



June 1, 2016

BACKGROUNDER ON SPYING: Civil Liberties Watchdog Sues Surveillance Agency Over Illegal Spying On Canadians

1. What is CSE?

The Communications Security Establishment (CSE), a federal spy agency, is Canada's national cryptologic¹ agency, the Canadian counterpart to the U.S. National Security Agency (NSA).

CSE is charged with collecting "signals intelligence," which includes the secret collection of electronic communications for the purpose of advancing Canadian interests in defence, security and international affairs.

CSE's operations are shrouded in secrecy. As former CSE chief John Adams admitted in 2013: "[t]here's no question that [CSE] is very, very biased towards the less the public knows the better".²

The number of CSE employees has more than doubled in the last 15 years, and its budget has quadrupled. It now spends \$580 million in taxpayer money every year. CSE's new 89,000 square meter state-of-the-art headquarters cost Canadians over \$1 billion dollars.

After the events of Sept. 11, 2001, the electronic eavesdropping agency was also given unprecedented new powers to intercept the private communications of Canadians and was directed to collect private information about citizens. CSE is required to have policies in place to protect the privacy of Canadians, but it has not provided the details of those policies to Canadians.

2. What is the legal basis for the BCCLA's case?

The lawsuit argues that two aspects of CSEC's operations violate the *Charter of Rights and Freedoms'* protections against unreasonable search and seizure and infringe on free expression:

¹ The CSE's cryptology encompasses both Signals Intelligence (SIGINT) and IT Security.

² See CBC News article at <http://www.cbc.ca/news/politics/spy-agency-csec-needs-mps-oversight-ex-director-says-1.1928983>

- 1) The interception of the private communications of Canadians;
- 2) The sweeping collection of metadata information produced by Canadians in their everyday activities online and through phone conversations.

The lawsuit was filed in 2013 is proceeding in federal court. It is the first and only challenge to the legality of CSE's spying activities against Canadians.

3. Does CSE spy on Canadians?

Yes. CSE uses secret ministerial authorizations to read Canadians' emails and text messages, and listen to their phone calls, in the course of surveillance targeted at foreigners abroad. However, in the process, the CSE captures an unknown quantity of purely domestic communications. Furthermore, the CSE need not demonstrate that its surveillance targets are the agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. CSE also collects Canadians' personal metadata information, which is the information associated with everyone's communications, , under secret ministerial directives.

4. What is a ministerial authorization?

Unique to CSE, Part V.I of the *National Defence Act* allows the Minister of National Defence to authorize CSE to intercept the private communications of Canadians in the course of surveillance targeted at foreigners abroad. The authorization is applied when a person inside of Canada is communicating with a person outside of the country.

Without the authorization scheme, eavesdropping on the private communications of Canadians would constitute a serious criminal offence under the *Criminal Code*.

The authorizations are very broad and do not specify who will be targeted, or what information is to be intercepted or what will be done with the information once it is gathered.

Ministerial authorizations are valid for up to 12 months and can be renewed indefinitely. CSE has taken the position that ministerial authorizations are classified documents and has kept their content and use secret. The agency has not notified those Canadians whose private communications have been intercepted as a result of a ministerial authorization, nor has it told Parliament how many Canadians have been spied on using a ministerial authorization.

The U.S. government admitted that in 2013 it had targeted nearly 90,000 foreign persons or organizations for surveillance.³ The Canadian government has not revealed how many persons or groups it targets, or how many Canadians have had their private communications intercepted.

5. What information can CSE collect under a ministerial authorization?

A ministerial authorization permits CSEC to intercept the private communications of Canadians when a Canadian or other person in Canada communicates with a foreign target of the agency located outside Canada.

Private communications are oral communications or telecommunications that are intended to be private. For example, using a ministerial authorization, CSE can read the content of emails and text messages, listen to the content of phone conversations, and watch video chats.

6. Why is the BCCLA concerned about ministerial authorizations?

The ministerial authorizations give CSE unprecedented powers to intercept the private communications of Canadians without any judicial oversight. This is a serious departure from the safeguards that protect Canadians from domestic spying and police agencies, such as CSIS and the RCMP. Those agencies must seek judicial warrants before intercepting the communications of Canadians.

The Minister's authorizations allow for the broad collection of Canadians' personal communications. The Minister is permitted pursuant to the *National Defense Act*, section 273.65(2) to authorize this broad collection of Canadians' personal communications if he is satisfied that the following criteria are met:

- (a) the interception will be directed at foreign entities located outside Canada;
- (b) the information to be obtained could not reasonably be obtained by other means;
- (c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
- (d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

³ https://www.washingtonpost.com/world/national-security/us-releases-data-on-sensitive-surveillance-programs-for-first-time/2014/06/27/46bbd47e-fe3a-11e3-8176-f2c941cf35f1_story.html?tid=a_inl

The Minister's determinations are made in secret and are not reviewable by the Canadian public. Unchecked government surveillance presents a grave threat to democratic freedoms. The BCCLA is deeply concerned that CSE is gaining secret, illegal access to the content of communications of ordinary Canadians, and there are no reasonable safeguards in place to monitor its activities.

