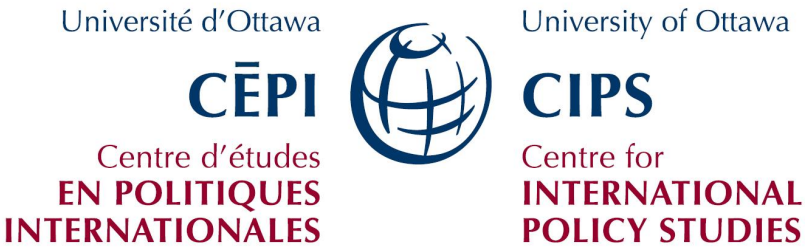


CIPS WORKING PAPER

# CSE AND LAWFUL ACCESS AFTER SNOWDEN

A Research Report funded by the Research and Knowledge Project Fund of the Office of the Privacy Commissioner of Canada[1]

**Wesley Wark**

Visiting Professor

Graduate School of Public and International Affairs
University of Ottawa

[1] The author wishes to acknowledge the financial support of the Office of the Privacy Commissioner of Canada in making this research possible. The views presented in this study are the author's alone and do not represent the official position of the Office of the Privacy Commissioner. The funding for the project, under a Contributions Agreement, allowed the hiring of several research assistants—MA candidates from the Graduate School of Public and International Affairs, University of Ottawa—whose help was invaluable in compiling research materials and data for the project. The students who worked on the project were Robert Matthew Ritchie for the first phases of the project in the summer and fall of 2015; and Evan Sweet, Vanessa Sunahara and Oxana Drozdova in the final stages of the project in early 2016.

# June 2016

TABLE OF CONTENTS

## ABOUT THE AUTHOR

Wesley Wark is currently a visiting professor at the University of Ottawa's Graduate School of Public and International Affairs. He is a professor emeritus at the University of Toronto's Munk School of Global Affairs. He holds a Ph.D. from the London School of Economics and an MA from Cambridge University.

He served for two terms on the Prime Minister of Canada's Advisory Council on National Security (2005-2009) and served on the Advisory Committee to the President of the Canada Border Services Agency from 2006 to 2010. From 1998 to 2001 he was on an Executive Interchange Canada appointment with the Privy Council Office, where he wrote a draft classified history of the Canadian intelligence community after 1945. He has appeared before Parliamentary committees on numerous occasions as an invited expert on matters dealing with security and intelligence. He has also served as an expert witness in several matters before the Federal Court of Canada, including on security certificate cases.

Professor Wark's most recent book is an edited volume: Secret Intelligence: A Reader (2009). He served as co-director of a research team at the University of Ottawa engaged on a study of the impact of national security and counter-terrorism policies on Canadians since 9/11, funded by Public Safety's Kanishka Project. He authored a study for the Canada 2020 Institute on accountability for security and intelligence, "Once More into the Breach: Strengthening Canadian Intelligence and Security Accountability" (March 2015). His essay on "C-51 and the Canadian Security and Intelligence Community: Finding the Balance for Security and Rights Protections," appeared in Edward Iacobucci and Stephen Toope, eds., After the Paris Attacks: Responses in Canada, Europe and Around the Globe (University of Toronto Press, 2015). His essay on "The Endless War?: Counter-Terrorism in the Early 21st Century" was a feature article in Global Brief (Spring/Summer 2015).

Professor Wark writes and comments extensively for the Canadian and international media on issues relating to intelligence, national security and terrorism. He was recently honoured with the "Excellence in Media Relations Award" by the University of Ottawa.

He can be reached at Wesley.Wark@uottawa.ca

# INTRODUCTION

On a Friday in early June 2013, a leak of a highly classified US intelligence document concerning a surveillance program called PRISM, which tapped into the servers of major US internet companies such as Apple, and Google, made the headlines of the UK newspaper, *The Guardian*[2]. It was the beginning of an unprecedented saga that roiled US politics and the US intelligence community, and impacted many other countries around the world, including Canada, because it touched on the sensitive issue of the interception of global and domestic communications. The source of the leaks was soon identified as Edward Snowden, a National Security Agency (NSA) contractor. Snowden had fled to Hong Kong and had chosen to give selected media representatives whom he trusted (especially Glenn Greenwald, then working for *The Guardian* newspaper, and documentary film maker Laura Poitras) full access to the material he had acquired, leaving it to them to frame the news reporting. Snowden also included, with a preliminary batch of NSA records he sent to Greenwald, a manifesto that he wanted to publish. It read:

"The US government, in conspiracy with their client states, chiefest among them the Five Eyes—the United Kingdom, Canada, Australia, and New Zealand—have inflicted upon the world a system of secret, pervasive surveillance from which there is no refuge. They protect their domestic system from the oversight of citizenry through classification and lies, and shield themselves from outrage in the event of leaks by overemphasizing limited protections they choose to grant the governed…"[3]

This was the beginning of Snowden's own perilous journey into whistleblowing, into exile, and into a version of fame, and the beginning of a massive and sustained period of media reporting about a subject that rarely made its way into the news—the practice of global signals intelligence.

Canadians first learned about the Snowden leaks through access to the global media and filtering of stories by Canadian media outlets. Global News, for example, gave an early Canadian twist to the PRISM story by citing concerns from Canadian Privacy Commissioners (federal and provincial) about the implications for Canada[4]. It took a few months for the Canadian penny to drop more resoundingly, but in October 2013,

---

[2] Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps into user data of Apple, Google and others," *The Guardian*, June 7, 2013, at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; The story of how Snowden contacted Greenwald, and the handling of the Snowden materials is told in Glenn Greenland, *No Place to Hide: Edward Snowden, The NSA and the US Surveillance State* (McClelland & Stewart, 2014); see also the documentary by Laura Poitras, "Citizen Four."

[3] Glenn Greenland, *No Place to Hide: Edward Snowden, The NSA and the US Surveillance State* (McClelland & Stewart, 2014), pp. 23–24.

[4] http://globalnews.ca/news/624105/u-s-prism-surveillance-program-puts-canadas-privacy-czar-on-alert/

Brazilian media reported on a Snowden leak that implicated Canada's signals intelligence agency, the Communications Security Establishment (CSE), our partner organization with the NSA, in a project to map the communications of a Brazilian government ministry, the Department of Mines and Energy, with a view to future exploitation. This was clearly a Five Eyes enterprise and it raised early concerns about governance of Canadian signals intelligence and decision-making around foreign targets[5]. One veil had been stripped away, and more were to come, particularly with regard to indications of signals intelligence operations touching on Canadian domestic targets. Glenn Greenwald promised, at the time of the Brazil revelation:

"There's a lot of other documents about Canadians spying on ordinary citizens, on allied governments, on the world, and their co-operation with the United States and the nature of that co-operation that I think most Canadian citizens will find quite surprising, if not shocking, because it's all done in secret and Canadians are not aware of it."[6]

Canadian media naturally pricked up their ears. The Greenwald hint resulted in a distinctive development that saw the Canadian Broadcasting Corporation (CBC) forge an arrangement with him in late 2013 to allow for special (exclusive) access to Snowden documents relating to Canada and its signals intelligence agency, the Communications Security Establishment (CSE). The CBC for a time fielded a special team of reporters to handle the material and worked out their own protocol around reporting issues of national security involving classified documents. The CBC thus became the leading Canadian narrator of the Snowden leaks story, with a focus on their Canadian content, reprising a role that the CBC had played, some 40 years earlier, in creating the very first TV documentary, "The Fifth Estate—the Espionage Establishment," exposing to public view the CSE's predecessor, The Communications Branch of the National Research Council (CBNRC).[7]

The first story to emerge from this media arrangement was published by the CBC under a shared byline involving the CBC's Greg Weston, then its lead reporter on

---

[5] I discussed these concerns in a piece written for the *Globe and Mail*, "Why is Canada spying in Brazilian industry? Time to examine priorities," October 8, 2013, at: http://www.theglobeandmail.com/opinion/why-is-canada-spying-on-brazilian-industry-time-to-examine-priorities/article14731233/

[6] Glenn Greenwald, quoted in a CBC New story, Laura Payton, "Brazil Summons Canadian Ambassador over spying allegations," October 7, 2013, at: http://www.cbc.ca/news/politics/brazil-summons-canadian-ambassador-over-spying-allegations-1.1928147

[7] The CBC documentary led the government to move the Canadian signals intelligence organization out of its nominal home in the National Research Council (where it had been hidden since 1946) and place it within the Department of National Defence, where it hoped its budget and practices would be better shielded from public scrutiny. At the same time, the organization received a new name, The Communications Security Establishment.

national security issues, and Glenn Greenwald, on November 27, 2013.[8] At the time of writing of this report, the last Canadian media story concerning Snowden materials with Canadian content was published by the CBC in May 2015[9]. In the period between November 2013 and May 2015, the CBC published an unprecedented string of stories regarding the intelligence gathering operations of the Communications Security Establishment. Many of these stories were accompanied by redacted versions of the Snowden documents. The stories and documents prompted a rare public discourse about CSE's powers and its legitimacy. This public debate was joined by the government, by CSE, by review bodies, by Parliament, by civil liberties organizations and by independent experts and advocates of all stripes. As promised by Greenwald, there were some surprises and shocks along the way. "Lawfulness" questions hung over this entire debate.

In a previous research study produced for the Office of the Privacy Commissioner in March 2012, prior to the Snowden leaks, I canvassed a range of responses to the challenges of surveillance that might help ensure that privacy and national security can be reconciled.[10] The Snowden CSE leaks provide a fresh opportunity to consider this question and to zero in more strongly on the nexus of that reconciliation posed by the challenges around the right conduct of signals intelligence as it impacts Canadians.

If the stream of Snowden revelations have effectively ended (and a question mark has to remain about that) what has remained are a whole series of important public policy issues with which states continue to struggle.[11] My focus is on the question of the impact of the Snowden documents on Canadian policy, and in particular on what the Snowden revelations tell us about the national security and democratic challenges of providing for legitimate access by intelligence services, and in particular by a signals intelligence agency, to communications, including the private communications of Canadians.

---

[8] CBC's access to the Snowden documents and its relationship with Glenn Greenwald were first revealed in an editorial note on November 28, 2013, by David Walmsley, the CBC's Director of News Content, see: http://www.cbc.ca/newsblogs/community/editorsblog/2013/11/reporting-on-secrets-and-national-security.html

[9] This research project was first conceived in the fall of 2014, when the Snowden leaks of were still appearing through the media in an abundant flow. Research commenced, following formal approval, in late June 2015 and concluded in March 2016. Even though the Snowden leaks had ceased prior to the launch of the research, there was a still a small but substantial body of Canadian content material in the "Snowden archives" to reflect on.

[10] Wesley Wark, "Electronic Communications Interception and Privacy: Can the Imperatives of Privacy and National Security be Reconciled?" March 2012. Available at: http://www.cips-cepi.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf

[11] Edward Snowden maintains a life in exile in Russia and a presence on the internet. Glenn Greenwald went on to leave *The Guardian* newspaper and, with financial backing, created an independent media organization, *The Intercept*, which publishes online stories about a range of security issues; it has begun to make available in its original form some of the unpublished Snowden "Archive." See *The Intercept*, at: https://theintercept.com

Two issues are front and centre: 1) the nature of, and control over, access; 2) the construction of legitimacy. The project has both descriptive and prescriptive dimensions; it is designed both to aid in understanding how the Canadian state currently deals with communications access issues in the context of signals intelligence operations, and to raise important questions about the shape of the future.

## 1. THE SNOWDEN "ARCHIVE" AND ITS CANADIAN CONTENT

It should come as no surprise that in a digital age and given the public interest in the documents leaked by Edward Snowden, an extraordinary variety of web-based archival platforms have been created to house and comment on the NSA sourced material. The longevity of these non-governmental archival sites and the extent to which they will be updated and maintained, remains to be seen, but at the moment they provide for substantial access to the original Snowden documents and many also contain contextual or media commentary.[12]

These archival platforms can be broken down, for the purposes of this study, into three types:

1. Snowden document repositories with general content

2. Canadian-specific Snowden repositories

3. Web sites devoted to comment, specifically on the Canadian dimensions of the Snowden revelations

In addition, Professor Andrew Clement, from the University of Toronto, and a colleague, Evan Light, have created something they call the "Snowden Archive in a Box," a stand-alone device in two formats that allows access to the "Snowden Surveillance Archive" using local wi-fi rather than a wider network and includes a built-in "packet sniffer," to display any traffic that would have been interceptable.[13]

[12] One of the original intentions behind this project was to create a document compilation of Snowden material that referenced Canadian signals intelligence activities. Two online collections of Canadian-specific documents were independently created before this project got underway; they are discussed and utilized in my report. I wish to thank Robert Matthew Ritchie, the first research assistant employed on the project, for his assistance in compiling data on key Snowden web-based archives, which is presented as **Appendix A**

[13] https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/portablearchive.html

Many of the general Snowden document repositories have been created by US civil liberties and privacy NGOs, seized by concerns about mass surveillance. What is more surprising, given the relatively limited quantity of Canadian materials in the Snowden documents, and the more episodic and less intense temperature of the Canadian debate over surveillance, is the extent to which Canadian-originated and Canadian-specific archival platforms have been created.

