PUTTING THE LAW TO WORK FOR CSE

Bill C-59 and Reforming the CSE Foreign Intelligence Collection and Cybersecurity Process

Brief to the Commons Standing Committee on Public Safety and National Security

5 December 2017

Craig Forcese
Faculty of Law, University of Ottawa, cforcese@uottawa.ca

OVERVIEW

Issue: CSE incidentally collects information in which Canadians have a reasonable expectation of privacy, without advance authorization by an independent judicial officer. This likely violates section 8 of the Charter. Bill C-59 attempts to cure this constitutional issue through a ministerial authorization process that involves vetting by an Intelligence Commissioner, a retired superior court judge. This is a creative solution, but it depends on steering all collection activities that might implicate acquisition of information in which a Canadian has a reasonable expectation of privacy (REP) into the authorization process.

Problem: C-59's present drafting only obliges this authorization process where "an Act of Parliament" would otherwise be contravened. This is an *underinclusive* "trigger" for the authorization process. There are instances where collection of information in which a Canadian has an REP – and thus a constitutional interest – would not violate an "Act of Parliament" (for example, some sorts of metadata).[1]

Recommendation:

Place a reference to "reasonable expectation of privacy" within the "trigger" sections of subs 23(3) and (4), as follows:

---

[1] Collecting content of a Canadian communication, even incidentally, would violate an Act of Parliament, and thus require an authorization. This information meets the definition of a "private communication" in Part VI of the Criminal Code. A private communication is basically a telecommunication or any oral communication that originates in Canada or is received in Canada, done with an expectation of privacy. But the government has construed the concept of "private communication" in the Criminal Code as excluding metadata. If correct, collecting metadata does not violate the Criminal Code. Nor is there any other Act of Parliament that would clearly be breached by the collection of metadata originating from Canadians. But the Charter privacy right now almost certainly reaches metadata. In the result, the C-59 proposal does not cure a key flaw existing in the current *National Defence Act* framework, one that has generated a lawsuit from the BC Civil Liberties Association.

Contravention of other Acts — foreign intelligence
(3) Activities carried out by the Establishment in furtherance of the foreign intelligence aspect of its mandate must not contravene any other Act of Parliament or involve the acquisition of information in which a Canadian has a reasonable expectation of privacy unless they are carried out under an authorization issued under subsection 27(1) or 41(1).

Contravention of other Acts — cybersecurity and information assurance
(4) Activities carried out by the Establishment in furtherance of the cybersecurity and information assurance aspect of its mandate must not contravene any other Act of Parliament or involve the acquisition of information in which a Canadian has a reasonable expectation of privacy unless they are carried out under an authorization issued under subsection 28(1) or (2) or 41(1).

BACKGROUND

Among other things, CSE is Canada's "signals intelligence" service, charged with acquiring foreign intelligence from the "global information infrastructure"; that is, electronic emissions and now also information from other technology networks such as the internet. It also has a cybersecurity mandate: "to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada".[2]

In conducting its foreign intelligence and cybersecurity function, CSE is to cast its eyes outward, past Canada: it cannot direct its activities at Canadians or any person in Canada. It is also to take steps to protect the privacy of Canadians.[3] This second proviso seems unnecessary if CSE cannot direct activities at Canadians. But it responds to a technical problem: the inevitability of *incidental* acquisition of Canadian information. In acquiring information from the global information infrastructure or performing its cybersecurity role, CSE cannot know in advance whether Canadian or Canadian-origin data will be swept within its acquisition activities.

In the current *National Defence Act*, therefore, CSE may (and does) obtain special "ministerial authorizations" where it might inadvertently sweep in Canadian "private communications" within the meaning of Part VI of the *Criminal Code*[4] – essentially "telecommunications" with a nexus to

---

[2] *National Defence Act* (NDA), R.S.C., 1985, c. N-5, ss. 274.61 and 273.64(1). These mandates are preserved in bill C-59, Part 3, *Communications Security Establishment Act* (CSE Act), ss. 2, 16, 17, and 18.

