Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET // SI // CEO

October 5, 2015

The Honourable Jason Kenney, P.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

The Honourable Peter MacKay, P.C., M.P.
Minister of Justice and Attorney General of Canada
284 Wellington St.
Ottawa, ON K1A 0H8

Dear Minister and Attorney General:

As the Communications Security Establishment Commissioner, I have a duty under paragraph 273.63(2)(*c*) of the *National Defence Act*[1] (*NDA*) to inform the Minister of National Defence and the Attorney General of Canada of any activity of the Communications Security Establishment (CSE) that I believe may not be in compliance with the law. Pursuant to this duty, I am writing to you with regard to a recent review of CSE's use of metadata in a signals intelligence context, during which CSE informed my office of certain activities that I believe do not comply with the law.

CSE collects, uses and discloses [redacted] metadata[3] under the authority of paragraph 273.64(1)(*a*) of the *NDA*, as affirmed by paragraph (3) of the *Ministerial*

[1] R.S.C., 1985, c. N-5.
[redacted] metadata is also referred to as [redacted] metadata, collected or shared without having gone through a targeting-selection process which ensures that at least one end of the associated communication is foreign and is related to a foreign intelligence priority of the Government of Canada.
[3] "Metadata means information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
T: 613-992-3044 F: 613-992-4096

Directive: Communications Security Establishment Collection and Use of Metadata, 21 November 2011 (Metadata MD). The collection, use and disclosure of metadata are meant to be carried out within the parameters set by the MD.

In accordance with the *NDA*, CSE's activities carried out under its foreign intelligence mandate (paragraph 273.64(1)(*a*)) shall not be directed at Canadians or any person in Canada and shall be subject to measures to protect the privacy of Canadians (para. 273.64(2)(*a*) and (*b*)). Section 273.66 places limits on CSE's activities, in that CSE may only undertake activities that are within its mandate, consistent with ministerial direction and authorization. The Metadata MD provides directions to CSE concerning the privacy protection measures that the Minister requires CSE to implement for the handling of [redacted] metadata. Minimization of [redacted] metadata is one of these privacy protection measures.

Minimization is the process by which Canadian Identity Information (CII)[4] contained in [redacted] metadata is altered in such a way that it is rendered unidentifiable prior to sharing with Second Party partners[5]. Specifically, section 7(5) of the Metadata MD states that:

> Canada's allies shall not be granted access to metadata known to be associated with Canadians located anywhere or persons located in Canada ([redacted] metadata) unless it is altered prior to granting access in such a way as to render impossible the identification of the persons to whom the metadata relates.

Additionally, long-standing agreements exist for CSE's foreign signals intelligence information sharing with Second Party partners, and include a commitment by the partners to respect the privacy of each other's citizens.

CSE cooperates very closely with its Five Eyes international partners, and is party to an agreement in which each partner, including CSE, [redacted] telephony (also known as Dialed Number Recorder, or DNR)

---

content." (*Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, 21 November 2011).

[4] Identity information means information about an identifiable individual, such as any number, symbol or other data uniquely assigned to an individual. In a SIGINT context, this usually includes phone numbers, email addresses, names, [redacted] and IP addresses, among others.

[5] CSE's "Second Party" partners are: the National Security Agency (United States), the Government Communications Headquarters (United Kingdom), the Australian Signals Directorate (Australia) and the Government Communications Security Bureau (New Zealand), also known collectively with CSE as the Five Eyes partners.

metadata [redacted] CSE has shared [redacted] telephony metadata in this manner [redacted]

In June 2014, CSE voluntarily informed my office that it discovered that it had not been properly minimizing certain CII contained in some of the telephony metadata shared with its Five Eyes partners. CSE informed my office that it had failed to ensure that equipment and systems, designed to automatically minimize this data, were up-to-date and functioning properly. As a result of this discovery, and on its own, CSE suspended sharing of [redacted] telephony metadata with its Five Eyes partners on March 14, 2014.

