Court File No. DES-1-16

FEDERAL COURT

BETWEEN:

THE BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

Respondent

- and –

THE ATTORNEY GENERAL OF CANADA

Applicant

RESPONDENT'S SUBMISSION ON THE APPLICANT'S SECTION 38 *CANADA EVIDENCE ACT* CLAIM

David J. Martin
Martin + Associates
863 Hamilton Street
Vancouver, BC V6B 2R7
(t): 604-682-4200
(f): 604-682-4209
(e): reception@martinandassociates.ca

Counsel for the Respondent
The British Columbia Civil Liberties Association

Court File No. DES-1-16

FEDERAL COURT

BETWEEN:

THE ATTORNEY GENERAL OF CANADA

Applicant

- and –

THE BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

Respondent

RESPONDENT'S SUBMISSION ON THE APPLICANT'S SECTION 38 *CANADA EVIDENCE ACT* CLAIM

PART I – FACTS

A. History of Proceedings

1. On October 27, 2014, the Respondent British Columbia Civil Liberties Association (the "BCCLA") filed a Statement of Claim seeking a declaration that ss. 273.65 and 273.68 (the "impugned provisions") of the *National Defence Act*, R.S.C. 1985, c. N-5 (the "*NDA*") unjustifiably infringe s. 8 of the *Canadian Charter of Rights and Freedoms* (the "*Charter*"), Part I of the *Constitution Act, 1982* being Schedule B to the *Canada Act, 1982*, c. 11, and are thus of no force and effect. The Respondent also seeks declarations that Authorizations to intercept private communications and Municipal Directives

to gather metadata issued pursuant to the Act unjustifiably infringe both s. 2(b) and s. 8 of the *Charter*.

2. On November 26, 2014, the Applicant Attorney General of Canada (the "AGC") filed a Response to Civil Claim. The Applicant has disclosed some documents deemed by it to be relevant to the action. On December 22, 2015, counsel for the Department of Justice provided a Notice to the Attorney General of Canada pursuant to s. 38.01(1) of the *Canada Evidence Act* (the "*CEA*") advising that she was required to disclose potentially injurious information. On January 8, 2016, the Attorney General of Canada, through her delegate, rendered a decision claiming that 201 redacted documents contained sensitive or potentially injurious information as defined under section 38 of the *CEA*.

B. Evidence led on the s.38 Application

3. The Applicant AGC has filed three public affidavits in support of its application seeking an order upholding the validity of the AGC's redactions to the disclosed documents ("the redactions"). Michel Guay, the Acting Director General of the Counter Intelligence and Counter Proliferation Division of the Canadian Security Intelligence Service ("CSIS") swore his affidavit on February 25, 2016. Robert Sinclair, Executive Director, Threat Assessment and Intelligence Services Division at the Department of Foreign Affairs, Trade and Development ("DFATD"), affirmed his affidavit on February 24, 2016. Scott Millar, Director General of Strategic Policy and Planning at the Communications Security Establishment ("CSE") affirmed his affidavit on February 25, 2016.

4. As summarized in the Applicant's public submission, Messrs. Guay, Sinclair and Millar described in their affidavits how their respective organizations function and advanced general principles in support of the Applicant's position

that the redactions should be maintained. On June 1 and 2, 2016, Messrs. Guay, Sinclair and Millar were subject to cross-examination on their affidavits.

5. The Respondent BCCLA filed an affidavit prepared by Professor Craig Forcese (the "Forcese Report") that was affirmed on April 29, 2016. On May 27, 2016, Professor Forcese affirmed a supplementary affidavit (the "Supplementary Forcese Report") describing the significance and effect of additional documents disclosed by the AGC on May 17, 2016. In his affidavits, Professor Forcese summarized the information already publically available relating to CSE's mandate and metadata activities, as well as the metadata collection activities of non-Canadian Five Eye (US, UK, Australia and New Zealand) signals intelligence services. The Applicants were availed of an opportunity to cross-examine Professor Forcese on his affidavits, but declined to so.

PART II – ISSUES

A. What is the applicable legal test on a section 38 *CEA* application?

B. Is the redacted material relevant to the adjudication of the Constitutional Questions raised in the Respondent's statement of claim?

C. Would disclosure of the redacted material be injurious to international relations, national defence or national security?

D. Does the public interest in disclosure outweigh the public interest in non-disclosure?

PART III – ARGUMENT

A. The legal test

6. Section 38.06 of the *CEA* is the operative section that this Court must apply in determining whether to uphold the Applicant's s. 38 objection to making full disclosure of all relevant documents:

> 38.06 (1) Unless the judge concludes that the disclosure of the information or facts referred to in subsection 38.02(1) would be injurious to international relations or national defence or national security, the judge may, by order, authorize the disclosure of the information or facts.
>
> (2) If the judge concludes that the disclosure of the information or facts would be injurious to international relations or national defence or national security but that the public interest in disclosure outweighs in importance the public interest in non-disclosure, the judge may by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any injury to international relations or national defence or national security resulting from disclosure, authorize the disclosure, subject to any conditions that the judge considers appropriate, of all or part of the information or facts, a summary of the information or a written admission of facts relating to the information.

7. On an application made pursuant to section 38.04 of the *CEA,* this Honourable Court will be guided by the Federal Court of Appeal's decision in *Canada (AG) v. Ribic.*[1] First, the Court will determine the relevance of the information in issue; second, the Court will determine if disclosure of the information would result in injury to national security, national defence or international relations; third, if the Court finds that disclosure would result in injury, it must determine whether the public interest in disclosure outweighs the public interest in non-disclosure.

---

[1] 2003 FCA 246 at paras.17-21

8. For the reasons detailed herein, it is the Respondent's respectful submission that, in general terms (subject to some very specific exceptions), the AGC's redactions should not be upheld. The disclosed documents are clearly relevant to the nature and extent of governmental intrusions on Canadians' reasonable expectations of privacy, which is the central issue in this litigation. Much of what is sought to be redacted is already in the public domain as a result of comparable litigation in other jurisdictions and as a result of the voluntary disclosures that the AGC has elected to make in this case. In addition, the Respondent does not seek the disclosure of information that would tend to reveal sources, targets or the identity of national security or intelligence, nor does the Respondent seek the granular details of specific operations or the specific no doubt evolving technologies that underpin investigative techniques. It is therefore difficult to identify how disclosure of the information sought, namely general information about the extent to which Canadians' privacy rights have been and are being violated, could be injurious to national security. The fact that full disclosure of the scope of CSE's activities might be met with an unfavorable response from Canadians or otherwise be embarrassing to Government interests does not mean it will be injurious to national security interests. It is respectfully submitted that as this case addresses the fundamental *Charter* rights of all Canadians the public interest in disclosure clearly outweighs the government's residual interest in the non-disclosure of the full details of CSE's operations, particularly, as here, where the information in question also reveals unlawfulness and *Charter* violations committed by CSE in carrying out its activities.

B. The redacted material is clearly relevant to the Respondent BCCLA's action

(i) The BCCLA's Claim

9. The Respondent BCCLA challenges the constitutionality of both CSE's interception of private communications and CSE's collection, use, retention,

domestic sharing and international dissemination of metadata. As detailed in the BCCLA's Statement of Claim, it submits that the impugned provisions of the *NDA* and Authorizations issued pursuant to the *NDA* violate both sections 2(b) and 8 of the *Charter*. For the purpose of this application, it is important to understand the Respondent Plaintiff's position on the merits of its Claim and the Applicant Defendant's Response to the Claim so as to identify the issues in contention and thus the evidence that will be relevant to the adjudication of the Claim.