[3] NDA, s.273.64(2); CSE Act, ss.17, 18, 23, and 25.

[4] NDA, ss.273.65, 273.61.

Canada.[5] There are presently three authorizations for foreign intelligence and one for cybersecurity. The authorizations are broad – involving classes of activities and not individual activities.

The current rules suffer, however, from two key problems.

THE CURRENT CSE AUTHORIZATION PROCESS IS CONSTITUTIONALLY DOUBTFUL

First, technology has evolved considerably since the original enactment of CSE's powers in 2001. Now, the focus is on "metadata" – the information that surrounds a communication, such as email addresses, routing information, duration and place of cell calls and the like. The government's view has been that these metadata are not a component of a private communication for which a ministerial authorization must be sought – a conclusion dependent on a narrow reading of the definition of "telecommunication" in the *Interpretation Act*.[6]

But second, whether CSE obtains a ministerial authorization or not, there are evident constitutional issues under section 8 of the Charter, ones anticipated many years ago but never resolved.[7] Section 8 protects against unreasonable searches and seizures. In practice, that usually means that authorities may only interfere with a reasonable expectation of privacy under a warrant authorized in advance by an independent judicial officer; that is, someone able to act judicially.[8] Wiretaps of communications, for instance, must be authorized by judicial warrant in almost all circumstances.

Whatever else he or she may be, the minister of defence is not an independent judicial officer, and yet under the current Act it is his or her authorization that permits CSE's collection of private communication.

For their part, metadata do not include the content of a communication. But pieced together (and even alone) they can be remarkably revealing of a person's habits, beliefs and conduct. Metadata are often information in which there is a reasonable expectation of privacy, especially when

---

5 *Criminal Code,* R.S.C., 1985, c. C-46, s. 183.

6 *Interpretation Act*, R.S.C., 1985, c. I-21, s.35 (defining "telecommunications" as "the emission, transmission or reception of *signs*, *signals*, writing, images, sounds or *intelligence of any nature* by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system" (emphasis added)).

7 See, e.g., Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, ON: LexisNexis Butterworths, 2005) at 232.

8 *Hunter v. Southam*, [1984] 2 SCR 145 at 162.

compiled as a mosaic.[9] This conclusion is supported, if not quite decided, by the Supreme Court's decision in *R. v Spencer*,[10] holding that even the most innocuous of nameplate information tied to a digital trail – subscriber information associated with an IP address – attracts constitutional protection.

The risk, therefore, is that CSE now acquires information that enjoys constitutional protection, without going through the independent judicial officer process (or anything approximating the process) that the constitution requires before the state acquires this information. That is, at core, the issue in a constitutional challenge brought by the British Columbia Civil Liberties Association to CSE's law and metadata practices.[11]

The fact that CSE's acquisition of private communications and metadata is incidental does not matter, since the collection of at least some constitutionally-protected information is *foreseeable* and *inevitable*. Our constitutional standards for search and seizure do not say: "you are protected against unreasonable search and seizures, except when the search and seizure is simply a predictable, foreseen accident stemming from other activities". Put another way, the fact that information in which Canadians have a reasonable expectation of privacy is incidentally but foreseeably (rather than intentionally) collected by the state should not abrogate the constitutional right (although I accept it may shape the precise protections that the *Charter* will then require, see below).

CONSTITUTIONAL DOUBTS CONCERNING CSE'S COLLECTION COULD CONTAMINATE OTHER NATIONAL SECURITY PROCEEDINGS

More than this, the incidentally-collected information is then placed in circulation by CSE internationally and domestically. Canadian identifying information is "minimized" (redacted), but the redactions can be lifted on request from a partner (and, unfortunately, some has been shared without minimization because of technical glitches).[12]

---

[9] For a fuller discussion of metadata and privacy rules, see Craig Forcese, "Law, Logarithms and Liberties: Legal IssuesArising from CSEC's Metadata Collection Initiatives," in Michael Geist (ed) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (University of Ottawa Press, 2015), online: https://ssrn.com/abstract=2436615

[10] 2014 SCC 43.