For the purposes of accessing Canadian-specific CSE records from the Snowden leaks, two sites in particular are valuable: the CBC archive of news reporting on the Snowden leaks, collated as "Canada's Snowden files;" and a compilation created by Dr. Christopher Parsons, a post-doctoral fellow at the University of Toronto, called "The Canadian SIGINT summaries." The CBC's "Snowden files" contains 9 CSE documents derived from the Snowden leaks and reported on by the CBC. This document set is not complete, as it only encompasses the material that the CBC acquired after it had reached its agreement with Glenn Greenwald and also only includes documents that the CBC decided to report publicly on. Dr. Parsons' "Canadian SIGINT summaries" contains 27 documents. The reason for the difference is that the additional documents listed in Dr. Parson's collation include records generated by Canada's Five Eyes partners, especially the NSA and Britain's GCHQ, which relate to Canadian activities. The CBC Snowden files are incomplete; while the Parsons' set is not restricted to CSE-originated documents. In collating CSE originated records from among the various Snowden archive sets, I have identified 14 documents, with an additional 2 directly relating to relations between CSE and the NSA and providing comment on CSE operations.[14]

To provide an idea of the sample size of Canadian material versus the larger public Snowden archive, the Courage Foundation, an NGO authorized by Edward Snowden to support his cause, lists a total of 579 Snowden documents made public from 2013 to the present. Its search engine function tallies 30 documents relating to Canada; and 13 specific to the Communications Security Establishment. If the overall Courage Foundation data set is reasonably accurate, this would indicate that Canadian/CSE material in the Snowden leaks represents about 5.2% of the total.

CSE-originated material in the Snowden archive is small in number and inevitably very fragmentary and atomized in nature. It represents a date range from c. 2009 to the spring of 2013. How and why this selection of CSE documents ended up in the material that Snowden collected from the NSA database and subsequently leaked remains unknown. Any interpretation of this material has to take into account that it represents only a tiny portion of a vastly larger CSE operational archive; that the documents exist out of any larger context; that some of them may be out of date; and that some of the material has been redacted by the media sources to whom Snowden entrusted it. The challenges of interpretation are compounded by the fact that the

[14] A list of the 14 CSE documents can be found at **Appendix B**

documents represent, for the most part, highly classified briefings on complex technical issues prepared by CSE officials for delivery at sessions with their Five Eyes counterparts. They are not policy documents and were never written for a general audience of the sort that they are now exposed to. The Snowden "archive," both the general set and the Canadian-specific material, is not an archive in the usual meaning of the word. If you can imagine a magpie avatar in the secret world, it is a magpie's stolen "treasure" and like such "treasure," a real jumble.

The 14 CSE documents that I have identified in the Snowden archive can, nevertheless, be subject to characterization and, within limits, analysis. These records amount to a rare collection of original sources on CSE operations and their value stems in part from this breach of long-held secrecy. This tiny cache of once highly classified documents contains material that speaks to four distinctive issues:

*Canadian foreign intelligence activities targeting foreign state entities*

*Canada's role in the Five Eyes signals intelligence community, including its partnership with the US NSA*

*Unique Canadian SIGINT operations and tradecraft*

*Canadian cyber security operations, including cyber counter-intelligence*

All of these issues reflect the hybrid nature of CSE in a post 9/11 world and the complex nature of its current mandate.

***The Snowden "archive," both the general set and the Canadian-specific material, is not an archive in the usual meaning of the word. If you can imagine a magpie avatar in the secret world, it is a magpie's stolen "treasure" and like such treasure", a real jumble.***

## 2. CSE'S MANDATE

Between its post-war creation in 1946, and 2001, CSE and its predecessors operated under secret Orders in Council. In 2001, following the 9/11 attacks, the Canadian Government passed omnibus anti-terrorism legislation (Bill C-36), which included statutory provisions for CSE, involving amendments to the National Defence Act. These provisions are important in three particular ways: they establish a hybrid, multi-role mandate for CSE; they spell out the role of the Minister of National Defence in authorising CSE collection that might "inadvertently" involve the interception of Canadians' private communications; and they confirm the role of the review body for

CSE, the Office of the CSE Commissioner, which had been operating since 1996.[15]

The Anti-Terrorism Act codified the hybrid, tripartite mandate of CSE, under three headings, usually referred to as Parts A, B, and C.[16]

Its Part A mandate involved its traditional foreign intelligence collection role, updated to reflect the new information environment in which CSE operated. It read: *"to acquire, and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with the Government of Canada intelligence priorities."*

Its Part B mandate reflects CSE's relatively new role in cyber security protection for federal government critical information infrastructure. It read: "*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"*

CSE's Part C mandate involved the provision of technical assistance to other elements of the Canadian security and intelligence community. It read: *"to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."* The lawful duties element is important because it signals the fact that when engaged in Part C mandate operations, CSE operates on behalf of agencies that have acquired their own lawful authority for the interception of communications, usually through warrants. CSE thus shares the legal umbrella of those authorities.

CSE's enabling legislation in the 2001 Anti-Terrorism Act largely confirmed a set of roles it was already undertaking, wrapped in a new operational focus on counter-terrorism. But there was one new and unprecedented provision. This provision allowed CSE, under signed Ministerial authorization, to collect "private communications," defined in Canadian law as any communications that originate or terminate in Canada where such communications are attended with a reasonable expectation of privacy [Section 183 of the Criminal Code]. The Act laid out that such private communications could only be collected in fulfillment of either CSE's foreign intelligence mandate (A) or information security mandate (B) and that the Minister would have to be satisfied regarding a set of listed conditions. These conditions were explicitly spelled out in the Anti-Terrorism Act. With regard to foreign intelligence, the legislation specified that a Ministerial authorization to collect the private communications of Canadians could only be granted if four conditions were met:

---

[15] I discussed CSE's new legislation in a previous research project funded by the Office of the Privacy Commissioner. See Wesley Wark, "Electronic Communications Interception and Privacy," March 2012, available at: http://www.cips-cepi.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf

[16] CSE's legislative statute consists of amendments to the National Defence Act, Part V.1, sections 273.61 to 273.7; Available at: http://laws-lois.justice.gc.ca/PDF/N-5.pdf

a) The interception had to be directed [targeted] at foreign entities located outside Canada

b) The interception could not reasonably be obtained by other means

c) The interception was justified by its anticipated value

d) The privacy of Canadians would be protected and information retained or used only if it was essential to international affairs, defence or security

The criteria that had to be met to justify Ministerial authorizations in pursuit of CSE's cyber security (B) mandate were similar, although the value proposition was differently expressed. The criteria upheld the same conditions of the protection of Canadian privacy, the use or retention of private communications only when "essential," and the absence of reasonable alternatives. The value proposition was not based on any balancing of means and end (anticipated value), but framed as a matter of "necessity" in order to "identify, isolate or prevent harm to Government of Canada computer systems or networks."

The Anti-Terrorism legislation also spelled out the functions of the Office of the Communications Security Establishment Commissioner (abbreviated as OCSEC), its official watchdog body.[17] The CSE Commissioner was to have important rules in terms of determining the lawfulness of CSE operations, the fidelity of CSE to Ministerial direction, and the scrutiny of CSE's privacy protections.[18] The legislation provides the CSE Commissioner with specific authority to: "review activities carried out under an [Ministerial] authorization to ensure that they are authorized and report annually to the Minister." While the meaning of this authority might seem opaque, it is important to understand that it does not involve the CSE Commissioner questioning the decisions made by a Minister; the scrutiny is restricted to how CSE operationalized its Ministerial authority to incidentally acquire Canadian private communications.

[17] The CSE Commissioner's mandate is spelled out in the National Defence Act, Part V.1, S.273.63 to S.273.65. The mandate is also included in the annual public reports prepared by the CSE Commissioner for submission to Parliament.

[18] While the CSE Commissioner has taken on a primary role around the scrutiny of privacy protections in the course of CSE activities, the federal Privacy Commissioner retains a potential, independent role under his/her authorities under the Privacy Act.

## 3. THE KEY THEMES IN THE SNOWDEN CSE DOCUMENT SET

CSE's foreign intelligence gathering activities were the starting point for Snowden revelations relating to Canada. The Snowden leaks first spotlighted Canadian SIGINT in a story regarding a Canadian development project to map the communications of Brazil's Mines and Energy Ministry using a Canadian SIGINT system called "Olympia," as a starting point for future potential exploitation. Subsequent to this revelation, from early October 2013, a handful of other Snowden documents provided some indication of Canadian foreign intelligence SIGINT efforts targeting foreign state entities, including efforts against Mexico, and the hosting of signals intelligence collection capabilities in overseas diplomatic outposts.[19]

Several of the Canadian-content Snowden documents speak to the role of the Communications Security Establishment within the Five Eyes alliance. The NSA memo, "NSA Intelligence Relationship with CSEC," published on December 9, 2013, is perhaps the most explicit about Canada's role within the Five Eyes and its links to its US partner. It provided a short history of the US–Canada SIGINT relationship, described Canada as a "highly valued second party partner" (alongside the other members of the Five Eyes alliance, the UK, Australia, and New Zealand), described cooperative targeting, the sharing of technological developments, and an intelligence exchange covering "worldwide national and transnational targets." From a US perspective, Canada was described as offering "resources for advanced collection, processing and analysis, and has opened covert sites at the request of NSA. CSEC shares with NSA their unique geographic access to areas unavailable to the US [material redacted]."[20]

[19] CSE slide deck presentation, "And They Said to the Titans: Watch out Olympians in the House," Christopher Parsons' *Canadian SIGINT summaries*, document 24, dated June 2012, published November 30, 3013. Associated Press, "Canadian Spies Targeted Brazil's Mines Ministry," October 7, 2013; CBC *Canada's Snowden Files*, Laura Payton, "Brazil Summons Canadian Ambassador over spying allegations," October 7, 2013

[20] NSA Information paper, "NSA Intelligence Relationship with Canada's Communications Security Establishment Canada," dated April 3, 2013; published December 9, 2013, Christopher Parsons' *Canadian SIGINT summaries*, document 21. CBC's *Canada's Snowden Files*, Greg Weston, Glenn Greenwald, Ryan Gallagher, "Snowden Document Shows Canada set up spy posts for NSA," December 9, 2013.

***Canada's role in the Five Eyes alliance had long been known, and the close partnership between CSE and NSA long understood, but never before had the Canadian public seen this intelligence alliance relationship spelled out***

Canada's role in the Five Eyes alliance had long been known, and the close partnership between CSE and NSA long understood, but never before had the Canadian public seen this intelligence alliance relationship spelled out. The original agreement (known as CANUSA) between Canada and the US that ushered Canada into what would become the Five Eyes partnership, dates back to 1949 and remains under wraps, although the foundational records from the UK and the US spelling out the origins of a postwar signals intelligence alliance, are now available in their respective national archives.

The Snowden document set also describes some unique Canadian SIGINT capabilities and operations. Two examples stand out, relevant to this research project. One described CSE's "Levitation" project, which targeted Free File Upload (FFU) sites on a massive scale. Levitation depended for its raw material on a "special source" codenamed "Atomic Banjo," which allowed for the supply of 10–15 million so-called "download events" per day, from 102 different FFU sites. The nature of "Atomic Banjo" was not specified in the Snowden leak. This massive quantity of data was processed through two Five Eyes-operated databases—the NSA's "Marina," which contains intercepted metadata; and GCHQ's "Mutant Broth," also built on metadata.

The public release of this document on the "Levitation" project occasioned media commentary on two key issues—the effectiveness of mass surveillance sweeps of data, and the privacy implications of such programs. One source contacted by the CBC for comment, Tamir Israel, who works for the University of Ottawa's Canadian Internet Policy and Public Interest Clinic, argued that "the invasion of privacy is disproportionate to the benefit." Glenn Greenwald, who contributed to reporting on this document, urged Canadians to ask "tough questions" about spending on "very sophisticated means of surveillance," when terrorist plotters (he cited the Boston Marathon bombers and the Charlie Hebdo attackers in Paris) remained undetected.[21]

Another CSE Snowden document that outlined a unique Canadian operation was even

[21] CSE slide deck, "Levitation and the FFU Hypothesis," unknown date of origin, but after March 2012, published January 27, 2015, Christopher Parsons' *Canadian SIGINT summaries,*" document 9; CBC *Canada's Snowden Files,* Amber Hildebrandt, Michael Pereira and Dave Seglins, "CSE Tracks Millions of Downloads Daily," January 27, 2015

more controversial. This involved the so-called "Airport Wi-Fi" project, revealed in a Snowden leak of a document with a more banal title, "IP Profiling Analytics and Mission Impacts." What was particularly controversial about the airport Wi-Fi project was that it used metadata collected from public wireless traffic at a major Canadian airport to develop what the CSE called a "model" for operations under its foreign intelligence mandate designed to allow for the geolocation of IP [internet protocol] addresses and to try to match specific personal identifiers across public wi-fi and land line telephone communications. The model was meant to test the ability to locate and follow a terrorist suspect abroad by correlating wi-fi usage and land-line telephone communications.