At the same time, CSE informed my office that it had also discovered compliance issues related to the sharing of Digital Network Intelligence (DNI) metadata with its Five Eyes partners. DNI metadata pertains to Internet-based communications. Fields that are considered to constitute CII include email address and Internet Protocol (IP) address information. [redacted] DNI metadata [redacted] CSE is required to validate the identifiers submitted to ensure that they do not pertain to Canadians or persons in Canada. CSE failed to validate the identifiers prior to returning DNI metadata containing unminimized IP addresses, some of which may have pertained to Canadians. CSE believes that its systems have failed to minimize IP addresses in this manner since the inception of automated DNI sharing, in 2009. As a result of this discovery, CSE suspended DNI metadata sharing on April 3, 2014.

The automated sharing of both DNR and DNI metadata with Five-Eyes partners remains suspended. CSE has indicated that it will remain so until the Chief CSE is satisfied that proper systems are in place to ensure that all shared CII is properly minimized, in accordance with the Metadata MD. CSE also informed the Minister of National Defence about these matters.

While the problems with minimization have been longstanding, CSE could not precisely define the scope of the privacy impact, nor could it undertake a comprehensive damage assessment, due to the complexity involved in such a task. CSE has provided my office with briefing notes that were originally sent to former

CSE Chief John Forster in April 2014 outlining the issues, and my officials began investigating this as part of a review of CSE's use of metadata in a signals intelligence context that was already underway at the time. This included a review of written documentation, interviews with CSE staff, and discussions with senior CSE officials and Justice Canada's Director of Legal Services at CSE. I have also received the advice of both my in-house and external independent legal counsel on this matter. My officials and I have had several meetings with CSE to discuss this issue, and CSE has cooperated fully with my office in providing in-depth written accounts of the minimization deficiencies, as well as the current status of corrective efforts.

In undertaking activities under any part of its mandate, outlined above, CSE must comply with the laws of Canada, including the *NDA*, the *Privacy Act*[6], the *Criminal Code of Canada*[7] and the *Canadian Charter of Rights and Freedoms*. In addition, CSE must comply with Ministerial Directives issued by the Minister of National Defence, as well as with its own internal operational policies and procedures.

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

Paragraph 273.64(2)(*b*) of the *NDA* requires CSE's foreign signals intelligence activities to be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information. While this paragraph does not reference the need for measures to protect the privacy of Canadians in the disclosure of intercepted information, I believe a court would read that provision as imposing such an obligation on CSE's mandate, including the disclosure of intercepted information in the course of providing foreign intelligence. Parliament did not dictate the measures that the Minister and CSE were to adopt to protect the privacy of Canadians. However, once CSE and the Minister have acted to adopt certain privacy standards, such as those set out in the Metadata MD, those standards become the norm against which the activities of CSE are to be measured. CSE must comply with these standards by virtue of sections 273.64(2)(*b*) and 273.66 of the *NDA*.

---

[6] R.S.C., 1985, c. P-21.
[7] R.S.C., 1985, c. C-46.
[8] Due diligence is defined in Black's Law Dictionary, 8th ed. as "[t]he diligence reasonably expected from, and ordinarily exercised by, a person who seeks to satisfy a legal requirement or to discharge an obligation."

Although CSE had other measures in place to protect the privacy of Canadians, which may constitute a mitigating factor in this situation, the fact remains that the most important measures to protect the privacy of Canadians are set out in the Metadata MD, and are not limited to restrictions that may be contained in agreements with Second Parties or other privacy measures that may be in place. 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 believe 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*.