7. What is the Ministerial Directive on the Collection and Use of Metadata?

The Ministerial Directive on the Collection and Use of Metadata – a secret decree not scrutinized by Parliament - was originally issued by the Minister of National Defence in 2005, and was reissued in slightly modified form by the Minister in 2011.

This secret ministerial directive allows CSE to collect, retain, review, analyze, use and share metadata produced by Canadians.

8. What is metadata?

Metadata is information that is automatically created every time an email or text message is sent, every time a mobile phone call is made, and every time the internet is searched. The purpose of metadata is to identify, describe, manage or route the message, phone call or data.

For example, the metadata information attached to a mobile phone conversation would describe the phone number of the caller, the phone number of the recipient, the time and date of the call, and the length of the conversation. The metadata associated with an email would include the email address of the sender, the email address of the recipient, the time it was sent and the size of the email.

9. Why is BCCLA concerned about the collection of metadata?

The collection of metadata is digital surveillance. CSE spies on Canadians every time it collects metadata about a Canadian email or text message, a Canadian phone call, or a Canadian visit to an internet site. Analysis of this personal information could enable CSE, or partner agencies such as CSIS and the RCMP, to create a highly revealing picture of a Canadian and his or her relationships with other Canadians. This digital spying is conducted without any real oversight or accountability. CSE doesn't report its activities to Parliament or to the Canadian public. This kind of widespread surveillance without accountability is fundamentally incompatible with Canadian democracy.

10. What information does CSE share with agencies in other countries?

CSE is a member of the "Five Eyes" intelligence alliance, which includes the United Kingdom, New Zealand, Australia, and the United States. CSE shares information with its partner agencies

in those countries, but it has not told Canadians what information it shares, how it protects Canadians' privacy or how much of the information it collects about Canadians is shared.

11. How big is CSE's staff and budget?

The organization employs approximately 2,100 people and has an annual budget of approximately \$580 million.

12. What kind of oversight is there for CSE?

There is no court or parliamentary committee that monitors CSE's interception of Canadians' private communications and metadata information, and there is no judicial oversight over its sweeping powers.

The Office of the CSE Commissioner is the only government office charged with reviewing the activities of CSE. The CSE Commissioner reports to the Minister of National Defence. The "micro agency," as it was recently called by the out-going CSE commissioner, has a budget of roughly \$2 million dollars and a staff of 11 people. For most of its history, the Commissioner's office did not have independent funding and was a line item in the budget of the Department of National Defence until 2007.

The Commissioner does not review CSE's spying activities before they occur. His review is limited to the activities CSE has already undertaken, sometimes years in the past.

The Office of the CSE Commissioner has raised concerns about CSE's domestic spying activities. For example, since the enactment of the *Anti-Terrorism Act* in December 2001, the CSE Commissioner has repeatedly recommended to the Minister of National Defence and to the Attorney General of Canada that the law be amended to clarify the legal requirements to intercept Canadians' private communications. No such amendments have been enacted. In January 2016, the Commissioner declared that CSE had broken the law by failing to take effective measures to protect Canadian privacy when sharing metadata with its Five Eyes allies. Sharing of the metadata in question has been "suspended" pending modifications to CSE's metadata-sharing procedures.

13. Why did the BCCLA file this lawsuit?

This lawsuit calls on the government to state clearly who it is watching, what is being collected and how it is handling Canadians' private communications and information. The BCCLA filed this

lawsuit to uphold the constitutional rights of Canadians, which include implementing safeguards to protect the privacy rights of all Canadians.

14. What is the new government's position on the issues raised by the BCCLA's lawsuit?

Members of the new government have on numerous occasions stated that Canada needs enhanced accountability of national security activities through judicial oversight and by independent review bodies and parliamentarians. Many of the concerns they have raised are the same or consistent with the issues the plaintiffs have identified in this litigation.

For example:

- In June 2014, Joyce Murray, M.P., introduced Bill C 622, known as the CSEC Accountability and Transparency Act, a comprehensive private members' initiative that would impose new reporting and disclosure requirements on the Communication Security Establishment. Importantly, the Bill would have required that a judge, rather than the Minister of National Defence, issue the authorizations which permit CSE to collect private communications. At the time, Ms. Murray stated, "This bill would help improve transparency, an important Liberal value, and would restore public trust in this important establishment that is so vital to protecting the security of Canadians." Her Bill was supported by both the Liberals and the NDP, but it was defeated by the then government on November 5, 2014, in a 142 to 120 vote.
- On October 11, 2015, Mr. Trudeau unveiled the Liberal Party of Canada's full election platform, which endorsed key features of Bill C 622 and committed the Liberal Party to "limit Communications Security Establishment's powers by requiring a warrant to engage in the surveillance of Canadians."
- The Prime Minister directed, in his mandate letter to the Minister of Public Safety and Emergency Preparedness that new legislation on national security is needed to better balance collective security with rights and freedoms.
- Since taking office, the government has on numerous occasions stated that it plans an extensive consultation in relation to national security matters and that it is committed to the enhanced oversight of national security agencies.

However, despite the various pledges to enhance accountability, the new government continues to challenge the BCCLA's lawsuit, without any changes in its legal position.

15. Where can I learn more about the BCCLA's lawsuit?

Read more about the BCCLA's lawsuit and access documents filed in the case at <http://bccla.org/stop-illegal-spying/>