	115/230 V AC ± 15 % 47-63 Hz	115/230 V AC ± 15 % 47-63 Hz
Consumption	300 VA	400 VA
Size	19" 2U	19" 3U
Weight	< 10 kg	< 27 kg
Operating temperature	0°C to +40°C	0°C to +40°C
Storage temperature	-40°C to +70°C	-40°C to +70°C

go2INTERCEPT active basic:
IMSI catcher –
Identify, control, locate, 2G, 3G.

The go2INTERCEPT active basic is a tactical equipment managing target identification and localization through their IMSI or IMEI on 2G (GSM - DCS) and 3G (UMTS) networks. Designed to be operated by non specialists, it can be used for mobile or fixed operations.

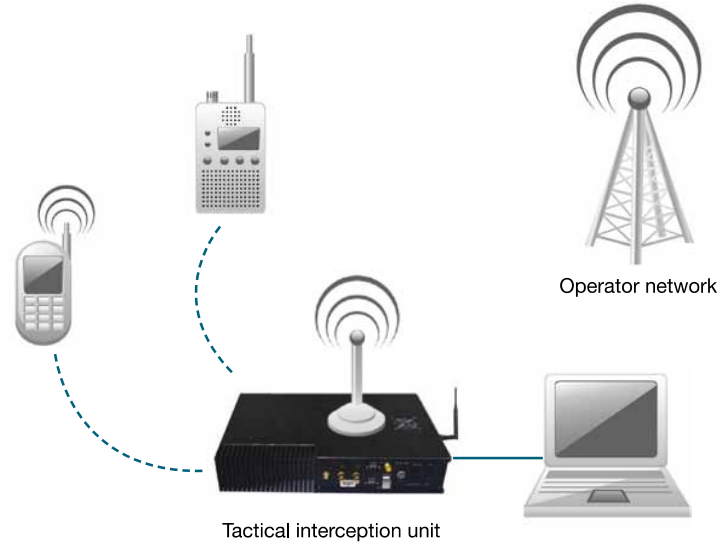
The equipment clones a neighboring cell (BTS or Node-B) with user controlled parameters, forcing the surrounding mobile equipments to identify themselves. Once identified, the mobiles can either be kept within the cloned cell for further intelligence, eavesdrop or send SMS in 2G, ringing the phone, released on the original network, disabling it.

Cell cloning is pursued thanks to an advanced automatic 2G and 3G spectrum scanner.

The front end can be connected to the deciphering box (go2DECIPHER) through ethernet connection using either Vsat, 3G or cable links. In the case of a powerful deciphering box, multiple front ends can be connected.

Key features

- Embedded power amplifier
- Multi-bands and multicells (GSM, DCS and UMTS)
- Fast 2G/3G scanner
- Target identification, target localization, SMS interception, SMS sending, mobile ringing for localization purpose, 3G -> 2G switch, mobile disabling, interception of called numbers, listening of environmental sounds
- Data mining with a on-line and off-line exploitation



Technical specifications

Mission Preparation	
Organisation	■ Use of predefined scenarios or manual configuration ■ Off-line & on-line mission creation ■ Automatic generation of scenarios from environment (quick start)
Mission options	■ Power ramp effect ■ Mission scheduler: multi clone start / stop ■ Ability to follow a moving target with continuous adaptation of clones to the environment (roaming)
Tools	■ 2G/3G fast scanning, advanced configuration & cloning tool ■ Clone coverage indicator
Catching	
Capacity	Multi-cells, multi-operators, multi-bands: GSM-900, DCS-1800, UMTS 900 and UMTS- 2100 (other frequency bands on request)
Action and data gathering	■ IMSI and IMEI ■ New contact / previously catched IMSI highlight ■ Multi localization ■ SMS (send / receive) (2G only) ■ Ringing for localization purpose (2G only) ■ Presence management (2G only) ■ Silent call for localization purpose ■ Blocking (2G only) / disabling of the mobile ■ Forcing target from 3G to 2G ■ Interception of called numbers (2G only) ■ Listening of ambient sounds (2G only) ■ Searching of mobile location with display on a map
Administration	
Station	Semi-ruggedized laptop
Post-analysis	■ Inter-case / inter-mission search ■ Multiple catched IMSI and IMEI focus ■ Wild card search ■ Data base export ■ Eavesdropped SMS search / export ■ Display of Vortex-Air location when capturing
Contact identifications	■ IMSI & IMEI full or partial ■ Attributes (photos, notes, friends, enemies and associated actions [block, unblock, disable])
User profile	User restriction or full access
Packages	
Pack 1 - pedestrian: backpack configuration with enhanced battery autonomy	■ 2 omnidirectional antennas and 1 high gain directional antenna ■ 1 hot-swap battery (1.5 hour) with charger ■ Back rack
Pack 2 - vehicle: installation in a vehicle with enhanced autonomy and high coverage	■ 2 omnidirectional antennas and 2 high gain directional antennas ■ Lighter adapter
Pack 3 - fixed: monitoring and site protection	2 omnidirectional antennas and 2 high gain directional antennas
Physical specifications	
Dimnesion	400 x 268 x 80 mm
Weight	5.3 kg
Energy	110/220 V AC (power supply provided) or 9/24 V DC < 140 W
Power	
Amplifier	40W at 900 MHz, 60W at 1800 MHz, 100 W at 2100 MHz
Antenna output	10 W mean in the band, up to 20 W peak

go2INTERCEPT active extended:
IMSI catcher and voice interception – intercept, control, track, 2G, 3G.

The powerful intelligence tool allows effectively track targets activities by monitoring their most used device – their cell phone.

The IMSI catcher and voice interception system of go2INTERCEPT is a state-of-the-art system that was designed to monitor, track, manipulate and control cell phones both in GSM networks and 3G (UMTS) networks.

Key features

- Extract the phone identities – IMSI, IMEI, MSISDN
- Collect the identities (IMSI/IMEI) of all phones in area of interest
- Alert about presence of target phones in the area
- Blocks phone communication – for all phones or selectively
- Intercept multiple calls and SMS simultaneously in random and target mode (inbound and out-bound communication)
- Disconnect designated calls
- Reroute calls and SMS to designated destination
- Change the content of target SMS
- Send fake SMS to target, or on behalf of a target
- Locate phones/target position
- Disable GSM activated explosive devices
- Covers multiple GSM and 3G networks simultaneously
- Handles effectively any network encryption (A5.0, A5.2, A5.1, A5.3)
- Tactical design for intuitive operation, easy transport and fast deployment

Description

go2INTERCEPT (active extended) is designed to perform man-in-the-middle attacks for mobile phones over GSM (2G, 2.5G) and UMTS (3G) networks.

The system emulates a real cell (base station) attempting the surrounding phones to select and register to the fake cell. As a result, the system becomes the serving cell of the surrounding phones (all phones or only designated phones) and consequently controls the phones communication.

As such, the system is used to extract the target identity, to track the target location, to monitor the target communication and to manipulate the target phone in advanced methods.

Typical applications

Calls and SMS interception

go2INTERCEPT (active extended) conducts seamless interception of target inbound and outbound and SMS over GSM networks with-out cooperation or authorization from the GSM operator. The system can monitor as much targets as required and handle multiple live calls simulta-neously.

Calls and SMS manipulations

Besides of monitoring the target calls and SMS, the system allows to manipulate the target communication in various ways:

- Block or disconnect specific or all calls and SMS-messages of any target.
- Send fake SMS messages (fake content and fake identity) to the target or on behalf of the target.
- Reroute calls and SMS from/to the target.
- Change SMS content that was sent from/to the target.