Building a model for a foreign intelligence operation under CSE's part A SIGINT mandate using domestic metadata caused much concern with regard to privacy impacts, data retention issues, and blurred legal authorities. The then Ontario Privacy Commissioner, Ann Cavoukian, was particularly vocal in denouncing what she saw as a totalitarian form of surveillance of Canadians.[22] Both the chief of CSE, then John Forster, and the Government, were forced to explain and defend the airport Wi-Fi project.

As with the "Levitation" project, the ability of CSE to engage in the airport Wi-Fi study for operational modeling was dependent on access to raw telecommunications data, from an unnamed "special source."[23] This material comprised a metadata compilation of two weeks of travellers' wireless data from the [unnamed, but presumed to have been Pearson International in Toronto] airport Wi-Fi system.

Both the Airport Wi-Fi and Levitation documents raise inevitable concerns about CSE's access to and use of Canadian communications, especially metadata, providing a parallel of sorts to the much more extensive collection of NSA records released by Snowden and the debate they have generated about mass surveillance and the targeting of US citizens' communications.

## 4. SNOWDEN CSE LEAKS ON CYBER SECURITY

There is one particular subset of the CSE-originated material in the Snowden archive that warrants special attention in terms of issues around access to Canadian communications. This sub-set of documents represents 50% (or 7 of the 14 records) of the Canadian CSE material now publically available from Snowden; the sub-set

[22] Quoted in Greg Weston, Glenn Greenwald, Ryan Gallagher, "CSEC used Airport Wi-Fi to track Canadian Travellers: Edward Snowden documents," January 30, 2014.

[23] CSE, "IP Profiling Analytics and Mission Impacts," dated May 10, 2012, published January 30, 2014, Christopher Parsons' *Canadian SIGINT summaries,* document 19. CBC, *Canada's Snowden Files,"* Greg Weston, Glenn Greenwald, Ryan Gallagher. "CSEC used airport Wi-Fi to track Canadian travellers," January 30, 2014

references CSE's cyber security operations, conducted under its Part B mandate.[24]

In order to fulfill its protective Part B mandate, CSE of necessity is involved in the interception of communications that might constitute private communications under Canadian law. It has to monitor potentially malicious traffic within the federal government information infrastructure, as well as malicious actor traffic entering and leaving that information space. Under the conditions attached to the issuance of Ministerial authorizations for cyber security operations, CSE is enjoined to ensure "satisfactory" measures for the protection of the privacy of Canadians. But otherwise the strictures are pretty weak, leaving CSE cyber security operations with wide latitude. This is not to say that CSE's legislation permits unchecked mass surveillance for cyber security purposes, but the limitations involve calculations around what is necessary "to identify, isolate, or prevent harm to Government of Canada computer systems or networks." As for retaining or using information derived from cyber security operations, the law, as we have seen, stipulates that this must be "essential" to the protection of Government of Canada information infrastructure. In theory, the Minister (of National Defence) makes these determinations. In practice, CSE does.

CSE's cyber security operations have the legislative equivalent of rocket fuel, but they are also conducted in the face of serious national security threats, and enormous technological challenges. Wide legal latitude for cyber security operations reflects these national security and technological imperatives. In testimony before the Senate Standing Committee on National Security and Defence on March 21, 2016, the CSE chief, Greta Bossenmaier, stated:

"The number of nation-states and non-state actors that possess the capacity to conduct persistent, malicious cyber operations is growing and Canada is an attractive target…CSE's sophisticated cyber defence mechanisms block over 100 million malicious cyber actions against the Government of Canada every day[25]

On its website, CSE indicates a different cyber-attack statistic—"every day, thousands of attempts are made to access and infiltrate government networks."[26]Whatever the precise number of daily attacks and their nature, the statistics are staggering. CSE makes clear that its cyber defence operations include working to detect unauthorized intrusions, block them and repair any damage. CSE's foreign intelligence capabilities are described as important for this effort. Again, from the CSE website, we learn:

"CSE uses our foreign signals intelligence capabilities and information from our allies to better understand the people and organizations who are trying to exploit our

[24] This subset of Snowden CSE records is listed in Appendix C

[25]Statement of the Chief, CSE, before the Senate Standing Committee on National Security and Defence, March 21, 2016 [add link]

[26] CSE website, "Cyber Defence," https://www.cse-cst.gc.ca/en/group-groupe/cyber-defence

systems and the techniques they try to use. We also learn as much as we can about evolving cyber threats and the best ways to detect and prevent them. With this knowledge, CSE is better positioned to stop nefarious cyber activities and intrusions **before they reach our networks [**emphasis added]…[27]

Scrutiny of CSE's cyber security operations (under its Mandate B) bring us into an arena where some form of mass surveillance of communications traffic is a necessity, where the national security stakes are high and so are the technological challenges, and where the authorization regime that allows for the interception of Canadians' private communications is of wide latitude. As CSE indicates, its cyber security operations require it to monitor Canadian internet space and it does so uniquely under its Mandate B.[28] CSE's cyber security operations also reach into its foreign SIGINT capacity (Mandate A) and its involvement with Five Eyes partners. When it comes to issues of the construction of "lawfulness" around access to, and use of, Canadian communications, CSE's cyber security operations may pose the most significant questions of all of its varied activities under its three part Mandate.

The seven available CSE documents referring to cyber security operations take on special importance in this regard. Yet they have not been the focus of public and media attention. Again, a caution is warranted. The seven documents, although they represent an unprecedented piercing of the veil of secrecy, are a tiny fragment, date between 2009 and 2011, are technical in nature, and in some cases speak to future planning, which may or may not have been realized. In an engagement with CBC, CSE itself references this set of documents by saying that:

> the leaked materials are dated documents, and some explored possible ideas to better protect the Government of Canada's information systems while also seeking cost efficiencies. As a result, information in these documents does not necessarily reflect current CSE practices or programs, or the degree to which CSE has visibility into global or Canadian infrastructure…[29]

What this small set of documents does reveal is nevertheless important. It provides insights into organisational changes to meet the cyber security threat, into the nature of scanning systems, the reliance on metadata collection and analysis, the desire to create a layered system of defence, the intertwining of Canada's cyber security efforts with those of its Five Eyes partners, and desire to move beyond a passive defensive posture to engage in more offensive cyber operations.

---

[27] Ibid.

[28] CSE response to CBC questions, March 6, 2015, available at: http://s3.documentcloud.org/documents/1690243/csestatements.pdf

[29] CSE response to CBC questions, March 2, 2015, available at: http://s3.documentcloud.org/documents/1690243/csestatements.pdf

The leaked Snowden documents (mostly 2009 to 2011) indicate that CSE created at least two new units to enhance cyber security and was intent on boosting its research and development capacity. One of the new units was a CCNE team (Counter Computer Network Exploitation), probably formed in 2010. It represented the cyber equivalent of a counter-intelligence effort, designed to improve CSE knowledge about malicious actors engaged in network exploitation, to provide "situational awareness" and to allow CSE to review its own operational security. The CCNE team utilized a CSE threat detection platform called "EONBLUE," which had been years in development, and itself involved the deployment of a global array of some 200 sensors (many of these sensor platforms were presumably deployed by Five Eyes partners but available to Canada). CCNE and other dimensions of its cyber security effort relied on the ability to apply network traffic analysis though access to "Special Source" (SSO), warranted traffic, and 2nd party (e.g. Five Eyes) collection "in raw, unprocessed form."[30]

The EONBLUE sensor detection platform was also discussed in a separate Snowden/CSE document which highlighted its capabilities for both the tracking of known cyber threats based on message "signature," and the discovery of new threats, based on anomaly detection. EONBLUE operated alongside a detection program called "Photonic Prism" which surveiled Government of Canada cyber communications. Both apparently involved message "packet" inspection. Photonic Prism was a Mandate B tool that monitored three message streams: Domestic to Government; Foreign to Government; and Government to Government. EONBLUE was described as a Mandate A (and C) instrument which tapped into the global information infrastructure to monitor its own traffic streams, described as: Foreign to Domestic; Foreign to Foreign; and Domestic to Domestic. What this document was proposing, as of 2009, was the building of a spectrum of cyber security operations from defensive network monitoring of the type provided by Photonic Prism, all the way to what were called "active operations" in Computer Network Exploitation, including various "disruption" (covert) operations in an adversary's network and infrastructure space. A special program called "Covenant" was deployed to assist in Section 16 operations (e.g. CSIS monitoring of foreign intelligence within Canada involving CSE under its Part C Mandate).[31]

Apart from an ambitious vision to combine defensive and offensive cyber security operations, and bring the cyber security and foreign intelligence missions of CSE closer together, the briefing on CSE's cyber threat capabilities also indicated the scale on which domestic sensors were operating. In 2009 this involved storing of 300TB of

[30] "'CSEC SIGINT Cyber Discovery: Summary of the Current Effort,' Discovery Conference, GCHQ, November 2010, "https://assets.documentcloud.org/documents/1690221/doc-4-csec-sigint-discocon-2010.pdf

[31] CSEC "Cyber Threat Detection," https://assets.documentcloud.org/documents/1690222/doc-5-cyber-csec-sdf-gchq-nov2009.pdf

what "full take" data for the purposes, it was stated, of historical analysis and anomaly detection. CSE had also developed an algorithm based botnet detection system for metadata exploration which was deployed at CSE SSO (special source operation) sites.

The CCNE team, involved in higher-end cyber security exploitation, is mentioned in another of the leaked Snowden documents, this time in a presentation in June 2010 at a conference organised by the NSA. This document told the story of one CCNE success, which involved the uncovering of an intruder operation codenamed "Snowglobe" which CSE was able to technically identify and profile and which evidence suggested was a French state implant operation. More broadly, CSE was interested in efforts to "deconflict" CCNE activities, so as to be able to identify both friendly and non-friendly/foreign actors operating covertly against the same network targets. As CSE indicated "State-sponsored landscape is very busy…"[32]

A third CSE document from 2010 discussed the work of a new unit called N2E, which was designed to shift the focus of CSE cyber security operations from what was described as "firefighting" to "hunting." The document noted use of an alert system for emailing scanning called "Pony Express." This system processed 400,000 emails in the Government of Canada system per day; sent 400 for internal CSE alert analysis; and typically reported about 1% of these (of 4 per day) to client departments. But the CSE feeling at the time was that the program was unsustainable because of mounting information overload, changes in cyber-attack strategies (in particular with regard to phishing attacks) and because front-line analysts had to handle too much metadata. Instead CSE looked to build a predictive system to move away from the scanning of all email traffic to an identification of suspicious traffic based on various criteria that would reduce the amount of traffic that would undergo what was called a "deep scan." As of 2010, the N2E team was still being built, but had what was described as "excellent access to full take data," and was making progress on policy support, including for the use of "intercepted private communications."

Documents relating to such new units as CCNE and NE2 fitted into a broader picture of efforts on the part of CSE at the time to improve its modest research and development capacity, including a "Cyber Defence Futures" group and the new "Cyber Threat Evaluation Centre."[33]This R and D thrust was visible to CSE's partner, NSA, which in a brief on the current state of NSA–CSE relations noted that "CSEC has

[32] CSEC CCNE, "Pay Attention to that Man behind the Curtain: Discovering Aliens on CNE infrastructure," SIGDEV Conference, NSA, June 2010; https://edwardsnowden.com/wp-content/uploads/2015/01/media-35688.pdf

[33] CSEC CCNE, "Pay Attention to that Man behind the Curtain: Discovering Aliens on CNE infrastructure," SIGDEV Conference, NSA, June 2010; https://edwardsnowden.com/wp-content/uploads/2015/01/media-35688.pdf

increased investment on R and D projects of mutual interest."[34]

The CSE toolkit for cyber security operations, from what can be inferred from this small sample of leaked documents was sophisticated, expansive and drove ambitious planning and visions that looked to merge CSE's SIGINT and cyber security functions, provide an ability to move from passive to more "active" forms of cyber defence, and engage CSE fully in the Five Eyes partnership. Where these fragmentary insights potentially come together is in a single CSE document outlining a project called "Cascade."[35] Cascade looked ahead to 2015 [date of creation unknown, but probably 2011] and described an integrated sensor system involving both the Photonic Prism and EONBLUE platforms. The idea behind "Cascade" appeared to be to bring the two sensor systems into better alignment in what was called a "complete eco-system." It described a "Canadian cyber sensor grid," that would provide for defensive monitoring of Government of Canada information infrastructure, target the gateways connecting the foreign to the Canadian internet space, explore the foreign internet space, and monitor satellite linked communications.