[11] See BCCLA website: https://bccla.org/our_work/stop-illegal-spying/. (In the interest of full disclosure: on behalf of BCCLA, I provided factual background information for use by the court in that proceeding).

[12] See Communications Security Establishment Commissioner, *Annual Report 2015-2016*, online: https://www.ocsec-bccst.gc.ca/s21/s68/d365/eng/highlights-reports-submitted-minister#toc-tm-2

The legal standards for this lifting are unclear. I have reviewed operational policies and the reports of CSE's review body, the CSE Commissioner.[13] From the information on the record that I have seen, it appears Canadian identifying information redactions may be lifted when there is a *Privacy Act* justification for doing so. It is my understanding that some of this lifting may done for the Canadian Security Intelligence Service (CSIS) or federal law enforcement even in the absence of a warrant, if still within the requesting agency's mandate. In the result, CSE may be administratively sharing information that other agencies could only themselves collect pursuant to a warrant.

We have been down this constitutional path before and the Supreme Court has regarded administrative end-runs around the constitution as themselves unconstitutional.[14] If this sort of information then seeds a police investigation that culminates in criminal charges, we may end up with a classic "fruit of the poisoned tree" scenario, causing criminal cases to collapse and compounding Canada's longstanding difficulties in transforming intelligence to evidence.[15]

To be clear, there is no malice in any of this. There is no intent to do an end-run. What has happened is that the technology has outstripped rules and procedures designed for a simpler technological era, and a different threat environment.

IT IS POSSIBLE TO MINIMIZE THESE CONSTITUTIONAL DOUBTS

Cleaning-up the procedure should be a priority for public safety as much as for principled constitutional reasons. The challenge lies in creating a regime

---

[13] See, e.g., CSE Commissioner, Annual Report 2014-2105, https://www.ocsec-bccst.gc.ca/s21/s20/d274/eng/highlights-reviews-reports-submitted#toc-tm-7-6

[14] *R. v. Cole*, 2012 SCC 53 at para. 67 ("The fact that the school board had acquired lawful possession of the laptop *for its own administrative purposes* did not vest in the police a delegated or derivative power to appropriate and search the computer *for the purposes of a criminal investigation*."); *R. v. Colarusso*, [1994] 1 SCR 20 at 58-60 ("[A] seizure by a coroner will only be reasonable while the evidence is used for the purpose for which it was seized, namely, for determining whether an inquest into the death of the individual is warranted. Once the evidence has been appropriated by the criminal law enforcement arm of the state for use in criminal proceedings, there is no foundation on which to argue that the coroner's seizure continues to be reasonable.")

[15] For a discussion of intelligence-to-evidence dilemmas, see Craig Forcese, Craig, *Staying Left of Bang: Reforming Canada's Approach to Anti-Terrorism Investigations* (May 29, 2017). Ottawa Faculty of Law Working Paper No. 2017-23. Available online: https://ssrn.com/abstract=2976441

that meets the constitutional standards while recognizing that CSE's collection activities are very different from conventional surveillance activities done by police or CSIS. The latter agencies invade privacy under warrants that meet strict specificity standards, identifying targets and the scope and nature of the intrusion.

CSE, by comparison, does not target Canadians and persons in Canada under its foreign intelligence and cybersecurity mandates – and therefore never *intentionally* targets the privacy of any constitutionally-protected individual. An authorization regime must, therefore, take into the account the "foreseeable but incidental" nature of the collection. And that means it can never include a warrant-style specificity requirement.

In Canada, we know the Charter does not require cookie-cutter warrants for all forms of search and seizure. As the Federal Court of Appeal decided (in applying different criteria to a CSIS warrant than to a police wiretap): "To conclude…a different standard should apply where national security is involved *is not necessarily to apply a lower standard but rather one which takes account of reality*" (emphasis mine).[16] And so in that case, it made no sense to require CSIS to show it was investigating a criminal offence -- its mandate is to investigate threats to the security of Canada.