IMSI and IMEI extraction

The system allows to extract the identity of any phone in the area and also to alert about the presence of specific phones or targets in a certain area.

Denial-of-service

The system can block the communication of all phones in a certain area or to block the communication of only specific phones.

Find a target

The system force the phone to transmit a seamless signal. The phone signal is tracked by a dedicated receiver and allows getting closer to the target till final resolution of its position.

3G (UMTS) handling

Since interception is not possible over 3G networks, the 3G module generates a signal to the 3G phones that cause them to move to the GSM network.

Once the phone moves to the GSM network, the GSM module takes over and conducts the interception of the target as well as all other actions that are described above.

Main modules of the system

GSM modules

Each GSM module works on a specific band (e.g. 850, 900, 1800, 1900 MHz) and can emulate one GSM network at a time. It is possible to change the emulated network on the fly. If there is a need to work on several networks in parallel or the networks are using different bands, then several GSM modules are required in the system.

3G (UMTS) module

Each 3G module works on a specific band (e.g. 850, 1900, 2100 MHz) and can emulate one 3G network at a time. It is possible to change the emulated network on the fly. If there is a need to work on several networks in parallel or the networks are using different bands and/or multiple UMTS channels, then several UMTS modules are required in the system.

Routing modems

The modems in the system are used to reroute the calls of the target to the real GSM network and vice versa, in order to conduct full and seamless interception of the targets' inbound and outbound calls and SMS.

Software application and UI (User Interface)

Installed on a standard laptop, the software (SW) management application allows conducting all tasks related to the system, to monitor in real time the intercepted calls and to record all calls and interrogated information. The SW application includes also a back-office that presents all logged data and conduct applicable queries on the collected data.

Internal power amplifiers

To boost the transmission signal of the system, the system includes 4W integrated power amplifiers per each GSM module and 25W integrated power amplifiers per each 3G module.

Additional peripheral equipment that may be used with the system

go2DECIPHER

Most GSM networks are using A5.1 or A5.2 encryption protocol to enhance the privacy measures for its subscribers calls.

Yet, some networks allow calls to be conducted with no encryption (AKA A5.0) when the phone does not support the encryption protocol.

When A5.0 is allowed in the network, go2INTERCEPT (active extended) reduces all intercepted calls to A5.0 and does not need any external breaker, however, in cases were the network does not allow to reduce to A5.0, it will be mandatory to connect the system to an A5.1/A5.2 breaker that breaks in real time the encrypted key (AKA Kc) in order to allow the interception of the call or SMS.

The breaker can be located next to the system unit or remotely with any TCP/IP connection (i.e. LAN, WIFI, UMTS connection).

External GSM power amplifier

In certain cases when more transmission power is required to extend the effective range of the system, it is possible to connect 25W external GSM power amplifier.

External antennas

Various types of antennas can be deployed and used for the system operation. The selection of antennas depends on the operation scenario and the system setup such as magnetic omni-antennas when patrolling with a vehicle in and urban area or hi-gain directional antenna installed on a tripod or mast in a long-range operation.

System specifications

Technical parameters	Value
GSM frequency bands	850, 900, 1800, 1900 MHz
3G frequency bands	850, 1900, 2100 MHz
Simultaneous duplex channels	4, 6 or more
Simultaneous GSM BTS	2 or more
Simultaneous 3G BaseStations	2 or more
Interception of outbound calls	Yes
Interception of inbound calls	Yes
Interception of outbound SMS	Yes
Interception of inbound SMS	Yes

Technical parameters	Value
Detected identities	IMSI, IMEI, MSISDN
Voice codec types	LPT-RPE, FR, EFR, HR, AMR
Random & Target Mode	Yes
DTMF tones interception	Yes
Ability to handle 3G phones	Yes
Ability to locate target phones	Yes
Ability to change SMS content	Yes
Ability to interrupt calls	Yes
Ability to prevent calls	Yes

go2SIGNALS

... monitoring a connected world


go2DECODE


go2MONITOR


go2ANALYSE


go2RECORD


go2INTERCEPT


go2DECIPHER

PLATH AG

Stauffacherstrasse 65

3014 Bern

Switzerland

Tel: +41 31 311 6446

Fax: +41 31 311 6447

Email: info@go2signals.ch

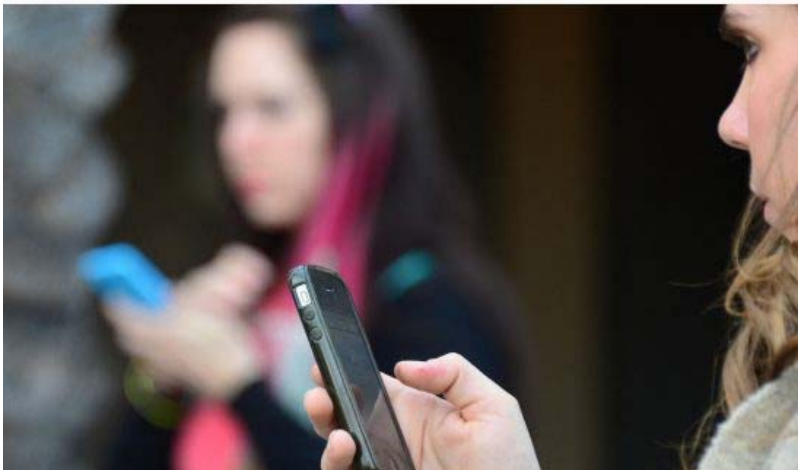
Further information on www.go2signals.ch

Version: V1.0 / 10 2013 (Subject to modification)

News / Canada

The cellphone spyware the police don't want to acknowledge

Canada's two largest police forces are refusing to say if they use stingrays, which work by scooping up the cellphone signals of everyone nearby.



VIEW 2 PHOTOS

FREDERIC J. BROWN / AFP/GETTY IMAGES

Canada's two largest police forces won't say if they use surveillance technology that allows them to spy on people's cellphones.

By: Robin Levinson King Staff Reporter, Published on Tue Dec 15 2015

High-tech surveillance equipment called "stingrays" allows police to listen in on your cellphone conversations and text messages — even if you've done nothing wrong.

But Canada's two largest police forces are refusing to say if they use these devices, which work by scooping up the cellphone signals of people nearby.

The Royal Canadian Mounted Police and the Ontario Provincial Police have both declined to tell the Star if they use International Mobile Subscriber Identity (IMSI) catchers – also known as "stingrays" – because they say giving out that information could interfere with their investigations.

"With respect to the question you have been asking, I'm not in the position to speak given the operational nature of the question, so regrettably I cannot provide a response," said OPP spokesperson Sgt. Peter Leon. "I hope you do understand the position of the OPP with respect to this matter."

The RCMP also refused to provide any information about whether or how it uses stingray technology. When the Star used the Access to Information Act to request policies related to the RCMP's use of the technology, the RCMP wrote back that those records were exempt from disclosure.