To advance this project, the Cascade document called for three things in particular:

- expansion of CSE's "access footprint" to "increase Special Source access to include all international gateways accessible from Canada"
- build a better system of cyber threat analysis
- enable "effects" operations

By "effects operations" Project Cascade is talking about the ability to engage in active defence, or cyber 'covert operations" to intrude and take action against cyber threat actors and their networks and infrastructure. It noted that Canada, in cooperation with its Five Eyes partners could, when it detected malicious cyber action, "affect change at the core of the internet" through such things as modifying traffic routes, silently discarding malicious traffic, and inserting "payload to disrupt adversaries." The Cascade document noted that such cyber covert operations would require both policy authority, and new technical and analytical capabilities.

The CSE planners involved in drafting Cascade were clear in their minds that current approaches to cyber security based on close defence of cyber systems was inadequate. Their logic was that the defence was being outstripped by the offense, that "gateway/device/end-node protection is not sufficient," and that the only way forward was "rather than plugging one hole at a time, build better layered defence." In

[34] NSA/Central Security Service, Information Paper, "NSA Intelligence Relationship with Canada's Communications Security Establishment," 3 April 2013; https://fveydocs.org/media/documents/nsa-relationship-cse-1.pdf#page=1

[35] CSEC Project "Cascade," http://www.documentcloud.org/documents/1690204-cascade-2011.html#document/p1

the Cascade planners' minds, better layered defence included manipulation of malicious traffic.

Project Cascade drafters were also very clear, as they thought their way into the future of cyber defence, that the Five Eyes partnership was both crucial and needed adaptation. The Cascade authors wanted to move away from independent Five Eyes cyber security operations towards a fully integrated Five Eyes system that would "expose cyber information across the community" and get rid of a system of 2nd party (Five Eyes allies') tasking and targeting requests. On cyber security, the Five Eyes partnership would be turned into a system of mutual and collective cyber defence.

The final slide in the Cascade presentation [audience unknown] has an Orwellian ring: "The Network is the sensor."[36]

The status of project "Cascade" is unknown, including whether its ambitious agenda for change was ever implemented in whole or in part. But its importance ranges beyond the question of its operational status. It tells us about the ways in which cyber security operations were being seen as involving a layered or perimeter system of defence, extending well outwards from defending host infrastructure in the Government of Canada, that cyber threat detection platforms were expanding, that there was end-game interest in going on the cyber "offensive," and that the Five Eyes partnership and its adaptation to meet an evolving cyber threat were crucial to achieving Canadian objectives.

The Cascade document, along with the other suite of CSE cyber security presentations made available through the Snowden leaks, gives us a better generic sense of how internet traffic was accessed. It involved a range of tools, from the passive monitoring of Government of Canada systems achieved through Photonic Prism, to monitoring of gateways connecting the foreign and domestic internet spaces using Special Source operations [SSO] and EONBLUE, to monitoring of the global internet space through EONBLUE and the available sensor global sensor grid, to ingestion of Five Eyes internet take, to satellite downlink monitoring, and into the specialized world of the interception of foreign intelligence communications in Canada through CSE support [Covenant] to CSIS Section 16 collection [usually presumed to target foreign embassies and consulates on Canadian soil]. Warranted communications interception clearly played a role, including in Special Source Operations. Although we know little to nothing about the Canadian development of special source operations, the best assumption is that Canadian operations mirror a much larger US effort revealed by Snowden. In the NSA case, SSO is run from a special directorate, whose emblem is an American eagle with its talons grasping global fiber optic communications lines. In one slide presentation SSO is characterised as "leveraging unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches

[36] ibid

and/or routers throughout the world." This is a reference to the PRISM program. Collection through SSO domestically is described as depending on various US lawful authorities including the Foreign Intelligence Surveillance Act, and the FISA Amendment Act of 2008.[37]

In the Canadian case, lawful access descends into the murkier world of Ministerial authorizations, Five Eyes intelligence sharing, and warranted access in its Part C assistance mandate, using warrants and lawful authority obtained by Canadian agencies requesting CSE's technical assistance. The authority by which CSE acquires internet traffic through SSO for cyber security purposes at the internet gateways to Canada is unclear. The question of lawful access here falls into the protected realm of sensitive sources and methods.

Passive monitoring of Government of Canada communications infrastructure to defend against cyber threats is covered by the Ministerial authorization regime, which, as discussed above, provides wide latitude for the interception of Canadian "private communications." This passive monitoring is accompanied by massive data retention, for the purposes of ongoing analysis and what the documents describe as "anomaly detection." The nature and schedule of data retention as part of its cyber security mission is something which CSE refuses to divulge, on the explicit grounds that "to provide more detail could assist adversaries who want to conduct malicious cyber activity against government networks, or evade our foreign signals intelligence effort." Concerns about cyber security practices may be partly alleviated by CSE assurances that its data retention practices are strictly determined by operational needs and policies and that information gained through cyber security operations is only shared with the foreign signals intelligence side of CSE to advance legitimate SIGINT operations under its Mandate A. But as the Snowden leaks make clear automated monitoring of Government of Canada information infrastructure is not the end of cyber security operations—but rather a part of a more expansive cyber security network that ingests a massive amount of data "take" from a variety of sources.

While public controversy has not specifically attached itself to CSE's conduct of its cyber security operations, it has attached itself to revelations about the global reach of EONBLUE. One Canadian commentator, Matthew Braga, discussed the significance of EONBLUE in these terms:

"It's hard not to overstate the importance of what's happening here. There are more eyes than we realize watching our data as it travels around the world. And it's programs such as EONBLUE that prove the Canadian government is playing a much larger role in monitoring the internet than most might think—with a prowess that

[37] See https://www.edwardsnowden.com/wp-content/uploads/2013/11/sso.pdf

rivals both NSA and GCHQ."[38]

EONBLUE was also cited by the Canadian Privacy NGO, Open Media, as an example of what it calls "mass, suspicionless surveillance." Open Media argues that "Canadians, along with Internet users across the globe, are being caught in CSE's spying dragnet…"[39]

Christopher Parsons has attempted to compare EONBLUE with what is known of similar US systems. As he indicates the comparison is not definitive but at least helps advance questions about Canadian practices. In Parsons' mind the EONBLUE revelations lead to a need on the part of governments "to be more transparent about how they monitor telecommunications traffic, why, and what is done with the monitored traffic."[40]

The Snowden leaks have, in fact, forced the pace of greater transparency around all manner of intelligence operations, and continue to do so. The Canadian government has been tested to respond, both at the political level and through agency heads, Parliament has been engaged, the watchdog agency for CSE has been drawn into the debate, private sector ISPs have been under pressure to provide their own accounts of how they respond to access requests, and NGOs have taken their own steps in advocating change. As the transparency envelope has been nudged outwards, the key questions are what we might have learned about the rationale for domestic communications interception and monitoring; and what we have learned about the strengths and limits of controls around access to Canadians' communications.

**The Government Response to the Snowden leaks; Lawfulness Redux:**

The Government response to criticisms and concerns about CSE intelligence gathering claimed democratic legitimacy in a broad sense. CSE served a national interest and public good in three particular ways: CSE's intelligence work was an important contribution to national security, particularly in the face of terrorism threats; CSE's

---

[38] Matthew Braga, "How Canadian Spies Infiltrated the Internet's Core to Watch What you do Online," available at: http://motherboard.vice.com/read/how-canadian-spies-infiltrated-the-internets-core-to-watch-what-you-do-online ; also Bill Robinson's commentary on the Braga article in Lux et Umbra , "EONBLUE: CSE cyber threat detection system 'deployed across the globe,' February 11, 2015, available at: http://luxexumbra.blogspot.ca/2015/02/eonblue-cse-cyber-threat-detection.html

[39] Open Media, "Canada's Privacy Plan, Case Study #2: The CSE and Mass Surveillance," available at: https://privacyplan.ca/case-study-2-cse-and-mass-surveillance

[40] Christopher Parsons, Telecom Transparency Project, "Defending the Core of the Network: Canadian Vs. American Approaches," available at: https://www.telecomtransparency.org/defending-the-core-of-the-network/ ; also his Op Ed in the National Post, "Canada has a Spy problem," March 23, 2015, at: http://news.nationalpost.com/full-comment/christopher-parsons-canada-has-a-spy-problem

operations were lawful and in accord with its legislative statute; and public confidence in the significance and lawfulness of CSE's operations was affirmed by independent, external review conducted by the CSE Commissioner. While the political leadership of the Canadian government largely refused to be drawn into a public debate about CSE, these arguments provided brief talking points, as Snowden stories warranted. This democratic legitimacy argument was best exemplified in testimony that the Defence Minister, Rob Nicholson, gave to the House of Commons Standing Committee on National Defence on April 3, 2014. Nicholson told MPs that he wanted to "underline the important role that CSE plays in protecting Canada and Canadians." He cited its various contributions to national security, including "providing early warning to thwart foreign cyber threats to the Government of Canada and to critical information infrastructures and networks." He argued that CSE operates "in full accordance with the law" and as a trump reminded MPs that the independent CSE watchdog had never in 17 years of reporting found CSE to have acted lawfully and in fact had noted "CSE's culture of lawful compliance and genuine concern for protecting the privacy of Canadians."[41]

But aside from occasions like this, Government ministers by and large refused to be drawn in detail into the Snowden leaks debate.

Parliament's role in critically scrutinising the legitimacy of CSE SIGINT operations was inevitably hobbled by the absence of any Parliamentary capacity to access classified records or to receive classified briefings. Parliament had to be content with the media reporting. Like media reporting, and to an extent driven by it, Parliamentary scrutiny was episodic.

Although questions about CSE proliferated in the House and Senate during the 2013–2014 session (second session, 41st Parliament), the single most significant moment for Parliamentary engagement on the issue of the legitimacy of CSE intelligence collection came on February 3, 2014, following the Snowden leak about the CSE Airport Wi-Fi project.

On that occasion, the CSE chief, the National Security Advisor, and the Director of CSIS made a rare joint appearance before the Senate Standing Committee on National Security and Defence. The CSE chief's defence of his agency's operations naturally emphasized the themes of lawfulness, the pursuit of CSE's mandate for intelligence collection, and the exercise of Ministerial direction, but also tackled the focus on metadata collection directly. John Forster told the Senate committee that metadata collection was essential to the CSE's ability to understand global communication

[41] Rob Nicholson, Minister of National Defence, testimony at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=e&Mode=1&Parl=41&Ses=2&DocId=6511518

networks, and rather than being targeted at Canadians was used to ensure that CSE could maintain its mandated focus on foreign intelligence and cyber security. What the CSE chief was saying was that CSE lawfulness and appropriate targeting depended on the ability to use metadata from the global information infrastructure. Metadata collection was the lawful solution not a lawfulness problem. The CSE chief tried to turn privacy concerns about metadata collection on their head, while also acknowledging that some Canadian metadata would be netted by CSE as an incidental, rather than deliberate, part of their operations.

***What the CSE chief was saying was that CSE lawfulness and appropriate targeting depended on the ability to use metadata from the global information infrastructure. Metadata collection was the lawful solution not a lawfulness problem. The CSE chief tried to turn privacy concerns about metadata collection on their head, while also acknowledging that some Canadian metadata would be netted by CSE as an incidental, rather than deliberate, part of their operations.***

Forster told the Senate committee:

*When you collect metadata, it is impossible to exclude some Canadian metadata. It is all intermixed together, and good citizens and terrorists are all using the same networks. So when we collect it, we have no way of knowing at that point of disaggregating it until we look at it, and then we use it. If it is Canadian, then we have to make sure we protect the privacy of that information and how we use it. We have conditions from the Minister about how we do that.*[42]

While this statement said little in detail about the metadata collection program, it was designed to be reassuring, and to echo the findings of the CSE watchdog, the CSE Commissioner. The key elements of the statement stressed CSE's ability and determination to separate out "good" actor and "bad" actor communications, and the tight controls around privacy protection and use when captured bad actor communications turned out to be Canadian.

The CSE chief's defence of his agency's operations offered a future hostage to fortune, but was, in early 2014, broadly supported by the CSE watchdog agency, the Office of the CSE Commissioner (OCSEC).

[42] John Forster testimony, Senate Committee on National Security and Defence, February 3, 2014.