This suggests that there is at least some flexibility in design, so long as we preserve the core essentials of the section 8 jurisprudence: advance authorization by an independent judicial officer.

BILL C-59 GOES A CONSIDERABLE DISTANCE IN MINIMIZING THESE CONCERNS

This brings us to bill C-59. Bill C-59 is a lengthy, complex omnibus bill, addressing a host of national security matters. It is unquestionably the biggest overhaul of national security law and the institutional setting in which it operates since 1984, and the enactment of the *Canadian Security Intelligence Service Act*.

Among its parts, it enacts a "Communications Security Establishment Act". This statute has many novel aspects, but I shall focus on its response to the dilemma addressed in this brief. That response comes in two forms: one institutional and the second procedural.

Institutionally, bill C-59 creates a new office – the Intelligence Commissioner (IC).[17] This will be a retired superior court judge.[18] Here, the obvious intent is to create an office occupied by the "independent judicial officer" demanded by the Supreme Court jurisprudence under section 8 of

---

16 *Atwal v Canada,* [1988] 1 FC 107 at para. 35.

17 Bill C-59, Part 2, *Intelligence Commissioner Act* (IC Act).

18 IC Act, s.4.

the Charter. The alternative might have been to assign responsibility to a Federal Court judge. But the latter approach would have complicated a second institutional feature: the IC will have a staff, ideally one resourced and expert enough to grasp the arcane technological aspects of CSE's activities.

Among his or her functions, the IC is charged with reviewing "Foreign Intelligence Authorizations" and "Cybersecurity Authorizations" issued by the minister of national defence.[19]

This raises the second key area of reform: the procedural changes. The clear intent of the amendments is to steer CSE foreign intelligence and cybersecurity activities that might implicate Canadian constitutionally-protected information through a section 8-defensible regime. I think it comes very close to doing so, subject to one proposed fix that would confirm this result.

But before addressing that point, it is important first to describe the new process. The minister of national defence will continue to issue ministerial authorizations. This will place CSE activities on-side other law that might otherwise bar their collection, such as Part VI of the *Criminal Code* on electronic intercepts. To be clear, these will not be target-specific authorizations, but as in the current system, ones that authorize "activities or classes of activities". CSE cannot undertake activities requiring an authorization without first acquiring it.[20] This is, in many respects, an echo of the current rules.

The key difference between C-59 and the current regime is, however, the requirement that any ministerial authorization be vetted and approved, in writing, by the IC, before it is valid.[21] This is not *after the fact* review, but *advance* oversight by the IC – a judicial officer. This is the "warrant-like" feature of the proposed C-59 regime, although again the authorization will lack the specificity of a conventional warrant.

Whether this system satisfies the Charter will depend on a court being persuaded of the constitutionality of a novel authorization system that approves activities and classes of activities lacking the specificity of a regular warrant. As I have suggested, I believe this specificity requirement must be relaxed where the collection is foreseeable, but only incidental. I would add that the constitutionality of the system would be enhanced by robust rules on the management of this incidentally collection information.

---

19 IC Act, s.14.

20 CSE Act, ss. 27, 28, 51.

21 CSE Act, s.29.

These are not spelled out in the bill, but the CSE is instructed to put privacy rules in place to protect the privacy of Canadians and persons in Canada.[22]

Greater legislative granularity might have been preferred, but may not be required so long as these are meaningful rules – which, incidentally, will be subject to review by the specialized review body also being established by C-59. I continue to worry about the prospect of administrative de-minimization of Canadian information and sharing with other Canadian security services, at least where those services do not come with warrants. On the other hand, if the C-59 IC vetting system does meet section 8 standards, that brings the incidentally-collected information within the "constitutional tent" *at the point of CSE acquisition*. Further sharing with other services then might be within a constitutional safe-harbour that does not exist at present.[23]