(ii) Section 8 of the *Charter* generally

10. Ever since the Supreme Court of Canada's 1984 watershed decision in *Hunter v. Southam Inc.*[2] interpreting the meaning and effect of Charter s. 8, and striking down provisions of the *Combines Investigation Act* which purported to authorize the issuance of a form of "ministerial search warrant", it has been universally accepted that before the Government can search for or seize anything in relation to which a Canadian has a reasonable expectation of privacy the Government must have made an application to an independent judicial officer. Such an application must be made under oath, setting out particularized grounds, appropriate to the context, describing why it is entitled to obtain a form of "judicial warrant" that is appropriately limited to the circumstances and to the requirements of the statutory scheme which authorizes and conditions the search.

11. As the purpose of s. 8 of the *Charter* is to protect citizens from unjustified governmental intrusions upon their privacy the *Hunter v. Southam* Court held that Charter s. 8 requires a means of preventing unjustified searches before they happen, not simply of determining after the fact whether they ought to have occurred in the first place.[3] Thus it has been well-settled in Canada, for

---

[2] [1984] SCJ No 36
[3] *Hunter v. Southam, supra* at para. 27

more than three decades, that a system of prior authorization by way of "judicial warrant", is a fundamental precondition to a valid interception of "private communications", to a search for and seizure of the private data and records of Canadians and to compliance with *Charter* s. 8. Accordingly, (absent exigent circumstances and other inapplicable and tightly controlled situational related exceptions) all interceptions and searches without "judicial warrant" are presumed to be unreasonable and violative of *Charter* s. 8. All Canadian government agencies are subject to the judicial warrant requirement, including the Canadian security and intelligence community. CSIS is of course subject to precisely this judicial control.[4] Justice Noel succinctly described the reasons why even national security investigations must be made subject to judicial control in *Re Canadian Security Intelligence Service Act*, at para. 28:

> Warrants granted under the CSIS Act are extraordinary, intrusive, related to open-ended investigations, information-oriented with an emphasis on investigation, analysis and the formulation of intelligence...Because of the nature, invasiveness and sensitivity of the activities of CSIS, its modes of operations must be subject to a complete closed system of control by the judiciary. [5]

12. CSIS is subject to judicial control and there is no reason why CSE should not be. Indeed, because a significant component of CSIS's activities are already carried out by CSE on its behalf pursuant to NDA s. 273.63(i)(c) this Court already indirectly reviews CSE's activities. Pragmatic national security "system-wide" policy considerations strongly support comprehensive, rather than "stove-pipe", command and control. In sum, it is the Applicant's position on the underlying Claim that this Court should assume direct control of CSE's operations rather than permit the continuation of *ad hoc* indirect control that now exists to some limited degree. And, of course, the Respondent

---

[4] *Canadian Security Intelligence Service Act* R.S.C., 1985, c. C-23, Part II

[5] [2008] F.C. 300 at para.28

emphasizes that this is not merely a sound policy choice but that that sound policy choice is also explicitly required by the constitution of Canada including s. 8 of the Charter.

(iii) The Interception of Private Communications Dimension of the Claim

13. Canadian courts have also long recognized that there is a heightened expectation of privacy in private communications. In 1990, in *R. v. Duarte,* the Supreme Court of Canada spoke of the "insidious danger" inherent in allowing the state to make surreptitious recordings of its citizens' conversations, holding: "If the state were free, at its sole discretion, to make permanent electronic recordings of a person's private communications, there would be no meaningful residuum to the right to live free from surveillance." [6] These principles have been reiterated and amplified by the Supreme Court in cases like *R. v. Morelli* [7], *R. v. Tse*[8], *R. v. Cole* [9] *R. v. Telus Communications* [10] and most recently *U.S. v. Wakeling.* [11]

14. Accordingly, Part VI of the *Criminal Code of Canada* makes it an offence to willfully intercept a private communication by means of any electro-magnetic, acoustic, mechanical or other device. Such conduct is an indictable offence punishable by up to five years imprisonment. There are exceptions granted for law enforcement agents acting pursuant to a judicial warrant authorizing the interception.[12]

15. In 2001, the *National Defence Act* was amended to codify CSE's private communication interception powers. Pursuant to Mandate A, the collection of

---

[6] [1990] SCJ No 2
[7] [2010] SCJ No 8
[8] 2012 SCC 16
[9] 2012 SCC 53
[10] 2013 SCC 16 at para. 31
[11] [2014] 3 SCR 549 at para. 38
[12] *Criminal Code of Canada* R.S.C., 1985, c. C-46, s.184

foreign signals intelligence, CSE is now statutorily authorized by section 273.65 to intercept Canadian private communications and is exempt from Part VI *Criminal Code* liability by section 273.69 provided that the interception in issue was authorized by the Minister of National Defence. Pursuant to s.273.65, as a pre-condition to the issuance of a Ministerial Authorization aimed at intercepting private communications "in relation to an activity or class of activities" the Minister simply has to "be satisfied" that the interception is "aimed at" foreign entities and that "satisfactory measures" are in place to protect the privacy of Canadians.[13] The Minister's "authorizations" are highly generic and generalized and there is no question that in its pursuit of foreign intelligence, CSE intercepts the private communications of Canadians.[14] There is absolutely no judicial oversight of CSE's interception of private communications. Instead the CSE Commissioner merely reviews on an ex post facto basis CSE's activities carried out under an authorization issued under this section to ensure that they were in fact generally "authorized" and reports annually to the Minister on the review.[15]

16. It is the Respondent's position that the impugned provisions of the NDA which permit CSE to intercept the private communications of Canadians are unconstitutional because they are not subject to prior judicial authorization, nor to any form of direct judicial oversight whatsoever. Nor are they generally subject to any effective *ex post facto* accountability mechanism. In *Tse*, supra, the Supreme Court of Canada considered the constitutionality of s. 184.4 of the *Criminal Code of Canada* which permitted a very circumscribed, warrantless interception of private communications in exigent circumstances where there was an immediate threat of serious bodily harm and prior judicial authorization was practically unavailable. The Court held that while it was open to parliament in principle to enact laws that forego prior judicial authorization for

---

[13] *National Defence Act* R.S.C., 1985, c. N-5, ss.273.65
[14] Applicant's Response to Civil Claim, p. 5, para. 16
[15] *National Defence Act* R.S.C., 1985, c. N-5, ss.273.65

the interception of private communications in very limited exigent circumstances, s. 184.4 violated s. 8 of the Charter because it did not provide adequate mechanisms for oversight. At para. 89, Justices Moldaver and Karakatsanis for the Court held:

> "Accountability on the part of those who intercept private communications under s. 184.4 without judicial authorization is an important factor in assessing the constitutionality of s. 184.4."