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*. Although ss. 273.62(4) of the *NDA* stipulates that ministerial directions are not statutory instruments within the meaning of the *Statutory Instruments Act*[9], and would therefore not have force of law, s. 273.66 obliges CSE to undertake activities that are within its mandate and consistent with ministerial direction. In short, even if a ministerial directive does not have the force of law by itself, the limitations on CSE's mandate are established by the law, as expressed in s. 273.66 of the *NDA*. The minimization requirement found in the Metadata MD provides protection for the privacy of Canadians when metadata is to be shared with CSE's allies. The protection of the privacy of Canadians in the retention, use and disclosure of metadata containing CII is at the heart of the Metadata MD. Minimization is vital to preventing the disclosure of such metadata to the Second Parties. 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.

Finally, there are provisions of the *Privacy Act* which govern CSE's collection, use, retention and disclosure of personal information. CSE's mandate is to provide foreign intelligence in accordance with Government of Canada intelligence priorities. This has been interpreted to include the sharing of metadata with CSE's Second Party partners. Therefore, paragraphs 8(2)(*a*) and (*b*) of the *Privacy Act* would also permit such sharing. However, any disclosure must meet the requirements of the *NDA*. The disclosure must be subject to "measures to protect the privacy of Canadians" and must be in accordance with any restrictions set out in ministerial directives. If it is not, the sharing would not be authorized by the

[9] R.S.C., 1985, c.S-22.

NDA as required by paragraph 8(2)(*b*) of the *Privacy Act* because it would not be done "for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure." Nor would it be "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose", as required by paragraph 8(2)(*a*) of the *Privacy Act*. Accordingly, I believe that CSE's disclosure of un-minimized CII to Second Parties did not comply with the *Privacy Act*.

CSE's Department of Legal Services Solicitor-Client Privilege

Solicitor-Client Privilege

CSE acknowledges that it failed to comply with the Metadata MD, Solicitor-Client Priv

Solicitor-Client Privilege

The legal landscape concerning metadata in Canada, as well as in the international context, is evolving. For example, Canada's *Protecting Canadians from Online Crime Act* (Bill C-13) came into force in March 2015. Amendments to the *Criminal Code* brought by this *Bill* create a new type of warrant in order for law enforcement agencies to obtain transmission data (i.e. metadata) by means of a transmission data recorder if there are reasonable grounds to suspect that an offence has been or will be committed. Also, the Supreme Court of Canada found in *R. v. Spencer*[10] that anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure. Finally, there is also international awareness of these issues. In June 2015, the Independent Reviewer of Terrorism Legislation in the U.K., David Anderson Q.C., published his Report of the Investigatory Powers Review, entitled "A Question of Trust." Key recommendations dealt with the collection by security and intelligence agencies of communications data (i.e. metadata) in bulk as well as authorizations to collect communications data in bulk.

[10] 2014 SCC 43.

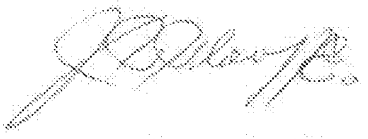
Considering the above, **I am recommending** to the Minister of National Defence that the *National Defence Act* be amended in order to clarify CSE's authority to collect, use, retain, share and disclose metadata.

CSE has been candid, forthcoming and cooperative throughout this process. I am pleased that CSE took proactive measures to limit non-compliance, by suspending the sharing of metadata with its Second Party partners, and that it is committed to ensuring that minimization processes function properly prior to the resumption of sharing [redacted] metadata.

My office continues to consider this matter as a high priority. I will keep both of you apprised of any further major developments related to this matter. I remain available to discuss this issue further at your convenience.

As a final note, in a broader context of SIGINT information sharing with allies, reported in my latest public annual report[11], in January 2015 I met with the Inspector General of the United States National Security Agency (NSA) to personally seek assurances beyond those CSE can provide to me, that the NSA respect the agreements to protect the privacy of Canadians. I am satisfied with the assurance I obtained.

Yours sincerely,



Jean-Pierre Plouffe

c.c. The Honourable Julian Fantino, Associate Minister of National Defence
Ms. Greta Bossenmaier, Chief, CSE

[11] I submitted my public annual report to the Minister of National Defence in June 2015. It has yet to be tabled in Parliament.