## 5. THE CSE COMMISSIONER: 'MAN IN THE MIDDLE' ATTACKS[43]

**5. The CSE Commissioner: "Man in the middle Attacks:**
The CSE Commissioner is mandated under the same legislative statute that governs CSE, passed as part of the anti-terrorism act in 2001, to provide an annual, unclassified report to the Minister of Defence for transmittal to Parliament. These annual reports provide the only authorized window into CSE operations available to the Canadian public.[44]

The CSE Commissioner's function was naturally tested by the unauthorized nature of the Snowden leaks of signals intelligence documents. The test could be characterized as a matter of truth-telling and therefore trust, but to pit a whistleblower against an official review agency may distract from the very different functions of both. The CSE Commissioner's task is, fundamentally, to hold CSE to legal account and to ensure that it remains true to Ministerial direction. Its truth-telling is, in that sense, limited, and is also constricted by the Security of Information Act (including, of course, the way it is interpreted by the CSE Commissioner's office). A whistleblower by definition is challenging the rightness of the conduct of something, not necessarily limited to the question of whether right and lawful align. Edward Snowden was driven by a belief that the activities of the National Security Agency were wrong and that the public deserved to know. But Snowden as whistleblower and the CSE Commissioner also misalign on the shared issue of the public need to know. In that regard, you have Edward Snowden as an "industrial scale" leaker and the CSE Commissioner operating in a very restricted and to a degree self-imposed space when it comes to public knowledge.

The Snowden leaks put the CSE Commissioner's Office in a difficult spot, forced to defend both the legitimacy of its own function and the legitimacy of the CSE. The way it was relied on by government officials to support the government stand on CSE operations did it no favours, as it turned the CSE Commissioner's Office into something it was not meant to be, a perceived semi-official mouthpiece in support of government policy.

How the CSE Commissioner's office responded to the Snowden leaks and the challenge to its own legitimacy that they represented came be seen in an examination of three annual reports—one pre-dating the Snowden leaks, which began in the

[43] In cyber operations, a man-in-the-middle attack has the attacker secretly relay and possibly alter the communication between two parties who believe they are directly communicating with each other. *I use the term as a deliberate pun in this section.*
[44] Unlike CSIS, CSE does not issue an annual public report.

summer of 2013, and two that were issued after the Snowden leaks started to flow.

The pre-Snowden annual report for 2012–2013 covered the period from April 2012 until the end of March 2013 and was tabled in Parliament on August 21, 2013, shortly after the first news reports based on the Snowden material.[45] It contained a message from the retiring CSE Commissioner, the Honourable Robert Decary, who served from June 2010 to September 2013.[46] The message was indicative of Commissioner Decary's view on the status of his office, arguing that the credibility of the CSE Commissioner's office was proven by the extent to which CSE had adopted its recommendations (92% of the time), by the "healthy relationship" established between the review body and CSE, built on mutual respect and good faith, on modest progress in increasing the transparency of reporting about CSE, and on limited gains in collaboration between the CSE Commissioner's Office and other security and intelligence review bodies, and on increased vigilance with regard to the capture of Canadians' private communications in the course of CSE cyber security operations.

Mr. Decary's final report as CSE Commissioner found no substantial problems with CSE, no unlawful activity, no diversions from Ministerial direction, and made no striking recommendations. Of the six classified reviews provided to the Minister and summarized in the public annual report, four included no recommendations at all. There was no explicit mention of CSE metadata collection and no indication of an ongoing study of this issue. The only foreshadowing of issues that would be raised by the Snowden leaks concerned an ongoing, and slow-moving, review of CSE's foreign signals intelligence sharing with its Five Eyes partners. The Commissioner noted that:

"CSEC sharing information with its international partners could affect a Canadian; it is in the international sharing of personal information where the risks are higher than for sharing involving domestic partners."[47]

One of the classified reports submitted by the CSE Commissioner to the Minister and summarized in the annual report concerned cyber security operations conducted on Government of Canada networks. The Commissioner indicated that the operations examined were those that did not require Ministerial authorization under CSE's Part B mandate, as they did not involve the direct interception of communications. CSE's efforts to detect, analyse and mitigate cyber security threats were based on data provided to CSE by Government system's owners, who operated under the Financial Administration Act, or by private sector operators who operated under Criminal Code

[45] The first news story based on the Snowden documents was published by Glenn Greenwald in *The Guardian* newspaper on June 6, 2013, "NSA Collecting phone records of millions of Verizon customers daily"

[46] Communications Security Establishment Commissioner, Annual Report 2012–2013, Commissioner's message at pp. 3–8. This annual report has been archived on the CSE Commissioner's website.

[47] Ibid., p. 38

authorities. The CSE Commissioner concluded: "I found that CSEC conducted its activities in accordance with the law and ministerial direction and I had no questions about the reporting and retained information examined." The CSE Commissioner did indicate that his Office would continue to conduct regular, in depth reviews of cyber security activities to verify compliance with the law and ensure that Canadians' privacy rights were upheld.[48]

The CSE Commissioner's last pre-Snowden report could not, of course, have anticipated anything like the Snowden leaks, the Canadian material they would contain, or the emphasize that they would place on cyber security operations. In a Canadian context, the leaks of highly sensitive signals intelligence documents were completely unprecedented. But the expressions of satisfaction with its role would not equip the CSE Commissioner's Office well to deal with the public controversies that attended the Snowden revelations.

The CSE Commissioner's annual report for 2013–2014 had to strike a new pose, even while maintaining its findings of lawfulness on the part of CSE, a finding trumpeted by the Minister of National Defence when the report was tabled in Parliament on August 20, 2014.[49] By this time, the Canadian public had been exposed to media stories based on the Snowden leaks for many months, including stories about operations against Brazil, NSA collaboration, and the airport Wi-Fi project. What had not yet come to the fore were the CSE Snowden leaks regarding cyber security operations. The 2013–14 report did not contain any mention of CSE cyber security activities but the work plan indicated that a review was underway of CSE Mandate B operations involving ministerial authorization and that this would be included in the following year's annual report.[50]

In the Annual Report for 2013–14, the new CSE Commissioner, the Honourable Jean-Pierre Plouffe, promised vigilance around the protection of Canadian privacy rights and vowed to pay particular attention to CSE metadata activities. Moving beyond the previous Commissioner's modest assessment of the Office's contribution to transparency, Mr. Plouffe promised to "push the limit" to enhance his office's public reporting and inform Canadians.[51]

That the CSE Commissioner's Office felt itself under pressure to respond to a new public appetite for information about Canadian signals intelligence based on the Snowden revelations was clearly apparent in the promise made to bring ongoing

[48] ibid, pp. 26–28
[49] Minister Nicholson's "Statement Following the Tabling of the Communications Establishment Commissioner's Report," August 20, 2014. [Parliament was in summer recess at the time]
[50] CSE Commissioner Annual Report 2013–2014, p. 52
[51] Wesley Wark, "Spy Agency Watchdog Strikes a New Pose," *The Ottawa Citizen*, August 22, 2014

review of metadata operations to the forefront. The Commissioner confirmed that his Office had been studying metadata activities since 2006 and that previous reviews had had an impact on CSE conduct. These previous reviews had "confirmed that metadata remains fundamental to CSEC's mandated activities." The Commissioner even repeated the basic justification presented by CSE Chief John Forster to the Senate Committee in February of 2014:

*CSEC used metadata, for example, to determine the location of a communication, to target the communications of foreign entities outside Canada, and to avoid targeting a Canadian or a person in Canada.*

Although there had been no mention of an ongoing metadata review in the previous annual report, Commissioner Plouffe stated that:

*Planning for a comprehensive review of metadata was underway prior to the unauthorized disclosures by Edward Snowden last June. In light of the significant public interest in this issue, this ongoing review is a high priority. It provides an opportunity to once again examine CSE's metadata activities, to assess changes to the activities and to determine compliance with the law and whether CSE protects the privacy of Canadians.*

The markers that Commissioner Plouffe set down: greater transparency; heightened attention to public concerns; more timely reporting on problematic areas of signals intelligence activities such as metadata, intelligence sharing partnerships and cyber security operations, were all stimulated by the Snowden leaks and represented a potential break from the past.

These markers faced their first test with the subsequent annual report for 2014–2015, which was completed in June 2015 but whose tabling in Parliament was delayed by the federal election and Parliamentary recesses. It was finally made public in late January, 2016.[52] A key focus of the Office's review work was clearly now on CSE metadata activities, and there is a promise that this focus will remain. The Commissioner's report included a further review of the Airport Wi-Fi project, and concluded that it was conducted in a lawful manner and that "CSE took measures to protect the privacy of Canadians in this activity."

But the new spotlight on CSE metadata operations overlapped with review of CSE's foreign intelligence partnerships and resulted in a disturbing and unprecedented finding around the Canadian sharing of metadata—namely that CSE had failed to properly "minimize" some shared intelligence. The CSE Commissioner described minimization as "a process by which Canadian identity information contained in metadata is rendered unidentifiable prior to being shared." The CSE Commissioner

[52] Communications Security Establishment Commissioner, Annual Report 2014–2015; Wesley Wark, "Canada's Spy Watchdogs: Good, but not Good Enough," *Globe and Mail*, February 1, 2016

indicated that minimization is meant to provide an important privacy protection and is prescribed in CSE's Ministerial directive on metadata and in CSE's in-house operational policies. The Commissioner found no intentional unlawful activity on CSE's part but the annual report indicated that the matter would continue to be reviewed by his office.

Because of the time that elapsed between the completion of the annual report and its tabling in Parliament, the CSE Commissioner was able to update his legal review and provide his conclusions on the matter of the failed minimization of Canadian metadata intelligence shared with Five Eyes partners. The Commissioner indicated that his ongoing study confirmed his belief that CSE's failure was not willful, that CSE had fully cooperated with his study and had provided his office with updates on corrective measures. Nevertheless he found that CSE had not acted with due diligence and the Commissioner was therefore compelled to inform the Minister of National Defence and the Attorney General of this instance of non-compliance with the law.[53]

This startling finding was an issue that the Minister of National Defence could not side-step. It undermined the basic approach taken by the previous government in terms of defending CSE's legitimacy in the face of Snowden revelations. The newly appointed Liberal Minister of National Defence, Harjit Sajjan, thus had to put his government's stamp on a defence of CSE. Minister Sajjan clearly wanted to be reassuring. He stated that:

"The metadata in question that was shared with Canada's partners did not contain names or enough information on its own to identify individuals. Taken together with CSE's suite of privacy protection measures, the privacy impact was low."[54]

Minister Sajjan also indicated he was satisfied with CSE's proactive measures to correct the problem and promised that "CSE will not resume sharing this information with our partners until I am fully satisfied the effective systems and measures are in place." Given that seven months had elapsed between the completion of the CSE Commissioner's report and the Minister's statement, it would appear that the corrective measures still being undertaken were, at least, technically complex. No explanation was provided as to why they had not been completed by January 2016, nor was any indication provided of the impact of the standstill on intelligence sharing with our allies.

---

[53] These details were provided by the Office of the CSE Commissioner in the press release that accompanied the tabling of the Commissioner's Annual report in Parliament on January 28, 2016. See: https://www.ocsec-bccst.gc.ca/s41/s60/d352/eng/commissioner-plouffe-report-tabled

[54] Statement from the Minister of National Defence on the CSE Commissioner's Annual Report for 2014–2015, January 28, 2016, available at: https://www.cse-cst.gc.ca/en/media/media-2016-01-28

It subsequently emerged in media reporting that the CSE Commissioner had found that CSE software meant to scrub Canadian identity information from metadata phone logs, called "Dialed Number Recognition" logs, and from internet metadata involving Canadian IP (internet protocol) address fields had both failed. According to the media reports based on court filings, the CSE Commissioner found that he could not determine the time period over which minimization procedures had failed, though the possibility existed that it was as long as a decade.[55]

The immediate legal issue of CSE non-compliance was put to bed by mutual agreement between the Minister of National Defence and the Attorney General. But the subsequent public revelations of the details of the CSE Commissioner's findings undermined Minister Sajjan's reassurance about low privacy impacts and gave further weight to the Commissioner's recommendation that CSE's legislative statute from 2001 "be amended to provide a clear framework for CSE's metadata activities."[56]That recommendation referred only to CSE's metadata collection in the context of foreign signals intelligence.[57]

But there was another arrow in the Commissioner's findings, one that was generally lost sight of in the media attention to the foreign intelligence metadata sharing issue. As promised, the CSE Commissioner included a summary of a review of CSE's cyber security operations under Ministerial authorization in the 2014–15 annual report.[58] His findings did not drive headlines but they were nevertheless as significant in their implications as was the metadata sharing concern.

Unlike the metadata issue, the CSE Commissioner did not address cyber security operations (information technology security) in the context of the Snowden leaks. No reference was made to any of the Snowden material that became of the subject of Canadian media reporting in February and March 2015, probably because of the closeness of these media stories and public surfacing of Snowden documents to the end of the Commissioner's annual review cycle. The cyber security activities studied by the Commissioner's office did cover the time frame indicated by the Snowden CSE leaks, 2009 to 2012. But we may have to wait on the Commissioner's 2015–16 annual report for any direct commentary on the Snowden material on cyber security. A "focused" review is promised in 2015–16 of "CSE's information technology security (IT) metadata activities."

---

[55]Colin Freeze, "Spy agency accidentally shared Canadians' data with allies for years," *Globe and Mail*, June 1, 2016. The court case referenced is the lawsuit brought by the British Columbia Civil Liberties Association against CSE.