17. As the NDA does not contain notice provisions equivalent to those required by Code s. 196 any Canadian whose private communications have been intercepted at CSE's discretion pursuant to the generic Ministerial Authorization disclosed in these proceedings will likely never know that this has occurred and thus will be unable to pursue measures to seek to hold CSE to account for their invasive activity. The Respondent resists any assertion that the Applicant may ultimately make to the effect that a CSE regime that involves judicial oversight would be practically unworkable. As detailed in the Forcese Report, in the United States, where the NSA seeks to collect communications data that is intermingled in data streams with American origin or destined communications, the *FISA Amendments Act* 702 process permits targeted, warrantless foreign personal data collection (in which US person data may be inadvertently or incidentally collected, but cannot be targeted). But this collection is supervised by the Foreign Intelligence Surveillance Court ("FISC"), which is charged with approving and reviewing the targeting and information retention/minimization procedures.[16] Further support for a regime that requires judicial authorization for CSE's interception of the private communications of Canadians and judicial oversight of privacy safeguards relating to the collection, use, retention, domestic sharing and international distribution of those communications may also be found in the pragmatic

---

[16] The Forcese Report, at para. 58

"model" for implementing judicial control of CSE contained in Bill C-622, The "*CSE Accountability and Transparency Act*" tabled by Liberal Member of Parliament Joyce Murray in November 2014.[17]

18. The Applicant's Response to Civil Claim at paras. 7-9 contends that any gathering of information in which a Canadian has a section 8-protected reasonable expectation of privacy which may occur as a result of the impugned provisions is reasonable because it is "authorized", in furtherance of "important government objectives", and is "minimally intrusive" because of the privacy safeguards imposed. Alternatively, the Applicant pleads that section 8 violations are justifiable under section 1 of the *Charter*, again claiming that the "incidental" interception of Canadians' private communications "minimally impairs any *Charter* protected rights affected" because of the privacy safeguards that CSE self imposes.[18]

19. The Respondent submits that any information in the Applicant's possession that reveals: (a) the frequency with which Canadians' private communications have been intercepted; (b) the frequency with which Canadians' private communications that have been "incidently" intercepted are retained, the policy reasons for such retentions, and the duration of those retentions; and (c) the frequency with which Canadians' private communications have been disseminated to domestic or foreign agencies, and whether that information is minimized prior to dissemination, is all highly relevant, indeed essential, to the proper adjudication of the Plaintiff's claim.

(iv) The Metadata Dimension of the Claim

20. Metadata has been described as "digital crumbs" that reveal "time and duration of a communication, the particular devices, addresses, or numbers contacted,

---

[17] Bill C 622, *An Act to amend the National Defence Act (transparency and accountability), to enact the Intelligence and Security Committee of Parliament Act and to make consequential amendments to other Acts, was* defeated on December 5, 2014, by the 41st Parliament, 2nd Session

which kinds of communications services we use, and at what geolocations."[19] In the words of CSE Commissioner Plouffe:

> "While metadata does not reveal the content of communications, it nevertheless has the potential to reveal a great deal of information about individuals, including details about [redaction]. As such, it can be of foreign intelligence value in many scenarios, and can correspond to significant privacy considerations in many others."[20]

21. The Supreme Court of Canada has long recognized that section 8 of the *Charter* extends to the protection of all core biographical information. More than 20 years ago, in 1993, in *R. v. Plant,* Justice Sopinka for the majority stated:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s.8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[21]

22. Accordingly, the Supreme Court has had no difficulty whatsoever in finding that section 8 protections extend to video surveillance [22], tracking devices used to monitor the movement of the citizenry [23], "the electronic roadmap" of internet activity retained in personal computers [24] as well as in work-place computers [25]. In *R. v. Cole,* speaking for the majority of the Court, just three years ago, Justice Fish held:

---

[18] Applicant's Response to Civil Claim dated January 20, 2014
[19] Ann Cavoukian, *A Primer on Metadata: Separating Fact from Fiction* (Information and Privacy Commissioner, Ontario, July 2013) at 3.
[20] OCSEC Review Report at 8
[21] [1993] 3 S.C.R. 281, at p. 293
[22] *R. v. Wong* [1990] SCJ No 118
[23] *R. v. Wise* [1992] SCJ No 16
[24] *R. v. Morelli, supra* at para. 3
[25] *R. v. Cole, supra* at paras. 2-3; *R. v. Vu* 2013 SCC 60

> Computers that are reasonably used for personal purposes — whether found in the workplace or the home — contain information that is meaningful, intimate, and touching on the user's biographical core. ***Vis-à-vis* the state, everyone in Canada is constitutionally entitled to expect privacy in personal information of this kind.**
>
> While workplace policies and practices may diminish an individual's expectation of privacy in a work computer, these sorts of operational realities do not in themselves remove the expectation entirely: **The nature of the information at stake exposes the likes, interests, thoughts, activities, ideas, and searches for information of the individual user**. [Emphasis added]

23. On June 13, 2014, in *R. v. Spencer,* the Supreme Court of Canada affirmed that the section 8 rights of Canadians are not limited to the content of their communications and that the reasonable expectation in privacy includes the general right to anonymity. In that case, at issue was the question of whether there was a reasonable expectation of privacy in the subscriber information associated with an Internet Protocol address. The Court unanimously held that there was such an expectation of privacy and that the police had violated the accused's section 8 *Charter* rights when they seized that information without warrant. In doing so, the Court cited with approval the 2012 judgment of the Ontario Court of Appeal in *R. v. Ward,* in which Justice Watt had held:

> 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.[26]

24. Nonetheless, despite the fact that Canadians clearly have a reasonable expectation of privacy in respect of information revealed by their presence on the internet and in their dealings with the digital universe, the *NDA* does not even require the issuance of Ministerial Authorizations as a pre-condition to the collection, use and dissemination of this all revealing information. In fact, there is no explicit reference to metadata in the *NDA* provisions relating to

CSE. In sum, it is less than clear whether CSE's collection of the metadata of Canadians is in fact "authorized" by law. Support for this proposition is reflected by the fact that the CSE Commissioner has recently recommended "that the *NDA* be amended to provide a clear framework for CSE's metadata activities." [27]

25. For the reasons cited by the Supreme Court of Canada in *Spencer, supra,* and in numerous other cases cited herein that hold that core biographical information is subject to section 8 *Charter* protections, the Respondent BCCLA contends that metadata collected without warrant from Canadians is done in violation of their section 8 *Charter* rights, even if the provisions of s. 273.64(i)(a) of the Act can be said to authorize such collection. The Applicant's Response to the BCCLA's Civil Claim, somewhat amorphously states:

> "[W]hen metadata acquired and used by CSE is the subject of a reasonable expectation of privacy, CSE has privacy safeguards in place. Certain of the Metadata acquired and used by CSE is not subject to a reasonable expectation of privacy."[28]

26. In adjudicating the underlying action, it will be necessary for this Honourable Court to make the first factual determination necessary to every section 8 *Charter* analysis, namely whether there is a reasonable expectation in privacy engaged in relation to that which is "seized"? The Applicant's position currently seems to be that they will not reveal what metadata CSE is intercepting, nor what they do with it, while simultaneously acknowledging the undeniable fact that some of the metadata it collects engages significant privacy interests. Clearly the disclosure that the Respondent seeks in this respect is relevant to the underlying action.

---

[26] *R. v. Spencer* 2014 SCC 43 at para.43; *R. v. Ward* 2012 ONCA 660 at para. 71

[27] Commissioner Plouffe's Report is Tabled in Parliament (January 28, 2016), at p. 3 of PDF, exhibit 34 to the Forcese Report

[28] Response to Civil Claim at p. 12, para. 6

27. The Respondent submits that any information in the Applicant's possession that reveals the following is relevant and should be disclosed:

(a) what types of metadata (non-content information in which Canadians have a privacy interest) is being intercepted by CSE;

(b) the volume of material being intercepted;

(c) whether these interceptions are being gathered in bulk,effectively indiscriminately (or without targeting);

(d) whether these interceptions include Canadian origin and terminus data;

(e) what use is made of this information;

(f) how this information is retained and for how long;

(g) the policy reasons underpinning such retentions;

(h) the duration of those retentions;

(i) the frequency and manner with which this information is being disseminated to domestic agencies;

(j) the frequency and manner with which this information is being disseminated to foreign agencies, and

(k) whether and to what extent the information is minimized prior to dissemination;

(v) Relevancy is a Low Threshold

28. As the Federal Court of Appeal held in *Ribic,* the first task of a judge hearing a section 38 *CEA* application is to determine whether the information sought to be disclosed is relevant or not. In *Ribic* this was described as "undoubtedly a

low threshold."[29] In *AGC v. Almalki et al,* Justice Mosley further refined the test for relevance in the context of the civil discovery process and the Respondent contends that this is the test that this Honourable Court must apply in this case:

> As the underlying matters in this case are civil actions, I think it appropriate to apply the standard of relevance as it relates to the discovery process in civil litigation. **In the Federal Court, information is relevant for discovery purposes if it may reasonably be useful to the party seeking production to advance its case or undermine that of the opposing party or may fairly lead to a "train of inquiry" that may have either of these two consequences: Rule 222(2)** *Federal Court Rules*, SOR/98-106; *Apotex Inc. v. Canada*, 2005 FCA 217 (CanLII), 337 N.R. 225 at paras. 15-16. The *Apotex* approach to relevance has been applied in Ontario, under the former rules: see for example *Benatta v. Canada (Attorney General),* [2009] O.J. No. 5392 at para. 20. **This conception of relevance applies not only to information that is direct evidence supporting the respondents' allegations but also to information that will permit inferences of fact to be drawn from the circumstances.**[30] [emphasis added]

29. As the Applicants in this case have conceded that the material that is the subject of this application would otherwise need to be disclosed pursuant to its discovery obligations, there should be no dispute that the redacted documents meet the low relevancy threshold. Nonetheless, as Justice Noel recognized in *Arar*, "sometimes the more relevant the redacted information, the greater the public interest in disclosure; and conversely, sometimes the less relevant the redacted information, the less the public interest in disclosure."[31] In this manner "relevance" is an important consideration to be weighed against other factors in making a final determination regarding disclosure. For this reason, the Respondent will attempt to detail the potential relevance of the redacted information.

---

[29] Supra at para. 17
[30] 2010 FC 1106 at para.61
[31] *Canada (AG) v. Commission of Inquiry in the Actions of Canadian Officials in relation to Maher Arar,* 2007 FC 766 at para. 45

(vi) The Material the Respondent seeks is Highly Relevant to the Adjudication of the Claim

30. As a preliminary matter the Respondent takes issue with the accuracy of the Applicant's assertions at paras. 128 and 155 of their Public Submissions to the effect that the Respondent has somehow "conceded" that certain categories of information are irrelevant to the underlying action. The Respondent has properly conceded that its claim does not reach to CSE's Mandate C activities. The BCCLA Claim did not include these activities because, as this Honourable Court observed at the Ottawa hearings on June 1 and 2, 2016, and the Respondent's witnesses seem to confirm, those activities will have been the subject of prior judicial authorization.[32] However, the Applicant also attributes to counsel for the Respondent broader statements which it now says limit its disclosure obligations. For example, counsel's comment during the examination of Mr. Millar regarding the "lawsuit not being about Mandate B" was made in the context of curbing Mr. Millar's unsolicited testimony with respect to the volume of cyberattacks that CSE defends daily.[33] It was not intended to be, nor should it be interpreted as, a waiver of the right to disclosure of information that is relevant to the analysis of whether Canadians' privacy rights are being violated as a result of unwarranted interceptions or the collection of private data made in furtherance of Mandate B purposes.

31. Similarly, while counsel for the Respondent repeatedly told the Court at the Ottawa hearings that he just wanted to know "what information is gathered, how its stored, to who its distributed and on what terms", and that he did not want to know anything about the targets of the investigations, ongoing operations, agency employees[34] or techniques associated with the management of the repositories,[35] his comments in this respect should not be interpreted in

---

[32] *Transcript of Proceedings, June 1, 2016,* pages 31, 32, 41; *Transcript of Proceedings, June 2, 2016,* page 213
[33] *Transcript of Proceedings, June 1, 2016,* page 109
[34] *Transcript of Proceedings, June 1, 2016,* page 140
[35] *Transcript of Proceedings, June 2, 2016,* page 197

the broad manner the Applicant suggests, namely that "the Respondent has conceded that operational, investigative technique and employee-specific information is not relevant to the underlying proceeding." [36]

32. Contrary to making explicit concessions limiting disclosure, during the Ottawa hearings counsel for the Respondent repeatedly advised this Honourable Court that he would be preparing a list to be delivered during this oral hearing that would delineate the disclosure that he believes is necessary to the adjudication of the BCCLA's action brought on behalf of the public.[37] As the Respondent does not know what information has been redacted, the following list should not be interpreted as an explicit or implicit waiver of a right to disclosure of all relevant documentation in the Respondent's possession. This list is however the Respondent's attempt to identify information, not yet disclosed, that the Respondent insists is highly relevant, and indeed necessary, for the adjudication of this Claim and the Constitutional Questions raised therein:

(a) The means by which the metadata of Canadians is collected

Mr. Millar confirmed at transcript p. 166, l. 21 to 27 that:

Q. CSEC gathers Canadian metadata.
A. Yes.
Q. ...and sorts it later?
A. When we collect it, we try and do it in a way that's targeted and afterwards, if we have looked at it and identified it Canadian, then we deal with it as per the law in our procedures.

And at transcript p. 171, l. 11 to 19 that:

Q. But for the purposes of this proceeding will you acknowledge that CSEC gathers – let's call it "Canadian metadata" – so that it can subsequently analyse it?
A. We do absolutely collect Canadian metadata in foreign matters.
Q. Okay.

---

[36] Public Submissions of the AGC at para.155
[37] *Transcript of Proceedings, June 1, 2016,* pages 29, 30, 62-64

A. ... in support of our foreign intelligence matters.

If CSE collects metadata "at all SIGNIT collection apertures for all telecommunication events" as described by the Commissioner at page 9 of his March 31, 2015 Confidential Report to the Minister ("the March 31, 2015 Report") then this should be disclosed, especially if it is done without notice to the owners of "the SIGNIT appetures" utilized. If notice is given to such owners and a demand made pursuant to the *NDA* s.273.64 (1) (a) then this completely innocuous fact, at least from a national security perspective, should also be disclosed. *CEA* s. 38 was never designed to permit the suppression of either improper or innocuous conduct.

(b) The types of metadata collected by CSE

In order to evaluate whether CSE has violated Canadians' reasonable expectations of privacy, this Honourable Court needs to know precisely what type of information is being gathered. Accordingly, the Respondent seeks full disclosure of the types (or "fields") of the metadata of Canadians collected or otherwise obtained by CSE, including metadata that (a) domestic partners, (b) foreign partners, or (c) private-sector organizations share with or otherwise make available to, or searchable by, CSE.

As noted in Table 1 of the primary Forcese Report, at para. 73, some "examples" of the types of metadata obtained by CSE have been disclosed, but this list is far from exhaustive and subject to numerous redactions.

(c) The volume of the information collected

In order to evaluate the scope, scale and significance of a potential violation of Canadians' privacy rights (and to adjudicate the section 1 justification defence raised by the Applicant), this Honourable Court needs to know the scale of CSE's surveillance activities. Accordingly, the Applicant seeks disclosure of the volume of private communications of Canadians that are allegedly "incidentally" collected, and the current daily average volume of metadata (a) collected or otherwise obtained per day by CSE and held permanently or temporarily in CSE repositories or other forms of data storage, and (b) collected or otherwise obtained per day by domestic private sector or foreign partner agencies and held permanently or temporarily in repositories or other forms of data storage shared with, or otherwise made available to, or searchable by, CSE.

As detailed at paragraph 74 of the Forcese Report, CSE is known to obtain metadata "in huge volumes", but no figures have been disclosed, albeit that Appendix D to the Commissioner's March 31, 2015 Report may contain such statistics.