Inside thestar.com


Video
Daesh claims responsibility for Brussels attacks


Desperate parents pray for federal action amid daycare 'anarchy'


1.6M workers in Ontario aren't entitled to paid sick days

Latest National Videos Watch more

Top News

NEW Rob Ford, former Toronto mayor, dead after battle with cancer

Updated LIVE: Daesh claims responsibility for Brussels attacks

Desperate parents want federal action amid daycare 'anarchy'

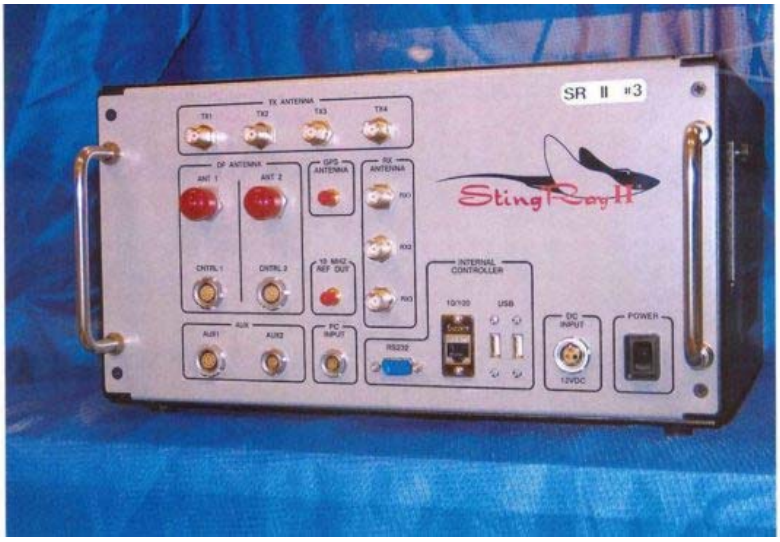
1.6M workers in Ontario aren't entitled to paid sick days

Updated Obama gives vision of U.S.-Cuba relations on live Cuban TV

Trudeau promises new budget will benefit middle class

Court appearance for Rosedale stabbing suspect

Elite PEAC private school finally taken over



AP

The StingRay II, manufactured by Harris Corporation, is a cellular site simulator that scops up cellphone data.

In reply to the Star's request, RCMP Supt. David Vauter cited sections of the law that exempt records because of attorney-client privilege and records that "could reasonably be expected to be injurious to the enforcement of any law of Canada or a province or the conduct of lawful investigations."

Later, an RCMP spokesperson reiterated that the RCMP does not comment on investigative techniques outside of the courtroom.

"The RCMP does not generally provide information on techniques or technologies used in criminal investigations. Investigative tools are ultimately assessed and tested by the courts," said RCMP spokesman Harold Pfleiderer in an email.

Stingrays electronically mimic cellphone towers, and trick cellphones within their range into connecting to them. Once a phone makes the connection, the stingray can grab data from it – including phone numbers, texts, phone calls and websites visited – in real time.

Ontario Privacy Commissioner Brian Beamish said the technology, which has a range of several kilometres, casts a wide net that doesn't distinguish between suspects in criminal cases and ordinary citizens.

"It's potentially so intrusive in terms of the amount of information it can gather, not only about a target but about other people as well, people that aren't under suspicion," Beamish said.

Ian Kerr, Canada Research Chair in Ethics, Law & Technology at the University of Ottawa, said that everybody's in the dark about whether police use stingrays – and if they do use them, how that might impact privacy.

"The problem is, we can't even know what those problems are," he said.

Although police won't say whether they use stingrays in Canada, use of the devices is widespread in the United States. Kerr said that he's spoken with many Canadian defence lawyers who believe the technology is used in police investigations here.

In August, the Office of the Ontario Privacy Commission upheld the Toronto Police Services Board's right to neither confirm nor deny that it owns stingrays.

"I specifically find that the disclosure of this information respecting the existence or non-existence of responsive records could reasonably be expected to reveal investigative techniques which are either in use or could likely be used in law enforcement," read the ruling written by Donald Hale, an adjudicator with the Office of the Ontario Privacy Commissioner.

That ruling related to a June 2014 access to information request by someone who wanted records of stingray purchases, which can cost upwards of $100,000 (U.S.).

". . . [D]ue to the nature of your inquiry surrounding the use of electronic surveillance

devices, disclosing such information could reveal classified operational procedures currently in practice by the Police Service; thus, potentially jeopardizing the effectiveness in fulfilling its policing mandate," read the original reply from the Toronto Police Services Board.

After the Star brought the ruling to his attention, Beamish said his office might not shield police from questions about stingray surveillance going forward.

"Having read and considered it (the ruling), it's not apparent to me that the public interest was given full consideration," Beamish said, adding the appeal to his office was the first of its kind related to stingrays.

"Were we to have another appeal, I think it could lead to a different conclusion, let me put it that way."

Following that ruling, Toronto police spokesperson Craig Brister told the Star that the force does not have a stingray. "I have made some inquiries and we do not use the Stingray technology and do not have one of the units," Brister said in an email.

Kerr said he doesn't buy into the other police forces' "excuse" that revealing general information about stingray technology could hurt their ability to do their jobs.

If police are using them, he said, they should come out and say how they use them and how they ensure that innocent citizens' privacy is protected.

More on thestar.com

Winter stations dismantled in the Beac...

Rona Ambrose's message to Liberals ah...

Restyle your home on a budget

Meet the Bernie Sanders toy

Relay for Life
After a week of unsettled weather, the..

Travel upgrade
Five reasons to upgrade your travel

Continuing Ed.
Finding what you love through classes

Era of excellece
The Marlies have influenced the Leafs

Whole30 cookbook
Reset your relationship with food

GTA real estate
Market hits record high

STINGRAYS

A Secret Catalogue of Government Gear for Spying on Your Cellphone

106

Jeremy Scahill, Margot Williams

Dec. 17 2015, 9:23 a.m.

THE INTERCEPT HAS OBTAINED a secret, internal U.S. government catalogue of dozens of cellphone surveillance devices used by the military and by intelligence agencies. The document, thick with previously undisclosed information, also offers rare insight into the spying

capabilities of federal law enforcement and local police inside the United States.

The catalogue includes details on the Stingray, a well-known brand of surveillance gear, as well as Boeing "dirt boxes" and dozens of more obscure devices that can be mounted on vehicles, drones, and piloted aircraft. Some are designed to be used at static locations, while others can be discreetly carried by an individual. They have names like Cyberhawk, Yellowstone, Blackfin, Maximus, Cyclone, and Spartacus. Within the catalogue, the NSA is listed as the vendor of one device, while another was developed for use by the CIA, and another was developed for a special forces requirement. Nearly a third of the entries focus on equipment that seems to have never been described in public before.

The Intercept obtained the catalogue from a source within the intelligence community concerned about the militarization of domestic law enforcement. (The original is here.)

A few of the devices can house a "target list" of as many as 10,000 unique phone identifiers. Most can be used to geolocate people, but the documents indicate that some have more advanced capabilities, like eavesdropping on calls and spying on SMS messages. Two systems, apparently designed for use on captured phones, are touted as having the ability to extract media files, address books, and notes, and one can retrieve deleted text messages.

Above all, the catalogue represents a trove of details on surveillance devices developed for military and intelligence purposes but increasingly used by law enforcement agencies to spy on people and convict them of crimes. The mass shooting earlier this month in San Bernardino, California, which President Barack Obama has called "an act of terrorism," prompted calls for state and local police forces to beef up their counterterrorism capabilities, a process that has historically involved adapting military technologies to civilian use. Meanwhile, civil liberties advocates and others are increasingly alarmed about how cellphone surveillance devices are used domestically and have called for a more open and informed debate about the trade-off between security and privacy — despite a virtual blackout by the federal government on any information about the specific capabilities of the gear.