[56] It was worth noting that CSE's first Ministerial directive on metadata collection dates from 2005, four years after the passage of the Anti-Terrorism Act and the provision of CSE's enabling legislation.

[57] CSE Commissioner's Annual Report, 2014–2015, p. 22

[58] "Review of CSE Information Technology Security Activities Conducted under Ministerial Mandate," ibid., pp. 26–32

The CSE Commissioner's office indicated that they had studied two kinds of cyber security operations based on Ministerial authorizations, both involving the potential interception of private communications. One involved the controlled testing by CSE of the computer system of a Government of Canada client "to assess vulnerabilities and test the reaction of the client environment to cyber threats." Interestingly, the CSE Commissioner found that CSE had stopped offering such controlled testing as of November 2012 because of limited demand and "technological advancements," which may refer to the government-wide automated scanning capacities of the Photonic Prism system.

A second type of cyber security activity studied by OCSEC was generically referred to as "cyber defence operations," to "detect and mitigate malicious activity directed towards Government of Canada computer systems and networks. Only a barebones description of the operational pathway that CSE deployed involving cyber threat alerts, analysis and confirmation was provided. Nothing was said about detection systems and the reach and nature of layered systems, which was at the heart of the Snowden leaks. OCSEC did indicate that automated scanning included an ability to determine the presence and number of private communications, but the summary of its report provided few details about retention and use. OCSEC did discover systems and human errors in this process of identifying private communications, a problem that would appear to offer parallels to software failures with regard to minimization of Canadian identity data in metadata shared with CSE's foreign intelligence partners. CSE also worked to resolve these problems. More review is promised in future.

The CSE Commissioner also canvassed some legal issues around the conduct of CSE's Mandate B operations in cyber security. He reached two conclusions, both with implications for future privacy protections. One was that the current wording of CSE's Ministerial authorization regime did not sufficiently capture the reality of cyber security activities. He recommended that the government amend Section 273.65 (3) "as soon as practicable to remove any ambiguities respecting CSE's authority to conduct IT security activities that risk the interception of private communications. This part of CSE's legislation states that:

"The Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization. "

What the CSE Commissioner felt unable to enlarge on in the unclassified summary of his review was the nature of the disconnect between CSE cyber security operations and the legal mandate. The CSE Commissioner was not criticising the scope of CSE cyber security operations, but was concerned about the legal protection for the

interception of private communications as currently provided in CSE legislation.

The second legal issue concerned the determination of what constituted a private communication when it came to cyber-attack messaging. Commissioner Jean-Pierre Plouffe was prepared to follow his predecessor, Commissioner Gonthier, in arguing that email traffic sent from a malicious actor to a Government of Canada employee containing nothing more than malicious code or deceptive content ("social engineering") does not rise to the threshold of being a private communication deserving rights protection. In such circumstances interception by CSE would not require Ministerial authorization and would not need to be reported to the Minister. The CSE Commissioner further commented that removing such traffic from the tally of intercepted private communications would prevent what he called the "distortion" of the privacy risks of CSE's cyber defence activities.[59]

While the CSE Commissioner has taken legal advice on this matter, and pronounces himself satisfied, the summary review does not provide sufficient detail to indicate, for example, how CSE differentiates between malicious email traffic containing the sort of minimal messaging referred to, and other forms of intercepted communications acquired through its Mandate B operations. Given the technological challenges that have beset CSE in terms of minimization for foreign metadata SIGINT sharing and the identification of private communications in its cyber security operations, the Commissioner's reasoning appears open to questioning, at least on operational grounds. Although the "majority" of private communications that the OCSEC examined consisted of this sort of minimal malicious messaging, what OCSEC saw was a sample only, from a distinct time frame stretching from 2009 to 2012. It was in this period, according to the Snowden leaks, that a more expansive Canadian cyber security network was being contemplated, but which was not yet fully operational. A determination that the privacy risks involved in the interception of communications for cyber security purposes are inherently lower than those involved in private communications intercepted under CSE's foreign signals intelligence mandate, may be premature, not least because they are based in a historically dated sample, and certainly need more contextual argument given what has been revealed through the Snowden leaks.

In reviewing the CSE Commissioner's annual reports since 2012–13, there are positive signs of change. The CSE Commissioner has been able to deliver on a promise of timelier reporting on contentious issues such as metadata, and to incorporate this into future review planning.

There is the promise of a sustained effort at greater transparency. CSE Commissioner Plouffe stated:

> *Transparency continues to be an important element of my approach, which is important to maintain public trust. Part of my role is to inform Parliament and Canadians about CSE's activities, and I believe it is important to support my*

[59] ibid, pp. 31–32

> *findings with as much explanation as possible, within the restriction of the Security of Information Act.*[60]

But the delivery of greater transparency, driven in part by the Snowden leaks, remains a long term proposition, that will have to be tested in future annual reports and other public pronouncements made by the Commissioner.

The Snowden leaks also impelled the creation of a new definition of how the CSE Commissioner served the public interest. The expression of this mixed a judicial calm in the face of public controversy, to avoid overreaction and "maintain perspective," alongside an effort to establish the unique position of the CSE Commissioner's office as being expert, independent, but fully versed in the secrets of CSE. The Commissioner contrasted his Office's knowledge base with concerns about: "public discussion that draws conclusions or forms opinions based on partial information. Without full context, he warned, "which cannot be revealed to those outside the 'security fence', partial information can be misleading and misinterpreted."[61] While this is true and points to a significant problem, it also resurrects claims about needing to trust the CSE Commissioner's findings and trust its expertise in ways that circle back to the need for greater transparency, greater timeliness, and a display of rigorous (tough) judgement to underline OCSEC's true independence.

Greater transparency is perhaps the hardest thing to measure when it comes to the work of CSE's review body, or indeed CSE itself, or Government pronouncements. The challenge posed by the Snowden leaks is a challenge to explain them and justify the programs they reveal. While this takes official bodies into the uncomfortable realm of having to deal with unauthorised leaks, it has become the new, or at least temporary benchmark of transparency, which has only been partly met, to date, more so for foreign SIGINT operations than for those involving cyber defence. As I indicated in an earlier study for the OPC, completed in March 2012, a review of CSE Commissioners' reports since their inception showed a tendency to focus on the privacy risks of CSE's foreign signals intelligence activities, leaving the other parts of its mandate as secondary areas of coverage "sometimes attended by early assumptions that they involved lesser risks."[62] It would appear that the CSE Commissioner's Office may still been influenced by this approach and is still engaged in catch-up, specifically in response to Snowden revelations.

Efforts on the part of Government Ministers and officials to explain CSE operations share common ground with those of the CSE watchdog in upholding the lawfulness of CSE operations in the face of the Snowden leaks. But upholding the claim of

---

[60] CSE Commissioner's Message, Annual Report 2014–2105, p. 5

[61] CSE Commissioner's Message, Annual Report 2014–15, p. 3

[62] Wesley Wark, "Electronic Communications Interception and Privacy: Can the Imperatives of Privacy and National Security be Reconciled," March 2012, available at: http://www.cips-cepi.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf

lawfulness has now morphed into calls for enhancements to technological protections for communications interception to ensure privacy rights and into calls for amendments to CSE legislation in order to tighten the nature of Ministerial authorizations for the interception private communications. The Snowden leaks have breathed new life into longstanding arguments made by successive CSE Commissioners that the Ministerial authorization regime set out in the 2001 anti-terrorism act was insufficient.

These calls for relatively modest adjustment to achieve lawful access by CSE, have been met by more sweeping proposals for change. One such proposal was contained in an ambitious private members bill tabled in June 2014 by the then Liberal opposition critic for Defence, MP Joyce Murray.

**Bill C-622. A good idea gets a new future?**

Ms. Murray's bill (C-622), "The CSEC Accountability and Transparency Act," was tabled in the House of Commons on June 18, 2014.[63] The bill was a response to the Snowden revelations and was designed to maintain CSE's three-part mandate while surrounding its operations with stronger democratic controls. To achieve this aim it proposed changes to enhance the reporting by the CSE chief to the Minister, to strengthen Ministerial accountability; it required greater transparency from CSE itself, in the form of a mandated public annual report on CSE activities; its strengthened the powers of the CSE Commissioner and included language calling for expanded OCSEC reporting to "to include a sufficiently detailed account of the Commissioner's findings to meaningfully inform Parliament and the public on matters of public interest," subject only to exclusions "that are necessary to protect the confidentiality of information associated with matters relating to international affairs, defence or security."

The private members bill tried to incorporate privacy protections for metadata by shifting the definition of "private communications" to a more expansive notion of a "protected communication, defined as "any information produced by, conveyed by, or associated with a telecommunication sent or received, inside or outside Canada, by a Canadian or a person in Canada."[64]

In a major change to the CSE legislation the bill proposed removing the responsibility for authorizing CSE's (inadvertent) collection of Canadian "protected" communications from the Minister of National Defence and giving it to the Federal Court, which would involve the creation of a Canadian equivalent capacity to the US

[63] Bill C-622, "CSEC Accountability and Transparency Act," http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6680729

[64] ibid,

Foreign Intelligence Surveillance (Act) court (FISC).

Finally Bill C-622 aimed to strengthen review of CSE and of the entire Canadian security and intelligence community by creating a special Committee of Parliamentarians, called the "Intelligence and Security Committee of Parliament." Its mandate would be to:

- review the legislative, regulatory, policy and administrative framework for intelligence and national security in Canada
- review the activities of federal government departments and agencies in relation to intelligence and national security
- report publicly on its activities, findings and recommendations

Ms. Murray, in her published background on the Bill called it ambitious, and so it was. The backgrounder called for "restoring the balance" between legitimate surveillance and Canadian privacy rights. It spoke to the need to restore public confidence in CSE.[65]

The Murray bill's solutions for the fundamental problem of constructing CSE's lawful access were indirect. The bill did not lay out strictures on intelligence sources and methods, but instead focused on an improved legal framework for authorized access to interception and use of Canadian 'protected' communications, heightened transparency, and strengthened accountability.

The Bill went to second reading but had no hope of passing in the face of a then Conservative majority in Parliament and in the face of a government seemingly uninterested in any of other major tenets of the bill. The media by and large treated the bill as it would all private members bills doomed to failure—by ignoring it.

But C-622 has proved to have staying power in a changed electoral and Parliamentary landscape. Elements of Bill C-622 have shaped the Liberal government's recent tabling of a bill to create a National Security and Intelligence Committee of Parliament (Bill C-22), particularly in terms of the general mandate of such a committee and its membership structure.

C-622 may also have staying power in another, future sense. While the government has not yet moved on any amendments to CSE's legislation, it has promised a cyber security review. And as an indication of where future legislative change may head, the Liberal Party's 2015 election platform contained this promise, taken from the C-622 playbook:

"We will introduce new legislation that will…limit Communications Security

[65] Joyce Murray, "Backgrounder on the CSEC Accountability and Transparency Act," http://joycemurray.parl.liberal.ca/backgrounder-csec-accountability-transparency-act/

Establishment's powers by requiring a warrant to engage in the surveillance of Canadians."[66]

## 6. A LEGAL CHALLENGE FROM WITHOUT

Shortly after the Snowden leaks began and well before most of the CSE material began to surface in Snowden releases, the British Columbia Civil Liberties Association (BCCLA), decided to launch a lawsuit challenging the CSE's legal powers to collect Canadians metadata and communications without a warrant. The lawsuit was first filed on October 22, 2013 and continues to make waves in Canada's Federal Court (hearings on document disclosure were held in June 2016). The basis of the BCCLA lawsuit, the first of its kind to challenge CSE's 2001 enabling legislation rested on the grounds that its interception of Canadian communications and metadata represented an infringement on Charter rights, in particular on Section 8 of the Charter which grants that "everyone has the right to be secure against unreasonable search and seizure." BCCLA also argues that metadata should be protected under Section 2(b) of the Charter: "the metadata that is associated with or produced by persons in Canada constitutes expressive content that is protected…"[67]

The Government countered the BCCLA lawsuit in a filing in January 2014, founded on a series of arguments, including that the BCCLA has no legal standing to bring the suit in so far as it had not identified any factual basis "on which to argue that an individual's Charter rights had been infringed." It also argued that the Court had no jurisdiction to interfere with the executive prerogative of Ministerial authorizations or directives. In particular the Government counter-claim was adamant in arguing that metadata collection could not infringe on freedom of expression rights protected by the Charter, as metadata "is not a communication that conveys or attempts to convey meaning. " The government further argued that any infringement of Section 8 charter rights that might occur in the course of CSE's foreign intelligence and IT security activities is lawfully authorized, "in furtherance of government objectives of the **utmost importance** [emphasis added] and is "minimally intrusive." The Government concluded its case by stating that:

> the beneficial effects of allowing CSE to carry out activities necessary to protect Canada's national security, foreign affairs and national defence as well as protect the government's electronic infrastructure are significant and far outweigh any minimal interference with either freedom of expression or

[66] Liberal Party of Canada, "Real Change: A New Plan for a Strong Middle Class," p. 53

[67] BCCLA statement of claim, https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf

privacy which may incidentally occur.[68]

The lawsuit has not yet been adjudicated on its merits and is currently stuck at a procedural stage involving claims around the disclosure of documents. The Attorney General has blocked the disclosure of sensitive CSE records, using Section 38 powers in the Canada Evidence Act, on the grounds that there release would be injurious to Canada's national security and international relations."