BUT C-59 FALLS SHORT OF COMPLETELY CURING THE CONSTITUTIONAL DOUBTS

My single concern is whether the C-59 changes will steer *each and every* activity that might implicate constitutionally-protected information through the IC-vetted ministerial authorization process. And here, I have profound doubts. For foreign intelligence and cybersecurity, the only clear "trigger" obliging a trip to the minister for authorization (that triggers the IC's involvement) is the possible contravention of any "Act of Parliament".[24] But the collection of metadata, for instance, does not clearly contravene an Act of Parliament, if one accepts the government's narrow construal of "private communication" in Part VI of the Criminal Code.

---

[22] CSE Act, s.25. The CSE Act also establishes the broad contours of a new information sharing system – that is, the sharing of incidentally collected information with partner agencies. CSE Act, s.44. Again, the standard is general, but does anticipate further details developed my ministerial designation. CSE Act, s.46. Done properly, this probably will satisfy another constitutional headache: ensuring standards applied in the sharing of constitutionally-protected information that meet the expectations of the Supreme Court in *Wakeling v United States*. 2014 SCC 72. Depending on how you read the split court decision in that matter, protective standards should include: information-sharing that is prescribed by a reasonable law; precision in terms of the purpose of the disclosure, sufficient precision in terms of to whom the disclosure was made, and (most importantly) the existence of safeguards. So even if you have a constitutional law authorizing sharing, you must still exercise it reasonably, and that means no information sharing where you know or ought to know that it will exploited to visit maltreatment on a person. In fact, it is my understanding that the government is now moving ahead with revamped ministerial directions for CSE designed to guard against this very possibility. The package may be, therefore, enough to pass muster.

[23] Note also the discussion *ibid* of the *Wakeling* issue.

[24] CSE Act, s.23.

In these circumstances, there is no clear *obligation* to seek authorization for the type of information that is now generating the greatest constitutional controversy. Another provision of the statute does specify that CSE "may acquire information relating to a Canadian or person in Canada incidentally in the course of carrying out activities" under a ministerial authorization.[25] But this section seems simply to affirm that incidental collection may occur within the scope of a ministerial authorization. It is not a straightforward obligation to seek such an authorization in the first place.

THESE DOUBTS WOULD BE RELIEVED BY A MINOR AMENDMENT

The uncertainty of the current drafting may be easily remedied. Over the course of the last several months, I have canvassed several possibilities, each with its own pros and cons. My current recommendation is simply to broaden the "trigger" to reach more than just violations of an "Act of Parliament" but also "reasonable expectations of privacy", the constitutional threshold for a Charter s.8 interest.

The risk is that uncertainty about the reach of this concept may leave considerable latitude in the hands of the government. On the other hand, a more defined concept tied, for example, to metadata may stale-date, as technology changes. On balance, therefore, I consider it wise to codify exactly the standard that must be met if the CSE is to avoid constitutional infractions in its activities.

A FAILURE TO CURE THIS SHORTCOMING MAY RENEW CONTROVERSY

I will end with a final point. These observations are very lawyerly, and may appear unimportant or nitpicky. Recent history has repeatedly suggested, however, that loose and uncertain legislative drafting in national security law may inspire suspicion of inherently secretive services. Moreover, if we fail to cure the existing problem with CSE's collection authorization process, a court may ultimately determine that CSE has been collecting massive quantities of data in violation of the constitution. Such a finding would decimate relations with civil society actors, placing CSE squarely in the cross-hairs of a renewed controversy and making it very difficult for private sector enterprises to partner with CSE on cybersecurity without risking reputational fall-out themselves.

With C-59, we have a chance to minimize this kind of problem. We all stand to benefit from a statute that gets the law out of the way as a source of doubt in CSE's foreign intelligence and cybersecurity function.

---

[25] CSE Act, s.24(4).