"We've seen a trend in the years since 9/11 to bring sophisticated surveillance technologies that were originally designed for

military use — like Stingrays or drones or biometrics — back home to the United States," said Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation, which has waged a legal battle challenging the use of cellphone surveillance devices domestically. "But using these technologies for domestic law enforcement purposes raises a host of issues that are different from a military context."

[redacted]

ANY OF THE DEVICES in the catalogue, including the Stingrays and dirt boxes, are cell-site simulators, which operate by mimicking the towers of major telecom companies like Verizon, AT&T, and T-Mobile. When someone's phone connects to the spoofed network, it transmits a unique identification code and, through the characteristics of its radio signals when they reach the receiver, information about the phone's location. There are also indications that cell-site simulators may be able to monitor calls and text messages.

In the catalogue, each device is listed with guidelines about how its use must be approved; the answer is usually via the "Ground Force Commander" or under one of two titles in the U.S. code governing military and intelligence operations, including covert action.

But domestically the devices have been used in a way that violates the constitutional rights of citizens, including the Fourth

Amendment prohibition on illegal search and seizure, critics like Lynch say. They have regularly been used without warrants, or with warrants that critics call overly broad. Judges and civil liberties groups alike have complained that the devices are used without full disclosure of how they work, even within court proceedings.

"Every time police drive the streets with a Stingray, these dragnet devices can identify and locate dozens or hundreds of innocent bystanders' phones," said Nathan Wessler, a staff attorney with the Speech, Privacy, and Technology Project of the American Civil Liberties Union.

The controversy around cellphone surveillance illustrates the friction that comes with redeploying military combat gear into civilian life. The U.S. government has been using cell-site simulators for at least 20 years, but their use by local law enforcement is a more recent development.

The archetypical cell-site simulator, the Stingray, was trademarked by Harris Corp. in 2003 and initially used by the military, intelligence agencies, and federal law enforcement. Another company, Digital Receiver Technology, now owned by Boeing, developed dirt boxes — more powerful cell-site simulators — which gained favor among the NSA, CIA, and U.S. military as good tools for hunting down suspected terrorists. The devices can reportedly track more than 200 phones over a wider range than the Stingray.

Amid the war on terror, companies selling cell-site simulators to the federal government thrived. In addition to large corporations

like Boeing and Harris, which clocked more than $2.6 billion in federal contracts last year, the catalogue obtained by *The Intercept* includes products from little-known outfits like Nevada-based Ventis, which appears to have been dissolved, and SR Technologies of Davie, Florida, which has a website that warns: "Due to the sensitive nature of this business, we require that all visitors be registered before accessing further information." (The catalogue obtained by *The Intercept* is not dated, but includes information about an event that occurred in 2012.)

The U.S. government eventually used cell-site simulators to target people for assassination in drone strikes, *The Intercept* has reported. But the CIA helped use the technology at home, too. For more than a decade, the agency worked with the U.S. Marshals Service to deploy planes with dirt boxes attached to track mobile phones across the U.S., the *Wall Street Journal* revealed.

After being used by federal agencies for years, cellular surveillance devices began to make their way into the arsenals of a small number of local police agencies. By 2007, Harris sought a license from the Federal Communications Commission to widely sell its devices to local law enforcement, and police flooded the FCC with letters of support. "The text of every letter was the same. The only difference was the law enforcement logo at the top," said Chris Soghoian, the principal technologist at the ACLU, who obtained copies of the letters from the FCC through a Freedom of Information Act request.

The lobbying campaign was a success. Today nearly 60 law enforcement agencies in 23 states are known to possess a Stingray or some form of cell-site simulator, though experts believe that

number likely underrepresents the real total. In some jurisdictions, police use cell-site simulators regularly. The Baltimore Police Department, for example, has used Stingrays more than 4,300 times since 2007.

Police often cite the war on terror in acquiring such systems. Michigan State Police claimed their Stingrays would "allow the State to track the physical location of a suspected terrorist," although the ACLU later found that in 128 uses of the devices last year, none were related to terrorism. In Tacoma, Washington, police claimed Stingrays could prevent attacks using improvised explosive devices — the roadside bombs that plagued soldiers in Iraq. "I am not aware of any case in which a police agency has used a cell-site simulator to find a terrorist," said Lynch. Instead, "law enforcement agencies have been using cell-site simulators to solve even the most minor domestic crimes."

The Intercept is not publishing information on devices in the catalogue where the disclosure is not relevant to the debate over the extent of domestic surveillance.

The Office of the Director of National Intelligence declined to comment for this article. The FBI, NSA, and U.S. military did not offer any comment after acknowledging *The Intercept*'s written requests. The Department of Justice "uses technology in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities," said Marc Raimondi, a Justice Department spokesperson who, for six years prior to working for the DOJ, worked for Harris Corp., the manufacturer of the Stingray.

WHILE INTEREST FROM local cops helped fuel the spread of cell-site simulators, funding from the federal government also played a role, incentivizing municipalities to buy more of the technology. In the years since 9/11, the U.S. has expanded its funding to provide military hardware to state and local law enforcement agencies via grants awarded by the Department of Homeland Security and the Justice Department. There's been a similar pattern with Stingray-like devices.

"The same grant programs that paid for local law enforcement agencies across the country to buy armored personnel carriers and drones have paid for Stingrays," said Soghoian. "Like drones, license plate readers, and biometric scanners, the Stingrays are yet another surveillance technology created by defense contractors for the military, and after years of use in war zones, it eventually trickles down to local and state agencies, paid for with DOJ and DHS money."

In 2013, the Florida Department of Law Enforcement reported the purchase of two HEATR long-range surveillance devices as well as $3 million worth of Stingray devices since 2008. In California, Alameda County and police departments in Oakland and Fremont are using $180,000 in Homeland Security grant money to buy Harris' Hailstorm cell-site simulator and the hand-held Thoracic surveillance device, made by Maryland security and intelligence company Keyw. As part of Project Archangel, which is described in government contract documents as a "border radio intercept

program," the Drug Enforcement Administration has contracted with Digital Receiver Technology for over $1 million in DRT surveillance box equipment. The Department of the Interior contracted with Keyw for more than half a million dollars of "reduced signature cellular precision geolocation."

Information on such purchases, like so much about cell-site simulators, has trickled out through freedom of information requests and public records. The capabilities of the devices are kept under lock and key — a secrecy that hearkens back to their military origins. When state or local police purchase the cell-site simulators, they are routinely required to sign non-disclosure agreements with the FBI that they may not reveal the "existence of and the capabilities provided by" the surveillance devices, or share "any information" about the equipment with the public.

Indeed, while several of the devices in the military catalogue obtained by *The Intercept* are actively deployed by federal and local law enforcement agencies, according to public records, judges have struggled to obtain details of how they work. Other products in the secret catalogue have never been publicly acknowledged and any use by state, local, and federal agencies inside the U.S. is, therefore, difficult to challenge.

"It can take decades for the public to learn what our police departments are doing, by which point constitutional violations may be widespread," Wessler said. "By showing what new surveillance capabilities are coming down the pike, these documents will help lawmakers, judges, and the public know what to look out for as police departments seek ever-more powerful electronic surveillance tools."

Sometimes it's not even clear how much police are spending on Stingray-like devices because they are bought with proceeds from assets seized under federal civil forfeiture law, in drug busts and other operations. Illinois, Michigan, and Maryland police forces have all used asset forfeiture funds to pay for Stingray-type equipment.