(d) The percentage of the metadata collected that is Canadian

Similarly, germane to a determination of both whether the search is reasonable, and to its potential impact on privacy rights, is the extent to which the metadata collected by CSE relates to communication in which both ends are in Canada and to one end in Canada involving a "Canadian" as that term is defined by the Act. Accordingly, the Respondent seeks disclosure of the percentage (or very best estimate thereof) of metadata held permanently or temporarily in each of the above categories (CSE, domestic partner, foreign partner, private sector) of repository or other forms of data storage that concern communications to, from, or associated with Canadians.

(e) The retention of intercepted information

In order to determine the extent to which the privacy rights of Canadians have been violated, this Honourable Court needs to know how long this data is held. Following on the Supreme Court of Canada decision in *R. v. Colarusso*, it has become well established that the retention of seized information engages s. 8. See S. Hutchison et al, *Search and Seizure Law in Canada (*Toronto: Carswell, 2005) at p. 18-1;

> It is only during the ongoing detention that the governmental intrusion into the privacy interests of the individual are realized. It is detention which allows examination, copying and forensic testing. These aspects of the seizure as much as the initial search itself, would seem to engage the interests of the individual which s. 8 of the Charter was intended to protect. As such, the ongoing detention should meet the same constitutional standard that the original seizure is measured against, that is, reasonableness.

Accordingly, the Applicant seeks disclosure of the maximum retention period(s) specified in CSE policy for all metadata held in CSE repositories or other forms of data storage.

As discussed in paras. 92-96 of the Forcese Report, these retention periods have been redacted from the materials released. The continuing growth in CSE data storage capacity raises the possibility that increasingly large volumes of data will be stored for increasingly long periods as time goes on and the storage capacities of computers continues to evolve exponentially.

In addition, as discussed in para. 92 of the Forcese Report, the Minister of National Defence can grant permission to CSE to retain some data for longer than the maximum period. No disclosure has been released detailing the

number and length of such extensions, if any, or the types of metadata that is the subject of such retention extension determinations.

(f) CSE "use" procedures

In order to assess CSE's use of the metadata that it acquires this Court requires an understanding of the types of metadata analyses undertaken by CSE and the nature of these analyses. Obviously such information is relevant to assess CSE's "search" of the information that it has "seized", (applying the lexicon of Charter s. 8) which in turn informs the assessment of the privacy implications of CSE's metadata activities. Accordingly, we seek disclosure of a general description of the manner in which CSE generates its intelligence reports including whether contact chaining and profiling methods are undertaken.

(g) Metadata-*like data*

The Respondent also submits that this Honourable Court also needs the equivalent information for all of the above subjects and categories for data types that would be considered by CSE to be metadata if they were associated with a specific telecommunication, e.g., "Identifiers in isolation, in address books, on buddy lists", including the source(s) of this data, and the use, retention, and procedural rules pertaining to it,.as discussed in Table 1 of the Forcese Report.

(h) Information sharing

To determine the nature and extent of the breaches of Canadians' reasonable expectations of privacy, this Honourable Court will need to know whether CSE disseminates the private information that it gathers from its citizens to other government agencies, domestic or foreign. And if this private information is so disseminated, pursuant to what conditions? Accordingly, the Respondent seeks disclosure of the types (i.e., "fields") and volumes of metadata and the percentage of that metadata that is associated with Canadians that CSE shares or has shared with or otherwise has made available to or searchable by (a) domestic partners and (b) foreign partners. The Respondent also seeks full disclosure of the minimization techniques employed by CSE to protect the privacy interests of Canadians and all of the particulars of the Commissioner's determination of CSE's failings in this respect as described in the March 31, 2015 Report.

As domestic and international "sharing" or "distribution" give rise to different considerations they are properly considered separately:

Domestic Distribution

Mr. Millar described in detail, (at transcript pg. 204, l 10 to 214, l. 10), the process by which CSE "shares" metadata with domestic law enforcement agencies. As will be elaborated in more detail infra, that description very well illustrates the profound ineffectiveness of the NDA non-Charter compliant CSE processes. To use the witness' reference to the tree and fruit metaphor, it is obvious that if CSE provides an intelligence report to one of the other Canadian national security apparatus actors that is based upon metadata collected by CSE that is not collected in a Charter compliant manner then the recipient agency may well be commencing its follow on investigation based upon "poisoned fruit". Of course if recipient agencies base their warrant applications upon such material the most apt analogy is that CSE is actually providing poisoned fruit as the very seed from which the recipient agency would then hope to grow a tree (a poisoned tree) of enforcement.

In the result, it is respectfully submitted that all information related to this domestic sharing process is highly relevant as its granular detail will conclusively demonstrate that all of the AGC's Charter s. 1 justifications are utterly meritless as no free and democratic society could ever rationally design a multi-agency national security and intelligence system that has such a profound institutional flaw at its very heart.

International Distribution

As the Commission's March 31, 2015 Metadata Report and his follow on October 5, 2015 Legality Report provide some insight into CSE's metadata collection, use, retention and domestic and international disclosure processes, the Respondents respectfully submit that all of the Commissioner's findings respecting CSE's activities are highly relevant to the full and effective adjudication of this case. The Commissioner's findings are relevant as they are both the product of the statutory review process mandated by the NDA s. 273.63 itself and because Mr. Millar has testified (at transcript pg. 115, l. 13 to pg. 117, l. 10) that CSE "has no reason to question any of the findings or analysis that the Commissioner has made".

As to the "other" documents disclosed by the Applicant, as detailed in para. 117 of the Forcese Report, the Respondent has to date also not received any disclosure of CSE policies with regard to retaining records of the metadata shared with foreign partners. Other than the very broad categories of DNR and DNI metadata, no details have been provided regarding the types, volumes, and percentage of the metadata associated with Canadians that has been made subject to un-minimized international sharing.

AGC 278 states that "Any metadata fields that could be analyzed and correlated with other information to identify a Canadian (e.g. phone numbers) are considered to be CII" and therefore must be minimized. But where is the line drawn in practice? Are all metadata fields that could be used to uniquely identify a communicant or a machine, given the availability of sufficient collateral information, minimized? Are steps taken to ensure that a foreign partner cannot invoke technological devices to "re-identify" the persons associated with the disseminated data? For the reasons discussed in para. 111 of the Forcese Report, it is important that for each metadata type requiring minimization, this Honourable Court fully understand the nature of the alteration required for that type to be considered "effectively minimized".

(i) Minimization Failings

As the Applicant's Statement of Defence pleads that Canadians' privacy rights have been negligibly or minimally impaired by CSE's activities because of the privacy safeguards CSE has imposed upon itself, it is imperative that this Court be given some meaningful disclosure as to what safeguards have been used and the sufficiency and effectiveness of those measures. The Applicant's position in this respect is of course significantly compromised where there is evidence that those safeguards have failed to ensure that information in which Canadians have a reasonable expectation of privacy is protected. This Honourable Court will want to examine those failings in great detail so as to assess whether "feather light" Ministerial control is adequate and whether CSE itself is capable of self governance..

As detailed in paras. 18-20 of the Supplemental Forcese Report, the Respondents have been provided very little information with respect to the types and volumes of metadata associated with Canadians that were improperly shared in un-minimized form with foreign partners as detailed in theMarch 31, 2015 Report. Other than the very broad categories of DNR and DNI metadata described no details of the types and volumes of the un-minimized metadata that has been indiscriminately shared has been disclosed. CSE has stated that it is unable to determine how much Canadian-associated metadata was improperly shared during these events. This assertion is unsettling as it suggests that the volume of private information being gathered is immense and that the dissemination of this information may similarly be utterly indiscriminate. Nonetheless, even accepting the veracity of CSE's assertion at face value, it the Respondent's submission that the redacted documents must at minimum contain material that would permit reliable inferences about the volume of Canadian metadata that was disseminated in an un-minimized form in violation of CSE's mandate.