Unlike Bill C-622, the BCCLA lawsuit does not indicate proposals for how CSE should engage in lawful access, beyond the implied suggestion that both metadata and Canadian's private communications should have higher walls of protection.

## 7. CSE LAWFUL ACCESS FIXES POST-SNOWDEN

If we take responses to the Snowden revelations surveyed in the previous sections of this report as indicating varieties of potential "fixes" for CSE lawful access, they range from initial political efforts at reassurance about lawfulness, through more detailed explanations offered by government officials about CSE operations and privacy protections, to the scrutiny of CSE's watchdog agency, which has been pushed to greater transparency, rigour and timeliness of reporting by the Snowden leaks. What binds all of these actors together are different forms of affirmation of lawfulness, combined in the CSE Commissioner's case with suggestions, sometimes opaque, for legislative amendments.

Moving beyond these defences of lawfulness are the Murray Bill, C-622, which posits solutions to lawfulness involving a nexus between enhanced transparency, enhanced accountability and a shift in the framework for authorising the interception of a more broadly defined class of "protected communications," by taking authority away from a Minister and putting it in the hands of an independent judge.

The BCCLA lawsuit moves still further by its all-out claim against the lawfulness of CSE's communications interception programs.

Interestingly, the government's response to the BCCLA claim takes us not just to the heart of the legal controversy over what constitutes lawful access, but also to the heart of another issue, of intelligence's significance and value-added, it's "beneficial effects."

[68] Defendant's Response to Civil Claim, https://bccla.org/wp-content/uploads/2014/10/20140120-Response-to-Civil-Claim.pdf

An assertion of intelligence's beneficial effects can assist us with defining the lawfulness of signals intelligence activities though claims of necessity and gestures towards a "balancing" proposition about security needs and civil liberties protections. But the beneficial effects—lawfulness equation can also be advanced differently by considering how an ethos of intelligence might help achieve democratic legitimacy. In this context, as I have argued elsewhere, drawing liberally from the work of former senior British intelligence officials, David Omand and Michael Herman, democratic legitimacy can be sustained in part by adopting a modified form of the classic "just war doctrine" and superimposing it on the world of intelligence.[69]

## 8. A JUST INTELLIGENCE ETHOS AND ITS ROLE IN CONSTRUCTING LAWFULNESS

This superimposed "just intelligence" model would require us to confront four issues drawn from just war doctrine (I discard the requirement for "last resort" use as inapplicable to intelligence):[70]

*Just cause*

*Right authority*

*Right methods (proportionality)*

*Reasonable prospect of success*

Just cause may be the easiest of these issues, but only in the sense that it depends on an ability to identify threats to national security. That identification occurs internally within government and to a degree externally in the public domain. The internal, and secretive, process is governed by an overarching intelligence priority setting exercise, supplemented by a process of constant adjustment and application through ongoing threat assessments contributed by the security and intelligence community. The intelligence priority setting exercised was described for the first time in testimony by the National Security Advisor to the Senate Committee on National Security and

[69] Wesley Wark, "C-51 and the Canadian Security and Intelligence Community: Finding the Rights Balance for Security and Rights Protections," in Edward M. Iacobucci and Stephen J. Toope, eds., *After the Paris Attacks* (University of Toronto Press, 2015), pp. 167–74. See also David Omand, *Securing the State* (NY: Columbia University Press, 2010); and Michael Herman, "Ethics and Intelligence after 9/11, ' in Christopher Andrew, Richard Aldrich and Wesley Wark, eds., *Secret Intelligence: A Reader* (Routledge, 2009), pp. 382–94

[70] My application of just war doctrine to intelligence mirrors that of David Omand, but adapts it in different ways, See Omand, *Securing the State*, especially, pp. 286–87.

Defence in February 2014, a session devoted primary to testimony driven by responses to the Snowden revelations. Stephen Rigby explained to the Cabinet that intelligence priorities are established by his office on an annual basis following consultation with key S and I agencies and presented as a draft plan to Cabinet. Cabinet approves the priorities, which are then converted into Ministerial directives to specific agencies, and placed into what he called the "work plan" of individual organizations.[71]

Externally the identification of threats, to the extent that this is subject to Government control, is propagated through a variety of means, including national security strategy statements, more focused counter terrorism and cyber security strategy documents, and the annual public reports issued by the Canadian Security Intelligence Service. I have argued elsewhere that these serve an important public education function, though there are persistent weaknesses in the Canadian approach, including in terms of fluctuating models for security statements, the lack of continuity, and the absence of sustained political support for their propagation and messaging.[72]

Just cause can be considered a foundational element in any striving for "lawful access." Without proper identification of threat actors and broad public understanding of the need to defend against such actors, lawful access lacks legitimacy. The element of "Right Authority" is another, but different foundation. It speaks to the important question in a democracy of 'who is in charge,'—important in order to provide for accountability as well as to reassure about good governance. In the case of the Communications Security Establishment and its operations, right authority is vested in two top levels in the chain of command, though it can also be exercised at lower levels of management. The two top levels are the Minister (of National Defence), and his deputy, the Chief of CSE. The Minister is engaged in approving intelligence priorities alongside his Cabinet colleagues, has the power to sign Ministerial authorizations for the interception of private communications, and provides CSE with high level Ministerial directives to ensure the proper pursuit of government mandated priorities. The Chief of CSE, under CSE's enabling legislation, is responsible for the overall leadership and management of CSE, and in particular for overseeing the implementation of formal "operational procedures," codified as mission statements, for the Establishment. Between them, the Minister and the Chief of CSE are responsible for ensuring that a culture of lawfulness and respect for privacy rights is instilled in CSE personnel and activities. This responsibility has been enhanced in recent years by reporting mechanisms within CSE that are meant to ensure organisational awareness and mitigation of security, data, and privacy

[71] Testimony of Stephen Rigby, National Security Advisor, to the Senate Committee on National Security and Defence, February 3, 2014.
[72] Wesley Wark, "'Worth Repeating Over and Over Again': the Canadian Search for a National Security Strategy," under review for publication in *Intelligence and National Security*.

breaches. The Minister strives to ensure that his exercise of accountability for CSE is a real one; while the CSE chief strives to ensure that he/she can sustain the efficacy and propriety standards for CSE's operations that are vital to success and legitimacy. These are challenging responsibilities that intersect with demands for greater transparency in a post-Snowden environment.

The "Right methods" element of a "just intelligence" doctrine involves calculations about the reasonableness of the use of different kinds of intelligence collection methods. There is, currently, no proportionality yardstick built into CSE's legislation, nothing similar to the reference to "strictly necessary" in the CSIS Act. This was an issue that Bill C-622 proposed to address, in particular by mandating the CSE Commissioner to review CSE's operations to ensure that they "do not involve an unreasonable or unnecessary exercise of the Establishment's lawful powers."[73] Even with the addition of such guidance into CSE legislation, the application of proportionality in the world of signals intelligence is fraught with challenges that are different from those that apply to a HUMINT (human intelligence) organisation such as CSIS. In CSE's case the challenges are a product of the reality of trying to extract from the "global information infrastructure," useful intelligence that meets Canadian needs and respects Canadian laws. Increasingly, signals intelligence agencies have been driven by a combination of technological capacity and technological need to engage in initial mass acquisition of communications data, including metadata and content data, in order to provide subsequent filtering and analysis to arrive at useful intelligence. This is the problem proverbially described as the search for the intelligence 'needle' in the communications 'haystack.' There is even a cartoon in one of the Snowden CSE documents that represents the finding of the needle (after too long a search!) Proportionality becomes a back-end calculation further down the intelligence processing chain, rather than a front end calculation about targeting. This means that there may be no initial identification of friend vs. foe, innocent vs. malicious actor, in SIGINT acquisition. Not only does this serve to displace any "right methods"/proportionality argument about intelligence collection it also sets up difficult to resolve debates around the actual effectiveness of an initial mass acquisition intelligence strategy, including in regards to timelines and the production of actionable intelligence.

The commission established by President Obama to respond to the controversies ignited by the Snowden revelations reached some interesting findings in regard to the proportionality ethos of SIGINT that might serve as guideline for future discussion in Canada. As a general principle the review group argued that surveillance decisions "should depend (to the extent feasible) on a careful assessment of the anticipated consequences, including the full range of relevant risks. The enumerated risks included national security, but also: privacy; freedom and civil liberties, including on the internet; risks to relationships with other nations; and risks to trade and

[73] Bill C-622, "CSEC Accountability and Transparency Act," S. 273.63 (2)(ii)

commerce.[74] The review group also recommended that, "The US government should

***What is intriguing about some of the planning documents revealed by Snowden regarding CSE cyber security activities is the sense that at least on the cyber security side, CSE itself saw the need to move away from mass surveillance to a system that would allow a quicker more targeted identification of malicious actor internet traffic. The grounds for this move appeared to be both the problems of information overload and the distortion of effort and unproductive nature of mass cyber security surveillance.***

examine the feasibility of creating software that would allow the National security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk collection of data."[75] Whether there is a feasible alternative to mass SIGINT acquisition is not a debate that we have begun to have in Canada, in part because we lack an authoritative platform from which to commence such a debate and in part because we lack sufficient knowledge about the actual operational pros and cons of mass vs. targeted information acquisition. What is intriguing about some of the planning documents revealed by Snowden regarding CSE cyber security activities is the sense that at least on the cyber security side, CSE itself saw the need to move away from mass surveillance to a system that would allow a quicker more targeted identification of malicious actor internet traffic. The grounds for this move appeared to be both the problems of information overload and the distortion of effort and unproductive nature of mass cyber security surveillance. Lawful access does not appear in these few records as a preoccupation but lawful access could definitely be aided by a more precise SIGINT targeting system.

## 9. LEARNING LAWFUL ACCESS LESSONS FROM OTHERS

Canada's closest ally among the Five Eyes SIGINT community is undoubtedly the United States. No country has been more impacted by the Snowden revelations than the United States. Snowden's whistleblowing has forced a major rethink around transparency on the part of US intelligence agencies, which is not just calculated on trying to meet a rising level of public expectation, but also to provide one possible safety value against future inclinations to leak. This suggestion was explicit in the

[74] "The NSA Report: Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," December 12, 2013. Discussion at xvi and xvii

[75] Ibid, Recommendation 20

recommendations advanced by the President's Review Group on Intelligence and Communications Technologies, which was created to consider the implications of the Snowden leaks and reported in December 2013.[76]

The US President also made a public pledge to change the transparency environment around the US intelligence community in a major speech on January 27, 2014, also prompted by the Snowden leaks. President Obama stated:

> *For our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world…we will reform programs and procedures in place to provide for greater transparency.*[77]

Three outcomes of this pledge are particularly worthy of study. Other national practices with regard to security and intelligence are not necessarily easy to transplant to a Canadian context, but these measures would all seem like good candidates for imitation. They include the creation of a dedicated public website hosted by the Office of the Director of National Intelligence, called "IC on the Record," which includes declassified documents, official statements, speeches and testimony.[78] IC on the record also carries occasional web Q and A sessions with the Director of National Intelligence.[79] One question for the DNI aired on the web chat was, "Why did you lie to Congress?"

A second practice includes the creation of a detailed report on the progress of reform initiatives across the US intelligence community.

The third candidate for imitation would be the creation of a US intelligence community action plan called the "Principles of Intelligence Transparency." The first principle endorsed by the action plan is straightforward:

> *Principle 1: Provide Appropriate Transparency to Enhance Public Understanding about a) the Intelligence Community's mission; b) the laws, directives, authorities and policies that govern the Intelligence Community's activities; and c) the compliance and oversight framework that ensures intelligence activities are*

---

[76] "The NSA Report: Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," December 12, 2013. See Recommendation 7 and the discussion at pp. 73–79.

[77] Transcript of President Obama's speech on NSA reforms, https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html

[78] Office of the Director of National Intelligence, "IC on the Record," https://icontherecord.tumblr.com

[79] The official website "IC on the Record" prompted the creation of a counter, unofficial "IC off the Record" website to host leaked documents. Available at: https://nsa.gov1.info/dni/

*conducted in accordance with applicable rules.*[80]

Some of this kind of transparency reporting is already provided by review bodies, including the CSE Commissioner. But the Canadian system is a patchwork, and the onus on explaining the Canadian intelligence community's mission, governance, and accountability framework should rest with the government and intelligence bodies, not with review agencies, who need, instead, to exercise a challenge function.

A greater effort at transparency on the part of government and the intelligence community is, I would argue, a precursor to moving forward with another partner in surveillance transparency, the private sector.