"The full extent of the secrecy surrounding cell-site simulators is completely unjustified and unlawful," said EFF's Lynch. "No police officer or detective should be allowed to withhold information from a court or criminal defendant about how the officer conducted an investigation."

JUDGES HAVE BEEN among the foremost advocates for ending the secrecy around cell-site simulators, including by pushing back on warrant requests. At times, police have attempted to hide their use of Stingrays in criminal cases, prompting at least one judge to throw out evidence obtained by the device. In 2012, a U.S. magistrate judge in Texas rejected an application by the Drug Enforcement Administration to use a cell-site simulator in an operation, saying that the agency had failed to explain "what the government would do with" the data collected from innocent people.

Law enforcement has responded with some limited forms of transparency. In September, the Justice Department issued new guidelines for the use of Stingrays and similar devices, including

that federal law enforcement agencies using them must obtain a warrant based on probable cause and must delete any data intercepted from individuals not under investigation.

Contained within the guidelines, however, is a clause stipulating vague "exceptional circumstances" under which agents could be exempt from the requirement to get a probable cause warrant.

"Cell-site simulator technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases," said Deputy Attorney General Sally Quillian Yates.

Meanwhile, parallel guidelines issued by the Department of Homeland Security in October do not require warrants for operations on the U.S. border, nor do the warrant requirements apply to state and local officials who purchased their Stingrays through grants from the federal government, such as those in Wisconsin, Maryland, and Florida.

The ACLU, EFF, and several prominent members of Congress have said the federal government's exceptions are too broad and leave the door open for abuses.

"Because cell-site simulators can collect so much information from innocent people, a simple warrant for their use is not enough," said Lynch, the EFF attorney. "Police officers should be required to limit their use of the device to a short and defined period of time. Officers also need to be clear in the probable cause affidavit supporting the warrant about the device's capabilities."

In November, a federal judge in Illinois published a legal

memorandum about the government's application to use a cell-tower spoofing technology in a drug-trafficking investigation. In his memo, Judge Iain Johnston sharply criticized the secrecy surrounding Stingrays and other surveillance devices, suggesting that it made weighing the constitutional implications of their use extremely difficult. "A cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization from a fully informed court," he wrote.

He added that Harris Corp. "is extremely protective about information regarding its device. In fact, Harris is so protective that it has been widely reported that prosecutors are negotiating plea deals far below what they could obtain so as to not disclose cell-site simulator information. … So where is one, including a federal judge, able to learn about cell-site simulators? A judge can ask a requesting Assistant United States Attorney or a federal agent, but they are tight-lipped about the device, too."

The ACLU and EFF believe that the public has a right to review the types of devices being used to encourage an informed debate on the potentially far-reaching implications of the technology. The catalogue obtained by *The Intercept*, said Wessler, "fills an important gap in our knowledge, but it is incumbent on law enforcement agencies to proactively disclose information about what surveillance equipment they use and what steps they take to protect Fourth Amendment privacy rights."

Research: Josh Begley

CONTACT THE AUTHOR:

Jeremy Scahill

jeremy.scahill@theintercept.com

@jeremyscahill

Margot Williams

margot.williams@theintercept.com

@MargotWilliams

106 Comments (closed)

Written Remarks for the German Parliament Committee of Inquiry

June 26, 2014

Christopher Soghoian, Ph.D.
Principal Technologist,
Speech, Privacy & Technology Project
The American Civil Liberties Union[1]

Introduction

Members of the committee, thank you for the invitation to testify before you today. I regret that I am not able to do so in person, due to a mechanical problem on my scheduled flight to Germany, but I hope to have the opportunity to do so at another date in the future.

In these written remarks, I will present my views on several topics related to surveillance. The main point I wish to make is this: The German government must prioritize information security if it wishes to protect itself, German companies, and the German people from surveillance by sophisticated foreign governments. This will require more than just establishing a "German cloud". Prioritizing security will also mean that the German police and intelligence services will also lose the ability to monitor phone calls, emails and cloud stored data that they likely will argue is essential to their work. To summarize: to keep the NSA from watching, you must also keep your own police and intelligence services from watching too.

The Limitations of Data Sovereignty

Even before the disclosures to the media in 2013 by Edward Snowden, European scholars had issued warnings about the FISA Amendments Act Section 702, and the ease with which it permitted the US government to compel US companies to provide data about their foreign customers.[2] After the media revealed the existence of PRISM, officials in several countries, including Brazil and Germany, voiced their concern about their countries' exposure to NSA surveillance. Germany's Interior Minister Hans-Peter Friedrich advised people who did not wish to have their communications monitored to "use services that don't go through American servers,"[3] while EU Commission Vice President Viviane Reding suggested that it was time for "Europeans to build their own cloud."[4]

European companies also seized the opportunity to use the NSA spying controversy to advertise their products. German email providers T-Online, GMX and web.de launched the "Email Made in Germany" program, which promised users that emails traveling between the three companies would never exit Germany.[5] Although it is of course always a good thing when companies improve the security of their

---

1 The opinions expressed in this testimony are my own alone.

2 *See* Joris Van Hoboken, Axel Arnbak and Nico Van Eijk, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad, June 9, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

3 *See* German Minister: Drop US Sites If You Fear Spying, Associated Press, July 3, 2013, http://bigstory.ap.org/article/german-minister-drop-google-if-you-fear-us-spying.

4 See Michael Scaturro, The Quest to Build an NSA-Proof Cloud, The Atlantic, November 21, 2013, http://www.theatlantic.com/international/archive/2013/11/the-quest-to-build-an-nsa-proof-cloud/281704/.

5 *See* Boom Triggered By NSA: German Email Services Report Surge in Demand, Spiegel Online, August 26, 2013, http://www.spiegel.de/international/germany/growing-demand-for-german-email-providers-after-nsa-scandal-a-918651.html.

products, the modest security measures announced by European companies to date, and the proposals for a “European cloud” from EU leaders will have a limited impact on the ability of the NSA or other well-resourced intelligence agencies to spy on Europeans.

These proposals assume that the only way that the NSA can monitor the communications of Europeans is by watching the data as it crosses international fiber optic cables, or demanding a copy of it it once it is stored on the servers of US companies. It is certainly true that the NSA and its 5-eyes partners engage in bulk collection of communications that flow through international communications cables they are able to access. It is also true that the NSA (through their friends at the FBI) are able to compel US cloud computing companies to turn over data in their possession. However, these are not the only ways for the NSA to get data.

When Britain's intelligence service, GCHQ, accessed the internal networks of Belgian telephone network operator Belgacom, they did so by hacking into the Belgian company.[6] Similarly, when GCHQ penetrated the networks of German satellite companies Stellar, Cetel and IABG, they did so by hacking.[7] The NSA's own hacking unit, the Tailored Access Operations (TAO) division, is reportedly “the largest and arguably the most important component of the NSA's huge Signal Intelligence Directorate, consisting of over 1,000 military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers.”[8]

Keeping data in Germany will not keep the NSA's legion of cyber-warriors out. Indeed, rather than focusing on *where* the data is kept, you should be focusing your attention on the need to encrypt data, so that when hackers do compromise German servers or gain access to internal German telecommunications networks, the only data they can steal is encrypted, and thus far less useful to them. Rather than focusing on the “German cloud”, you should instead be investing resources into the rapidly advancing field of “cloud cryptography”,[9] which permits you to put data in the cloud, without worrying about where it is stored, or which governments might be able to compel a service provider into turning it over.