As detailed in para. 100 of the Forcese Report, also undisclosed to date are the nature of the policies and procedures, if any, for un-minimizing metadata at the request of foreign partners. In particular, do such policies and

procedures differ from those pertaining to the release of suppressed CII in domestic SIGINT reports and, if so, how?

(j) Terminology

In order to understand the nature and extent to which Canadians' privacy rights are impacted by CSE's activities, it is important that the issues raised in paras. 7-12 and 17 of the Supplemental Forcese Report be answered through disclosure. As detailed therein, the CSE Commissioner has expressed concerns about the manner in which some key CSE terms are being defined: namely "collection", "acquisition" and "interception". This lack of clarity also extends to the language CSE uses for metadata that is collected *en masse* rather than through a targeted selection process. The latter is of course an important issue in this litigation because if CSE is in fact engaged in "bulk" or "unselected" collection of information in which Canadians have a reasonable expectation of privacy it constitutes a very significant violation of section 8. As detailed by Professor Forcese it was the disclosure of this type of collection that led to legislative reform in the United States. This type of collection could in fact include the interception of information which originated and terminated in Canada due to the complexity of information routing in the modern communications paradigm.

C. The Defendant's claims that disclosure would be injurious should be carefully scrutinized

(i) The AGC bears the burden of proof

33. Once this Honourable Court has determined that the redacted material is relevant, the burden shifts to the Attorney General of Canada.[38] The AGC must satisfy the reviewing judge that the injury alleged is probable, and not simply a possibility, or merely speculative.[39] In determining whether disclosure might potentially be injurious, this Court must be satisfied that executive opinions have a factual basis established by the evidence.[40] There must be some explanation of the linkage between disclosure of specific

[38] *Canada (AG) v. Kempo* [2004] FC 1678 at paras. 39 and 83.
[39] *Arar Inquiry, supra* at para. 49.
[40] *Khadr v. Canada* [2008] FCJ 770 at para.32; *Ribic supra* at para. 18; *Arar Inquiry, supra* at para. 47

information and harm to Canadian interests.[41] Information that is already in the public domain, including in circumstances where the Crown has disclosed documents in the course of litigation, is unlikely to cause injury.[42]

34. In the case at bar, the AGC will not be able to meet this burden of proof for much of the information withheld. First, for the reasons canvassed below, because the AGC has led no evidence capable of sustaining a factual, reasoned, non-speculative, detailed position that disclosure of the type of private information of Canadians that CSE is collecting and what it is doing with that information will somehow be injurious to national security. Further, as detailed in the Forcese Report, the information that the Applicant has refused to disclose is information that has already been either voluntarily disclosed, or is otherwise in the public domaingenerally describes what advanced democracies do in terms of digital intelligence interception. Disclosure of the fact that Canada engages in activities comparable to those that other advanced democracies employ could never be injurious to national interests.

35. The Respondent also urges this Court to be vigilant in ensuring that relevant disclosure is not suppressed based on exaggerated claims of national security threats. As the Supreme Court of Canada observed in *Canada v. Harkat*, this Court serves a vital role as the gatekeeper in guarding against this type of systemic overclaiming:

> The judge must be vigilant and skeptical with respect to the Minister's claims of confidentiality. Courts have commented on the government's tendency to exaggerate claims of national security confidentiality: *Canada (Attorney General) v. Almalki*, 2010 FC 1106 (CanLII), [2012] 2 F.C.R. 508, at para. 108; *Khadr v. Canada (Attorney General)*, 2008 FC 549 (CanLII), 329 F.T.R. 80, at paras. 73-77 and 98; see generally C. Forcese, "Canada's National Security 'Complex': Assessing the Secrecy Rules" (2009), 15:5 *IRPP Choices* 3. As Justice O'Connor commented in his report on the Arar inquiry,

---

[41] *K.F. Evans Ltd. v. Canada (Minister of Foreign Affairs)*, 1996 CarswellNat 37 (T.D.) at para. 34.
[42] *Arar Inquiry* at paras. 54-57; *Almaki, supra* at para. 81

> overclaiming exacerbates the transparency and procedural fairness problems that inevitably accompany any proceeding that can not be fully open because of [national security confidentiality concerns. It also promotes public suspicion and cynicism about legitimate claims by the Government of national security confidentiality.
>
> (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), at p. 302)[43]

(ii) Embarrassment does not constitute "injury"

36. This Court must be persuaded that disclosure of the redacted information will result in an "injury", or a damaging of national security interests.[44] If the government's primary purpose is to shield itself from criticism or embarrassment, then there is no "injury" under s. 38.[45]

37. This Court should guard against these positions in this case, particularly in light of the fact that we now know that CSE has failed for many years to properly minimize information seized from Canadians without warrant before sharing it with foreign governments. This Court needs to know the nature and extent of this section 8 violation and to date the Applicant has not disclosed detail that would permit this Honourable Court to understand the gravity of this systemic privacy breach. For example, other than the very broad categories of DNR and DNI metadata, no details of the types, volumes, and time periods involved have been disclosed. This information is of course critical to this Court's determination of whether the existing administrative oversight regime adequately safeguards Canadians' privacy as it professes to. CSE's "track record" in this respect much be the subject of scrutiny, and if the information sought is relevant it cannot be withheld simply because it would be

---

[43] 2014 SCC 37 at para. 63
[44] *Arar Inquiry* at paras. 51 to 52
[45] *Arar Inquiry* at para. 58.

"embarrassing". Given its applicability in this case, Justice Noel's comprehensive review in *Arar* of the jurisprudence that speaks to this issue is very helpful:

> As can be seen from the passage I have reproduced from *K.F. Evans Ltd*, above (at paragraph of this judgment), the Court will not prohibit disclosure where the Government's sole or primordial purpose for seeking the prohibition is to shield itself from criticism or embarrassment. This principle has also been confirmed by the Supreme Court in *Carey v. Ontario*, [1986] 2 S.C.R. 637 at paragraphs 84-85, where Justice LaForest, for the Court, wrote:
>
> > There is a further matter that militates in favour of disclosure of the documents in the present case. **The appellant here alleges unconscionable behaviour on the part of the government. As I see it, it is important that this question be aired not only in the interests of the administration of justice but also for the purpose for which it is sought to withhold the documents, namely, the proper functioning of the executive branch of government. For if there has been harsh or improper conduct in the dealings of the executive with the citizen, it ought to be revealed. The purpose of secrecy in government is to promote its proper functioning, not to facilitate improper conduct by the government.** This has been stated in relation to criminal accusations in *Whitlam*, and while the present case is of a civil nature, it is one where the behaviour of the government is alleged to have been tainted.
> >
> > **Divulgence is all the more important in our day when more open government is sought by the public. It serves to reinforce the faith of the citizen in his governmental institutions. This has important implications for the administration of justice, which is of prime concern to the courts. As Lord Keith of Kinkel noted in the *Burmah Oil* case, *supra*, at p. 725, it has a bearing on the perception of the litigant and the public on whether justice has been done.** [emphasis added]

Also of interest, Justice Mason of the High Court of Australia stated in his judgment in *Commonwealth of Australia v. John Fairfax & Sons Ltd.* (1980) 147 C.L.R. 39 at page 51:

> [...] But it can scarcely be a relevant detriment to the government that publication of material concerning its actions will merely expose it to public discussion and criticism. **It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss,**

> **review and criticise government action**. Accordingly, the court will determine the government's claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will be protected.[46] [emphasis added]

This passage was later cited with approval by Bingham L.J. and Lord Keith of Kinkel in their respective judgments in *Observer Ltd*, above.