Merkel-gate **and German law enforcement surveillance of telephones**

In October 2013, Der Spiegel revealed that the NSA had been spying on the telephone communications of German Chancellor Angela Merkel.[10] Subsequent news reports revealed that NSA's secretive Special Source Operations (SSO) division had installed electronic surveillance equipment in a “spy nest” on the roof of the American Embassy in Berlin.[11] Although German politicians were outraged to learn that the

---

6 *See* Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm, Spiegel Online, September 20, 2013, http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

7 *See* Laura Poitras, Marcel Rosenbach and Holger Stark, 'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel, Spiegel Online, March 29, 2014, http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

8 *See* Matthew Aid, Inside the NSA's Ultra-Secret China Hacking Group, Foreign Policy, June 10, 2013, http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group.

9 *See* Richard Falkenrath and Paul Rosenzweig, Op-Ed: Encryption, Not Restriction, Is The Key To Safe Cloud Computing, NextGov, October 5, 2012, http://www.nextgov.com/cloud-computing/2012/10/op-ed-encryption-not-restriction-key-safe-cloud-computing/58608/.

10 *See* Jacob Appelbaum, Holger Stark, Marcel Rosenbach and Jörg Schindler, Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?, Spiegel Online, October 23, 2013, http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html.

11 Embassy Espionage: The NSA's Secret Spy Hub in Berlin, Spiegel Online, October 27, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

Americans were spying on German telephone calls, this should not have come as a surprise. The millions of mobile telephones used by Germans are not secure and are vulnerable to interception using widely available equipment. One of the first companies in the world to sell special-purpose surveillance devices designed to track mobile phones and intercept telephone calls was Rohde & Schwarz, a German company.[12] The IMSI catchers sold by this company since the mid-1990s exploit well known security flaws that are still present in the latest $600 smartphones sold to consumers in the United States and in Germany.

IMSI catchers are used by law enforcement agencies in Germany and their use is authorized by statute,[13] which also mandates annual statistical reports describing their use be published by the Parliament.[14] There have been several formal parliamentary questions submitted regarding the use of IMSI catchers,[15] as well as a decision from the German Constitutional Court permitting their use.[16] It therefore cannot be said that IMSI catchers, or the fact that mobile telephones in Germany can be spied upon with special equipment, are a big secret. The only surprise, it is seems, is that the American government is using the same (or similar) surveillance equipment that the German police regularly use to monitor German citizens, and are using it to spy on your political leaders.

Each year, at the Chaos Computer Club Congress, some of the best security researchers in the world (many of whom are German) demonstrate serious security flaws in mobile telephone networks.[17] Each year, the cost of interception goes down,[18] yet governments, including Germany's, do nothing to make sure their citizens' telephone calls are secure.

The problem, of course, is that real telephone security, provided through “end-to-end” encryption technology, would make police wiretaps difficult, if not impossible. To effectively protect the phone calls of Germans from American, Russian, Chinese and Israeli surveillance, you would have to require that German phone networks upgrade to secure communications technologies that your own law enforcement agencies would also not be able to monitor. This would no doubt be unpopular with the German law enforcement community, but also perhaps many German voters, once they learned that terrorists, drug dealers and pedophiles could no longer be wiretapped or covertly tracked by the authorities.

There is no communications technology that exists that will keep out a sophisticated foreign intelligence agency, while still permitting “lawful access” by domestic law enforcement. If anything, lawful surveillance systems built into communications networks are an irresistible target for foreign intelligence agencies.[19] Once you accept that, then the real problem becomes political, not technical: Do

---

12 The earliest public document describing IMSI catchers and the Rohde & Schwarz products is an article in 1997 by Dirk Fox, a German security consultant. See Dirk Fox, IMSI-Catcher, Datenschutz und Datensicherheit, 21:539–539, 1997, available at http://www.secorvo.de/publikationen/imsi-catcher-fox-1997.pdf. Five years later, Fox published an updated, more in-depth article about the same technology. See Der IMSI-Catcher, Datenschutz und Datensicherheit, 26:212–215, 2002, http://www.secorvo.de/publikationen/imsicatcher-fox-2002.pdf.

13 *See* Section 9 of the Federal Constitution Protection Act (Special Forms of Data Collection), paragraph 4, http://www.gesetze-im-internet.de/bverfschg/__9.html.

14 *See* http://dip21.bundestag.de/dip21/btd/17/127/1712774.pdf (2011 data).

15 *See* http://dip21.bundestag.de/dip21/btd/14/068/1406885.pdf and http://dipbt.bundestag.de/dip21/btd/17/076/1707652.pdf.

16 *See* http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html.

17 *See* Karsten Nohl and Chris Paget, GSM — SRSLY ?, 26th Chaos Communication Congress (26C3), December 27, 2009, http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf.

18 *See* Jon Borland, $15 phone, 3 minutes all that's needed to eavesdrop on GSM call, Ars Technica, December 29, 2010, http://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/.

19 See Vassilis Prevelakis and Diomidis Spinellis, The Athens Affair, IEEE Spectrum, June 29, 2007,

you build your national communications to be secure, or to enable surveillance – knowing that surveillance will be possible by your own police, as well as several foreign intelligence agencies?

To date, Germany has prioritized surveillance-friendly communications networks. Perhaps that will change, but only if politicians are ready to accept that in order to keep the NSA out, the security technologies required will also necessarily prevent law enforcement agencies from conducting wiretaps and tracking legitimate targets.

A Regulatory Failure?

In December of 2013, Deutsche Telekom announced that it was the first German cellular telephone network operator to upgrade its network to deploy a more secure encryption algorithm ("A5/3") for voice communications over its cellular phone network.[20] This announcement was several months after the first Snowden disclosures, as well as the reports by Der Spiegel that Chancellor Merkel's phone calls were being monitored by the NSA.

Prior to the announcement, Deutsche Telekom, like most other wireless network operators, was likely using the A5/1 encryption algorithm. This algorithm, which was designed in the 1980s (and, weakened at the behest of several intelligence services),[21] was broken by researchers in the late 1990s,[22] but is still the most widely used cellular encryption algorithm in the world. Today, several surveillance companies (including firms in Germany[23]) sell sophisticated interception equipment capable of breaking this encryption algorithm and deciphering mobile conversations, in real-time.[24]

The A5/1 algorithm was broken by researchers in 1999, and in 2013, Deutsche Telekom finally upgraded their network to move from the weak A5/1 to the more secure A5/3. Why did it take 14 years and the largest surveillance scandal in decades for the customers of Germany's largest mobile operator to be upgraded to a more secure encryption algorithm?

I do not know the answer to this question, but I suggest that you ask your national telecommunications regulator, and see what, if anything, they have done to force German mobile network operators to promptly upgrade their networks and the phones used by their customers when they learn that a particular algorithm or cellular technology is insecure.

If, today, the phone calls of German journalists, business executives, and politicians can be intercepted with widely available equipment that can be purchased for just a few thousand euros, it suggests that

---

http://spectrum.ieee.org/telecom/security/the-athens-affair.

20 *See* Deutsche Telekom upgrades wiretapping protection in mobile communications, December 9, 2013, http://www.telekom.com/media/company/210108.

21 *See* Arild Færaas, Sources: We were pressured to weaken the mobile security in the 80's, Aftenposten, January 9, 2014, http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html (interviewing several experts involved with the creation of the original GSM A5/1 standard who claim the it was intentionally weakened as a result of pressure from the British government).

22 *See* Alex Biryukov and Adi Shamir, Real Time Cryptanalysis of the Alleged A5/1 on a PC (preliminary draft), December 9, 1999. Final paper published as Alex Biryukov, Adi Shamir and David Wagner, Real Time Cryptanalysis of A5/1 on a PC, Fast Software Encryption, Lecture Notes in Computer Science Volume 1978, 2001, pp 1-18. See http://cryptome.org/a51-bsw.htm.

23 See Passive GSM Monitoring System for A5.1, A 5.2 (A5.0) Encryption, http://www.pki-electronic.com/products/interception-and-monitoring-systems/passive-gsm-monitoring-system-for-a5-1-a-5-2-a5-0-encryption/

24 See Verint Sales Brouchure, 2013, http://s3.documentcloud.org/documents/885760/1278-verint-product-list-engage-gi2-engage-pi2.pdf.

your telecommunications regulator is not doing as much as they should to protect the security of Germany's telephone networks.

The role of technical experts in the surveillance oversight process

Surveillance is now, more than ever before, a highly-technical subject, the finer details of which can be difficult for political scientists and lawyers to understand. It is therefore vital that your committee, as well as every agency and committee with a role in the surveillance oversight process in Germany be assisted by technical experts, who can explain these deeply technical concepts to those making the decisions and writing the reports.

At the ACLU, I am embedded within a team of lawyers, who work on our surveillance related litigation. My primary job is to explain the technology to them, to make sure they understand the technical details related to the cases they are working on, and to ensure that the arguments we make in court are technically accurate. Prior to joining the ACLU, I worked for the Federal Trade Commission, the primary regulator of privacy in the United States Government, in a similar role.

I was the first technologist hired by the FTC and the ACLU. At both organizations, hiring technologists has changed the way they do business, and enabled them to make arguments that are far more technically sophisticated than they would have been able to do so before. After I left the FTC, the agency hired several more technologists, and even created a Chief Technologist position. Similarly, the ACLU this year hired a second full-time technologist. Technologists are a force-multiplier, enabling teams of lawyers to be far more effective at their jobs.

Inviting technical experts to testify before your committee is a great start. However, this is not enough. I urge you to hire technical advisors, and to ensure that the committees and courts that oversee your own national surveillance apparatus also have the technical expertise to really understand what is being done.

Thank you,

Christopher Soghoian
csoghoian@aclu.org

CURRENT AFFAIRS

Spy games turn real as eavesdropping technology spreads

16-08-2012 15:56 | Masha Volynsky

When is the last time you used your mobile phone? Did you say anything important? Are you sure no one else was listening? There are rising concerns in the Czech Republic about the increasingly common use of devices that can intercept your daily mobile communication. Masha Volynsky has more.

Download: MP3

Photo: Emin Ozkan, stock.XCHNG

It may sound like something out of the TV series The Wire, but a small box, known in the Czech Republic as Agáta, may be listening in on your mobile phone calls at any moment. Agáta, or IMSI Catcher, is essentially an eavesdropping device that, by using relatively simple hardware, can track phone calls and SMS messages coming in and out of mobile phones in a specific radius.

Jan Valos, a radio frequency engineer and hacker explains how an IMSI Catcher works once it is connected to a computer:

"It sends out a signal that is basically like the one coming from a cellular phone base station, which is why a mobile phone would voluntarily connect to it. If someone uses the device wisely and carefully, and does not stay in one place for too long, it is practically impossible to catch them."

The use of Agátas is becoming increasingly widespread in the Czech Republic. Although their functioning is practically undetectable to the users of phones being tracked, they can sometimes be intercepted by a police scanner.

The head of Czech Criminal Police unit for wiretapping, Tomáš Almer, confirmed they have been registering more and more uses of Agátas around the country. But no one has yet been caught for using an IMSI Catcher and it has not been determined how many Agátas are operating in the Czech Republic.

The Czech police sometimes use similar wiretapping devices during investigations, but they are required by law to obtain a court-sanctioned warrant. Most likely, though, there are not many Agátas in their possession, given their exorbitant pricing which can be up to 20 million Czech crowns. For private persons, it is illegal in the Czech Republic to turn an IMSI catcher on, but there are no laws prohibiting their purchase.

Andor Šándor, photo: Czech Television

Former head of the Czech Military Intelligence Agency and a security analyst Andor Šándor underscored the danger of the widespread sale of Agátas:

"It's been a known fact for a few years now that some companies do sell these devices. But if their use will not be in any way regulated, and access to these devices will not be in any way controlled, then a regular citizen can do absolutely nothing. The only way people can safeguard themselves is if they reveal only the necessary information during their mobile communication. But, obviously that goes against normal behavior of free persons."

At this point it is also becoming harder to trace who produces Agátas. Although an IMSI catcher was originally patented by a German company Rohde and Schwarz, it has been

FEATURED

Czech designers win main award at the International Fashion Showcase in London

Jan Velinger | Arts

1 | 2 | 3 | 4 | 5 | 6 | 7

MOST POPULAR

Český Krumlov - an island of unreality

12-03-2016 | Dominik Jůn

Český Krumlov is a small town situated in the far south of Bohemia, about 25km from the city of České Budějovice. Bordering the Šumava... More

Ethnic Czechs from Ukraine mark first year in their old-new homeland

10-03-2016 14:18 | Daniela Lazarová

A year has now passed since the start of a government sponsored repatriation program for ethnic Czechs from Ukraine. In its initial... More

08-03-2016 15:57 | Number of MPs aim to weaken anti-smoking legislation in name of smokers' rights

15-03-2016 | Koudelka taught me how to see, says helmer of One World film on great Czech photographer

11-03-2016 17:20 | Chinese investor plugs into significant Czech battery invention

ALSO IN THIS EDITION

Senate torpedoes church restitution bill

Daniela Lazarová

After hours of debate the opposition-controlled Senate on Wednesday rejected a controversial bill on the restitution of church property....More

hard to maintain exclusivity because of its generic nature. This year, Court of Appeal of England and Wales even invalidated the patent for reasons of obviousness.

Although Czech authorities are not willing to speculate on the subject, Mr. Šándor claims that the most likely private users of Agátas are security firms or rival businesses, or even companies trying to win high-stakes tenders. But there is no way to regulate the activities of either one of those groups. And there have been fears that some extortionist gangs may use this technology for nefarious purposes. So far, neither the police nor the lawmakers are doing anything to protect Czech residents from being unknowingly monitored.