The same principle has also been expressed in the *Johannesburg Principles: National Security, Freedom of Expression and Access to Information*, U.N. Doc. E/CN.4/1996/39 (1996), a tool for interpreting article 19 of the United Nations' International Covenant on Civil and Political Rights, which states at Principle 2(b):

> In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

Given the abundance of case law and legal documents advancing that information which is critical or embarrassing to the Government cannot be protected, there appears to me to be no reason to depart from the application of this principle.

(iii) The Respondent does not seek the disclosure of traditionally protected information

38. Disclosure has previously been found by this Honourable Court to be injurious within the proper construction of s. 38.04 where it would identify or tend to identify human sources, members of the intelligence service, targets of investigations, and technical data that would comprise the legal operations of intelligence agencies.[47]

---

[46] *Arar Inquiry,* paras.58-60

[47] *Kempo* at paras. 89 to 91; *Gold v. Canada*, 1986 CarswellNat 216 (Fed. C.A.) [Gold] at para. 18; *Henrie v. Canada (Security Intelligence Review Committee)*, 1988 CarswellNat 160 (F.C.T.D.), aff'd 1992 CarswellNat 194 (Fed. C.A.) [*Henrie*] at para. 31.

39. The Respondent does not seek this type of information. The Respondent's claim does not rest upon the identity of human sources nor upon the identity of members of the intelligence service. Other than disclosure of the number of CSE's targets the Respondent has no interest in the identity of the individuals and groups that CSE targets.. Similarly, apart from acquiring a general understanding of what types of private information is being collected and what is being done with this information, the Respondent likely has no interest in much of the information about the specific techniques employed by CSE.. Indeed, Mr. Millar conceded (at transcript pg. 136 l. 24 to 137, l. 8) that information about "how information is gathered, how it is stored, to whom it is distributed and on what terms" could be broadly so described without injury to national security.

(iv) The "Mosaic Effect" principle does not apply in this case

40. The "mosaic effect" is the idea that information which in isolation what appears meaningless or trivial could when fitted together permit a comprehensive understanding of the information being protected.[48] On its own, it will not usually provide sufficient reason to prevent disclosure of what would otherwise appear to be an innocuous piece of information.[49] Recently, this Court has raised concerns about the application of this principle as a justification for suppressing disclosure. As Justice Mosley noted in *Canada (AG) v. Almalki*:

> The respondents submit that the Court should be cautious in relying on the so-called "mosaic effect" to find injury or withhold information. The Major Inquiry report, above, notes at vol. III, pp. 175-76, that there is increasing judicial scepticism about this theory, citing my comments in *Khawaja*, above, at para. 136 and those of Justice Noël in *Arar*, above, at para. 84. The Commission was also skeptical about the validity of the effect in the absence of any evidence to demonstrate that it has occurred.

---

[48] *Arar Inquiry* at para. 82; *Henrie* at para. 30.
[49] *Arar Inquiry* at para. 84; *Canada (Attorney General) v. Khawaja*, 2007 FC 490 at para. 136.

> The mosaic effect may be one of those statements of the obvious that are difficult to prove or disprove. The problem arises in its application. How does the Court discern whether disclosure of a particular item of information will fill a gap in the knowledge of another person? Apart from reciting the principle, the witnesses heard in this and other cases have generally been unable to assist the Court to resolve that conundrum. In *Khawaja*, above at paragraph 136, I said that "...by itself the mosaic effect will usually not provide sufficient reason to prevent the disclosure of what would otherwise appear to be an innocuous piece of information. Something further must be asserted as to why that particular piece of information should not be disclosed." That continues to be my view.
>
> Mr. Evans acknowledged on cross-examination that the mosaic effect may also work in reverse when information is taken away, for example, by redaction. Thus, as the respondents suggest, the Court must be alert to the possibility that information which might be clear and relevant if the full context were to be disclosed may become obscure, equivocal, and even misleading when a piece of the context is removed. In one instance, for example, I concluded that an unredacted phrase would mislead the reader about the meaning of the rest of the paragraph that remained redacted. Accordingly, I ordered the disclosure of additional information.[50]

41. Although the AGC pleads the mosaic effect principle in these proceedings it is entirely inapplicable because, although there may well have been "secrecy" associated with CSE's interception and metadata activities in the past such "general secrecy" considerations no longer apply, inter alia, as a result of the Snowdon revelations, the CSEC Chief's follow on testimony before Parliament, the Commissioner's follow on public reports and statements, the disclosure of evidence related to similar processes in other 5-Eye countries associated with their legislative and judicial processes and, indeed, as a result of the un-redacted portions of documents (including the March 31st and October 5, 2015 Commissioner's reports) that the AGC has voluntarily disclosed in these proceedings.

(v) The Third Party Rule should not limit disclosure

---

[50] 2010 FC 1106 at paras. 117-119

42. While the Respondent acknowledges that the Court must consider potential damage to international relations if any of the relevant information over which privilege has been claimed is information that was shared by a foreign state, the Respondent urges the Court to guard against "over claiming" in this respect and to impose upon the Applicant's a duty to seek the third parties' consent to disclosure where appropriate. [51] Further, the Respondent notes that this Court has on occasion been able to find creative solutions to third party claims by purging only that information which could be sensitive to the originating country. [52] Additionally, and in any event, the Respondent submits that almost everything that it seeks the disclosure of originates domestically, in Canada, and that thus the third party rule is generally factually inapplicable to the information that is sought. Finally, to the extent that the Respondent seeks detail regarding the international sharing of metadata (and thus seeks data related to the conditions imposed on "second parties" and whether compliance with those conditions is monitored and enforced) it is noteworthy that Mr. Sinclair testified (transcript p./ 79, l. 18 to 27) that unlawful activity by the relevant agency, as here, "would definitely be a very significant factor to look at" when assessing the public interest in disclosure.

D. The public interest in disclosure outweighs the public interest in non-disclosure.

(i) The Law

43. Even in the event that some of the relevant disclosure in found to be theoretically injurious to national security, the Respondent submits that in this case the information in issue should be released. These Honourable Courts have held that balancing the public's interest in disclosure and its national

---

[51] *Almalki, supra* at paras.108-110, 141-151; *Arar, supra* at paras. 70-81
[52] *Almalki, supra* at para. 151

security interests to be a more stringent test than the usual relevancy rule.[53] Specific factors to consider may include:

- The nature of the interest sought to be protected;
- The admissibility and usefulness of the information;
- Its probative value to an issue at trial;
- Whether the application has established that there are no other reasonable ways of obtaining the information;
- Whether the disclosures sought amount to a fishing expedition by the applicant; and
- The seriousness of the charges or issues involved.[54]

44. Other factors may also require consideration in appropriate circumstances.[55] It is important to note that this Court has recognized that there are unique considerations applicable to the balancing of interests when it comes to determining whether to uphold national security objections over portions of reports issued pursuant to a statutory inquiry or administrative oversight body. For example, in the context of a dispute over disclosure of the findings of of the O'Conner Inquiry Report, this Court considered the following factors:

> (a) The extent of the injury: the less the injury, the greater the public interest in disclosure;
>
> (b) The relevancy of the redacted information to the procedure in which it would be used, or the objectives of the body wanting to disclose the information;
>
> (c) Whether the redacted information is already known to the public, and if so, the manner by which the information made its way into the public domain;

---

[53] *Ribic FCA* at para. 22.
[54] *Ribic FCA* at paras. 22 to 23; *Jose Pereira E. Hijos, S.A. v. Canada (Attorney General)*, 2002 FCA 470 at paras 16 to 18; *Kempo* at paras. 94 and 102; *Singh v. Canada (Attorney General)*, 2000 CarswellNat 1356 (T.D.) at para. 12; *Khan v. R.*, 1996 CarswellNat 177 at para. 25; *Goguen v. Gibson*, 1983 CarswellNat 20, aff'd 1984 CarswellNat 21; *Arar Inquiry* at para. 93.
[55] *Ribic FCA* at para. 23; *Kempo* at para. 103.

(d) The importance of the open court principle;

(e) The importance of the redacted information in the context of the underlying proceeding;

(f) Whether there are higher interests at stake, such as human rights issues, the right to make a full answer and defence in the criminal context, etc.; and

(g) Whether the redacted information relates to the recommendations of a commission, and if so whether the information is important for a comprehensive understanding of the said recommendation.[56]

45. It is respectfully submitted that these refined considerations must be applied to all of the redactions that have been made to the CSE Commissioner's March 31, 2015 and October 5, 2015 Reports. The Applicant cannot with one breath claim that Canadians need not be concerned about their privacy interests in relation to information CSE is intercepting because of the robust safeguards that they have put in place, but then seek to suppress the detailed basis for findings of the CSE Commissioner on March 31, 2015 that CSE has actually failed to ensure that those safeguards were operational for almost five years.

(ii) Unique Factors Applicable in the context of this case

46. Applying the criteria developed by Justice Noel in *Arar* to this case it is submitted:

(a) That the Applicant's three witnesses gave generalized and generic evidence to the effect that they had national security concerns but wholly failed to tie these concerns to any particular redactions or to any particular subject matter to which redactions had been applied. Merely to illustrate, (at transcript p. 200, l. 22 to p. 202, l. 13) Mr. Millar could give no rationale for the redactions made to the times limited for the retention by CSE of the Canadian metadata that it gathers.

---

[56] *Arar Inquiry* at paras. 93 and 98.

(b) The Respondent has set out the critical relevancy of the information sought in para. 32, supra.

(c) Very large portions of the redacted material related to the CSE "investigative technique" of collecting metadata, analyzing it and sharing it domestically and internationally has already been disclosed through entirely lawful means. Disclosure of macro details related to this "technique" so that this Honourable Court can properly adjudicate this case cannot rationally be said to somehow provide information to malevolent which would permit them to alter their behavior in any material way that has not already occurred as a result of generalized awareness that the national security and intelligence community utilizes sophisticated metadata collection and analysis processes to discern information by means of profiling and contact chaining. In sum, this "investigative technique" has been well known for many years with the result that the information that the Respondent seeks will not diminish the effectiveness or utility of that technique.

(d) The Canadian people properly perceive the Canadian Courts as the guardians and protectors of both the rule of law and the Canadian constitution. In this case the CSE Commissioner has found, at pgs. 4 and 5 of its October 5, 2015 Report that:

> By failing to minimize CII contained in metadata prior to sharing it with Second Parties, I believe CSE did not comply with section 273.64 and 273.66 of the *NDA* and section 8 of the *Privacy Act* and failed to act with due diligence.

And that:

> It is my view that the "failure to comply with the minimization requirement found in the Metadata MD constituted a failure to have in

> place measures to protect the privacy of Canadians" as required by paragraph 273.64(2)(b) of the *NDA*. I also believed that the failure to validate DNI identifiers submitted by Second Parties, and the subsequent provision by CSE of un-minimized IP addresses to the Second Parties constituted non-compliance with paragraph 273.64(2)(b) of the *NDA*.

And that:

> Furthermore by failing to minimize metadata containing CII before sharing it with the Second Parties, I believe CSE acted outside the parameters of its mandate as set out in s. 273.66 of the *NDA*.

And that:

> As a result of the foregoing I believe CSE did not act "consistent with ministerial direction" as prescribed by s. 273.66 of the *NDA*, i.e. prescribed by law.

It does not overstate to assert that these finding amply demonstrate that CSE has negligently distributed the private information of Canadians, apparently en masse, contrary to both the explicit requirements of the NDA and the Privacy Act and contrary to the administrative Ministerial Direction that purports to provide direction to CSE **for almost five years**.

In addition the Commissioner's findings are well founded. As outlined at page 43 of the Commissioner's March 31, 2016 report:

> "CSE had a compliance validation process in place to confirm that the minimization service was processing the result of [redacted] however, this process did not include the examination of minimization service outputs". Therefore, CSE was **under the impression that minimization was taking place when in fact it was not**."

The Canadian public is fully entitled to ask – "CSE gathers metadata, designs an automated system for distributing metadata around the world, designs another automated system to minimize our identity, but then fails to ensure that the minimization system actually works – and apparently this

cavalier treatment of our private information continues for five years – how could this possibly occur?".

In these very unique circumstances, the Canadian public is fully entitled to expect that its independent Courts will administer justice, find facts and grant appropriate remedies in open Court based upon all facts relevant to the determination of how these events could possibly occurred.

In sum, as described in *Carey* (as adopted by both Justices Noel and Mosley in analogous circumstances) "the purpose of secrecy in government is to promote its proper functioning, not to facilitate improper conduct:...". Or, as eloquently described by a national security commentator[57], the time for the Courts to address national security issues under "the dead weight of euphemistic language, the screen of obscurity, the exercise of obeisance to official secrecy" should be over, at least in the context of the unique circumstances of this case where the statutorily appointed review Commissioner has already made a finding of systemic unlawfulness.

(e) The Respondent respectfully submits that the macro details are absolutely essential to this Court's proper determination of the issues in this case. To illustrate, how can the Court possibly grant appropriate remedies to Canadians who have had their biographic core of privacy violated by CSE between 2009 and March, 2014 unless it, and the Respondent, actually knows all of "the facts" redacted from the Commissioner's March 31, 2015 Report. How can the Respondent seek to develop those facts in accordance with the rule of law entitlements guaranteed by this Court's Rule 222(2) if it is not permitted to access such primary facts?

---

[57] Wesley Wark, "Once More into the Breach: Strengthening Canadian Intelligence and Security Accountability" p. 8.

To further illustrate, how can this Court even begin to adjudicate the constitutional challenge without knowing the macro details of CSE's activities? Or for that matter, the Applicant asserted "defences" to such claims?

(f) As the Respondent has demonstrated by reference to the SCC's jurisprudence summarized at paras 13, 21, 22 and 23 our constitutional order and our Courts have sought to assiduously protect both the spatial and informational privacy rights of Canadians at every turn, in every dimension. It thus can be fairly said that nothing less than "the flourishing of an open and democratic society" is at stake in these proceedings.

(g) The CSE Commissioner is appointed pursuant to s. 273.63(1) of the Act and one of its duties as required by s. 273.63(2)(b) of the Act is to "review the activities of the Establishment to ensure that they are in compliance with the law". In carrying out his duties the Commissioner, by virtue of s. 273.63(4) has "the powers of a commissioner under Part II of the *Inquiries Act*" and, by virtue of s. 273.63(5) is authorized to engage staff to assist him to carry out his duties.

It is respectfully submitted that the Commissioner's March 31 and October 5, 2015 Reports, the product of diligent investigation activity, should be publically released in their entirety so that the accountability which they seek to promote can be fulfilled.

PART IV – ORDER SOUGHT

47. The Respondent requests an order authorizing disclosure of the information at issue;

48. Alternatively, should this Honourable Court find that any of the information at issue cannot be disclosed in its entirety, the Respondent requests an order authorizing the disclosure, subject to any conditions that the Court considers appropriate, of all or part of the information or facts, or a summary of the information or a written admission of facts relating to the information.

DATED this 22nd day of June, 2016 at Vancouver, British Columbia.

DAVID J. MARTIN/
TAMARA DUNCAN
Martin + Associates
Barristers
863 Hamilton Street
Vancouver, BC V6B 2R7
(t) 604-682-4200
(f) 604-682-4209
(e) reception@martinandassociates.ca

Counsel for the British Columbia Civil Liberties Association