Tools

SEND BY EMAIL
SUBSCRIBE TO RSS
PRINT

Social bookmarking

Like 5
Tweet

RELATED ARTICLES

Czech send record numbers of MMSes on Christmas Eve

25-12-2015 16:17 | Ruth Fraňková

People in the Czech Republic made 42.7 million calls from their mobile phones on Christmas Eve, the Czech News Agency wrote on Friday,... **More**

New stretch of Prague metro's A line to get mobile phone signal

18-11-2015 14:09 | Daniela Lazarová

People travelling along the new stretch of Prague metro's A line will no longer have to restrict their phone conversations to individual... **More**

25-10-2015 11:29 | Nearly 50 percent of Czech drivers use mobile phones while driving
06-10-2015 15:48 | Digital dependence claims one in four at addiction centre
02-10-2015 13:56 | Home Credit looks to US launch
25-08-2015 15:00 | HTC planned service centre in Brno now appears doomed

More

SECTION ARCHIVE

22-03-2016 15:23 | "Lex Babiš" threatens to topple ruling coalition
22-03-2016 15:23 | Researchers from Masaryk University uncover new evidence of how some cancer cells survive aggressive chemotherapy
21-03-2016 13:42 | Alfons Mucha's Slav Epic set for legal tug of war between Prague and painter's descendants
18-03-2016 15:42 | Opposition parties warn they will call vote of no-confidence over Stork's Nest

More

LATEST PROGRAMME IN ENGLISH

AAC:
64kbps

Archive

RSS and Podcasting
Take your pick from our new RSS channels

Facebook
Become a fan of Radio Prague

Twitter
Follow us on Twitter

More from Radio Prague

The New York Times | http://nyti.ms/1LhYJ1R

U.S.

Covert Electronic Surveillance Prompts Calls for Transparency

By TIMOTHY WILLIAMS SEPT. 28, 2015

Law enforcement officials across the United States have become enamored of the StingRay, an electronic surveillance device that can covertly track criminal suspects and is being used with little public disclosure and often under uncertain legal authority. Now, though, some states are pushing back, and are requiring the police to get a court order and local consent before turning to the high-tech tool.

Washington, Utah and Virginia recently approved laws requiring court orders for the use of such cell-site simulators by state and local police officers. California lawmakers this month approved such legislation by a wide margin. The California law would also require police agencies to get City Council approval before employing the devices, and to disclose on an agency website that they use the technology. Similar bills have been introduced in Texas and in Congress.

In Maryland, defense lawyers are re-examining thousands of cases to determine if the police have been deploying the technology legally.

“The public has finally become aware of what sorts of technologies are being used, and they are asking themselves, ‘Do we want to pay for this?’ and second, ‘What are the costs of this to our civil liberties?’ ” said Neil Richards, a

law professor at Washington University in St. Louis who studies privacy issues. “People do care about privacy. And it is reassuring that the system is working the way it’s supposed to — instead of law enforcement just saying, ‘The rules have changed when it comes to digital.’ ”

StingRays, one of several brands of such devices, are about the size of a suitcase. They mimic cellphone towers by forcing mobile phones in their vicinity to connect to the device, which allows the police to find the person with the phone.

The Federal Bureau of Investigation and local law enforcement officials say the devices are critical in locating dangerous criminal suspects. But the devices, which cost as much as $500,000, also collect data from all other cellphones in the area, whether those phones are on or off, without notifying phone users.

The F.B.I., which helps manage the distribution of the devices to police departments, requires agencies to sign nondisclosure agreements prohibiting them from discussing their use of the technology. In recent trials in Missouri and Maryland, prosecutors abruptly dropped cases after police officers declined to testify about the role the devices played in the arrests, according to lawyers and privacy advocates.

But after repeated criticism from members of Congress about the secret use of the technology, the Justice Department this month announced new guidelines that in most circumstances require F.B.I. and other federal agents to obtain search warrants before they use StingRays and prohibit agents from using the devices to collect emails, texts and other data from cellphones. Data obtained from the bystanders’ phones must be discarded at the end of each day.

The surveillance devices “are a really critical tool for us that we use in a variety of contexts,” said Sally Q. Yates, the deputy attorney general at the Justice Department, at a news conference this month announcing the new guidelines. “There’s a real legitimate interest in not letting out the details of

exactly how this works so sophisticated criminals and organizations can't then figure out how to defeat it."

"Would it be better for law enforcement if we didn't give up any of this information?" she continued. "Yeah, it probably would. But there's also an interest in transparency and in public confidence as well. We're trying to find the balance."

The directive does not cover local police departments, where agencies in at least 21 states use StingRays or similar devices, according to the American Civil Liberties Union.

In a 2008 case in Florida, the Tallahassee police used a StingRay or a similar device to find James L. Thomas in a housing complex. The police suspected him of raping a woman and stealing her purse, which contained the woman's cellphone.

"Using portable equipment, we were able to actually basically stand at every door and every window in that complex and determine, with relative certainty you know, the particular area of the apartment that that handset was emanating from," a police officer testified, according to court records.

But when Mr. Thomas's girlfriend opened the door and asked whether the officers had a search warrant, they forced their way inside, according to court documents. The police department later said it had not obtained a search warrant because officers did not want to reveal their use of the technology; they had signed a nondisclosure agreement with the F.B.I., according to the court records.

Mr. Thomas was convicted of sexual battery and theft. A judge later ruled that the search had been illegal and ordered a new trial.

In Baltimore, the public defender's office said it was examining hundreds, potentially thousands, of cases in which the police used StingRays without

telling defense lawyers. In all, the Baltimore police have acknowledged using StingRays 4,300 times since 2007.

Natalie Finegar, the deputy district public defender in Baltimore, said that when defense lawyers pressed for details about how the police located certain suspects, prosecutions had suddenly been withdrawn to avoid answering questions about StingRays.

“There are cases where it was never spelled out for the judge, and certainly not for us,” Ms. Finegar said. “Sometimes they dropped cases and other times they would say, ‘We’re not going to use that evidence.’ We didn’t think it was used very often at all. We had no idea.”

The United States Supreme Court has not yet taken a case challenging whether the use of StingRays by the police without search warrants violates the Fourth Amendment’s protections against unreasonable searches.

But in recent years, the court has ruled that the police must obtain a search warrant to either place a GPS device on a vehicle or to sift through the contents of a suspect’s cellphone.

The person who has perhaps been the most successful in pressing for public disclosure about StingRays is a 35-year-old Arizona man who was arrested after federal agents located him using similar technology.

The man, Daniel Rigmaiden, pleaded guilty to tax fraud in 2014; the authorities said he used the names of dead people and others to file $5.2 million in fraudulent tax claims. In an interview this month, he said that after his arrest in 2008, he told a lawyer, “I think they tracked me down by sending rays into my living room.”

“In retrospect, I can see how it might sound like something a crazy person might have come up with,” Mr. Rigmaiden added.

In his case, it turned it out to be true. At the time, the existence of

StingRays was still a closely held government secret.

Soon after, his lawyer — at least his fourth one — withdrew from the case; eventually Mr. Rigmaiden represented himself and spent nearly six years in prison. Before he pleaded guilty, he began researching StingRays, setting up shop in the prison library and collecting more than 40,000 pages of documents before finding a reference in a government report to the device.

His research helped convince the A.C.L.U. that federal agents had and were using the technology. Since then, the group has led efforts to investigate and change government use of the device. Mr. Rigmaiden volunteered with the A.C.L.U. as part of his community service requirement after his release from prison.

This year, Mr. Rigmaiden, who has become a privacy advocate, helped Washington State write its StingRay law, and he has also taught criminal defense lawyers how to challenge the use of the technology, the A.C.L.U. said.

In Utah, Ryan Wilcox, a former Republican state legislator who sponsored that state's StingRay law, said in an interview that he had been able to convince his colleagues of the potential danger of the warrantless use of StingRays in a new way: He used equipment he had bought at a local store to project the contents of his cellphone onto a conference room wall.

"Are you comfortable having all your information — your contacts, your appointments, your photos — this easy to access?" he asked them.

The legislation passed overwhelmingly.

A version of this article appears in print on September 29, 2015, on page A12 of the New York edition with the headline: Covert Electronic Surveillance Prompts Calls for Transparency .