## 10. TSP TRANSPARENCY REPORTING AND SIGINT: "KNOWN UNKNOWNS

Pressures for greater transparency regarding intelligence matters have pushed outwards beyond governments, intelligence agencies themselves, and their review bodies to impact on the private sector. This has been manifest in pressures to report data-sharing relationships between major Telecommunications Service Providers (TSPs) and government agencies (law enforcement agencies in particular).

In a recent speech the Federal Privacy Commissioner, Michael Therrien, made the point about the way that transparency progress ties together the public and private sectors.[81] The Privacy Commissioner has called for the maintenance of accurate records on lawful access requests and public reporting on "the nature, purpose and number of lawful requests" that government agencies make to telecommunications companies. Whether an organisation like CSE with a specialized intelligence gathering mission can reasonably be expected to fully adhere to this requirement is an open question. But some degree of what I call "masked transparency" around the partnership between CSE and private sector TSPs is, it seems to me, attainable and would be an important transparency initiative.

The Privacy Commissioner has also urged the private sector to respond to the passage of the most recent iteration of lawful access legislation, Bill C-13 (the "Protecting Canadians from Online Crime" Act) by providing "helpful" information to Canadians. The Privacy Commissioner has created voluntary guidelines for TSP reporting and is somewhat encouraged by the way that some telecommunications companies have

[80] Office of the Director of National Intelligence, "Principles of Intelligence Transparency: Implementation Plan," October 27, 2015. Available at: "IC on the Record."
[81] Commissioner Therrien address, "Striking the Right Balance between Privacy and National Security," June 8, 2016, Canadian Telecom Conference, Toronto

come forward to publish their corporate versions of transparency reports. The Commissioner also issued a thinly veiled warning that if the private sector does not come fully on board with appropriate transparency reporting, the seeking of legislative tools to compel disclosure might be contemplated.[82]

Major work on advocating for transparency reporting by Canadian TSPs and on collating data around their responses has been done by Dr. Christopher Parsons. Parsons spearheaded a campaign to encourage disclosure of data access requests by government to Canadian TSPs. He has recently produced a report which makes a series of recommendations for both private sector TSPs and government agencies.[83] His first recommendation is that "all Telecommunications Service Providers should publish Transparency Reports." Here Parsons and the Federal privacy Commissioner are in full agreement. Dr. Parsons's recommendations aimed at government bodies touch in some explicit ways on CSE (including the publication of Ministerial authorizations and directives) and an expanded statutory reporting of surveillance techniques. But the gradual opening up of TSP public reporting on law enforcement requests for information, which complements some statistical reporting by the government on requests made to TSPs, does not yet extend to signals intelligence.

When it comes to the issue of Canadian TSP interface with CSE, the situation is extremely murky. We know something, thanks to the Snowden leaks, about the CSE intercept architecture, which relies on something called Signals Intelligence Activity Designators (SIGADs) sitting at key network junctions in Canada and globally. CSE's EONBLUE program provides a filtering and analysis capability with regard to metadata ingested by the sensor system. But the extent to which EONBLUE and its ilk has been directly incorporated by Canadian TSPs is unclear.[84]

In reviewing the state of affairs in Canada around transparency and telecommunications surveillance, Parsons reaches some conclusions that are quite dire:

> *telecommunications surveillance establishes chilling conditions that are accentuated by poorly implemented or limited transparency efforts by corporations combined with weak government accountability practices…These chilling effects are accentuated by CSE's mass collection of data about Canada's telecommunications.*[85]

---

[82] ibid

[83] Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project report , https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf

[84] Christopher Parsons, "The Governance of Telecommunications Surveillance…"

[85] ibid., p. 86

This claim mirrors arguments made in the BCCLA lawsuit. Improved transparency and greater accountability are clearer needed, but the challenge is in translating these into the special circumstances of the realm of CSE.

We also need to appreciate the current limits of our understanding of the CSE–TSP partnership arrangement, which both supports the call for greater transparency and accountability imposes caution in reaching premature judgments.

The furthest we can go at the moment to fully understand the nature of the likely partnership between CSE's SIGINT activities and the private sector, including access to private sector traffic and data bases, is by considering the analogous situation in the US. One major Snowden leak considered a NSA presentation entitled "SSO Corporate Portfolio Overview."[86] SSO refers to "Special Source operations" a term which also recurs in CSE Snowden documents. The "overview" was designed to convey the nature of SSO collection, the surveillance programs and lawful authorities that it relied on. The starting point for the presentation was a description of SSO corporate access collection as involving: "Access and collection of telecommunications on cable, switch network, and/or routers made possible by the partnerships involving NSA and commercial telecommunications companies." In terms of quantity, SSO was reported to provide fully 80% of NSA's collection. The document also noted "because of partner relations and legal authorities, SSO Corporate sites are often controlled by the partner, who filters the communications before sending to NSA." The NSA presentation went on to document the variety of programs employed by NSA, their different collection mandates and capabilities, their geographic reach, their lawful authorities. As an example, the Program codenamed "Blarney" operated under the authority of the Foreign Intelligence Surveillance Act, involved 11 different SIGAD intercept posts, targeted diplomatic traffic, counterterrorism, foreign governments and economic data and was described as a "top contributor" to the President's *Daily Brief* (the high level compendium of intelligence reporting produced by the Director of National Intelligence for the President and key seniors).

We have no comparative knowledge of CSE SSO operations, at least not in the public domain, or ever summarized in CSE Commissioner reporting. But the Snowden leak is at least suggestive of two things—the importance of SSO and the private sector partnership; and the kids of questions that strengthened transparency and accountability might be designed to ask about Canadian programs.

These questions would include the nature of partnership control and filtering, the nature of lawful access, quantities and quality of the intelligence derived, and the general target set. Some of this information might have to be masked in future public

[86] NSA, "SSO Corporate Portfolio Overview," https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH2047.dir/doc.pdf

reporting, but the degree of masking would have to be weighed against impacts on intelligence effectiveness and the public interest.

This consideration of what transparency reporting around CSE SSO lawful access might look like, leads us back to the larger issues of the context and mechanisms required to make lawful access reporting meaningful and productive. Transparency reporting is not an end in itself and will not achieve improvements to the idea of lawful access on its own

## 11. CONCLUSION: FUTURE DIRECTIONS FOR CSE SIGNT AND LAWFUL ACCESS

How to make an inherently secretive process of access to Canadians' communications "lawful," especially in a signals intelligence and cyber security environment, is a large question that will continue to loom over policy making, legislation and whatever public debate on CSE might be to come. The Snowden revelations might have slowed or ceased but they have left us with a greater awareness of the complexity and scale of cyber surveillance, for both foreign intelligence and cyber security, and a conundrum about how to find a democratic path. The Snowden documents also suggest a dispiriting trend line that leads to ever greater mass surveillance in search of national security leads and actionable intelligence, ever greater storage of personal data, more erosion of privacy, and rising levels of angst about the actions of intelligence agencies.[87]

The discussion of lawful access with regard to signals intelligence, which is clearly a significant domain, though one distinct from domestic law enforcement and even domestic security intelligence as practiced by CSIS, needs, in my view, a new framework. We can identify components of that framework, but we also need to be clear about the purpose, which is ultimately to provide for democratic legitimacy around a practice that is inherently democracy-deficient. While we work to make lawful access more lawful we also have to find a way to make sure that the perception of lawfulness is fully entrenched. Better laws, more transparency, stronger accountability are the usual remedies advanced, often in isolation. What is required, in my view, is a bigger package of measures that are meant to cohere.

**The Five Change Factors:**

To that end, this study offers some ammunition for recommendations that advance five change factors.

[87] See the discussion in David Lyon, *Surveillance after Snowden* (Cambridge: Polity Press, 2015)

These five considerations are rooted in an argument that CSE's SIGINT activities under its various mandates pose unique challenges for a lawful access regime and need to be treated separately from the broader remit of lawful access as it applies to law enforcement agencies.

The first consideration is that more attention needs to be paid to the privacy risks attendant on the conduct of CSE's cyber security mandate, particularly in the context of the potential blurring, as the Snowden CSE documents suggest, of defensive and offensive cyber security operations and the ongoing march of technological change. Continual testing of the current hypothesis of the CSE Commissioner's Office regarding the inherently lower privacy risks involved in CSE's cyber security activities as opposed to its foreign SIGINT activities is required. This testing should include both ongoing review by the CSE Commissioner of the hypothesis in focused studies, of the sort that has been promised, and a more fulsome explanation for the rationale underpinning the OCSEC judgment. The Privacy Commissioner would appear to share my view that the notion that metadata, whether acquired through cyber security activities or foreign SIGINT activities, represents a low privacy risk is questionable.[88]

A second consideration is that for lawful access to be advanced when it comes to CSE SIGINT, there is an absolute requirement to change the laws governing CSE operations and to find as better to keep enabling legislation evergreen, so as to avoid the obsolescence that has crept over the CSE statute since 2001. In particular, this study follows the recommendations advanced in Bill, C-622, Joyce Murray's private members bill, to advance an altered definition of the nature of Canadian communications that deserve rights protection under the Charter and the Privacy Act. A broader definition of private communications to incorporate metadata under the term "protected communications" is in order. In addition, it is important that authority be transferred from the Minister to an independent judicial authority for approval of CSE SIGINT interception that might involve the capture of Canadians' "protected communications."

A third consideration involves a recognition of the need for greater transparency on the part of key actors who can provide a public rationale for the necessity of CSE activities under its mandates. These key actors include political leaders, including the Minister, the chief of CSE and his fellow deputy ministers, including the National Security Advisor, and the CSE watchdog, the CSE Commissioner. Unless ways can be found to roll back secrecy, the democratic legitimacy of CSE will ultimately continue to be challenged and undermined. Part of this roll back of secrecy must include a public narrative around how and why CSE acquires protected communications. But the limits of this roll back have also to be appreciated. It is fundamental to the

[88] Commissioner Therrien address, "Striking the Right Balance between Privacy and National Security," June 8, 2016, Canadian Telecom Conference, Toronto

effectiveness of intelligence agencies like CSE that their sources and methods be guarded from injurious disclosure. So the secrecy roll back may involve an end to the total secrecy around collection and the substitution of a "masked" narrative. This masked narrative, of the sort that the Snowden leaks have already set in train, might have knock-on effects in allowing some discussion of the nature of partnerships that exist between CSE and TSPs to occur, with "masked" contributions from both partners. If this does not sound like full-on transparency, such is the world of intelligence and a glass half full is better than nothing.

***Unless ways can be found to roll back secrecy, the democratic legitimacy of CSE will ultimately continue to be challenged and undermined.***

The need for greater transparency, bearing in mind its inevitable limits, accords with a complimentary need for more rigorous review of CSE activities, including reviews that go beyond lawfulness to consider the efficacy of CSE's operations. The CSE Commissioner, as I have argued in this paper, has been propelled to greater rigour by the Snowden leaks and the fact of being made one of the key spokespersons to explain the legitimacy of CSE activities. But review of CSE through the Commissioner's function needs to be extended to include proper Parliamentary scrutiny, of the sort that is promised in the Government's recently tabled Bill C-22. The Office of the Privacy Commissioner, as the expert reviewer, has an ongoing role to play in maintaining a watch on the privacy implications of CSE's activities, even though it is unlikely that the CSE Commissioner will cede scrutiny of CSE's operational privacy implications to the OPC.

A fourth consideration is that the Canadian discourse on CSE and SIGINT, prompted in large part by the Snowden leaks, must in future include an elaboration and discussion of the value proposition represented by intelligence activities for Canadian security. Without such a discussion, a lawful access regime, broadly imagined, can easily lose its way, either in a too restrictive or too generous direction, and can too easily be swayed by over-reaction to events. The value proposition has to include a greater willingness to discuss the benefits and challenges of Canada's involvement in the Five Eyes community, particularly around the sharing of Canadian protected information.

A fifth and final consideration is related to an energized and better informed discussion of intelligence. The Canadian security and intelligence community, and its political masters, need to embrace a doctrine of "just intelligence." Such a doctrine could provide a broad guidance framework to ensure the democratic legitimacy of intelligence as well as help ensure an ethical and law-abiding culture is sustained within intelligence and security agencies. A "just intelligence" ethos needs also to be communicated in the public domain as part of an effort to seed a public understanding of intelligence's value proposition.

The achievement of all, or any, of these advances requires two inter-related things. One is the expenditure of political capital by the ruling government. The other is a receptive public. Historically, it is fair to say that both have been in short supply in Canada. But changes in the security, technological and democratic environments suggest that the Canadian historical tendency to pay underwhelming attention to the right conduct of intelligence agencies is on the cusp of change.

It is worthwhile reminding ourselves of the original manifesto that Edward Snowden penned to accompany his leaks of the NSA surveillance records:

> The US government, in conspiracy with their client states, chiefest among them the Five Eyes—the United Kingdom, Canada, Australia, and New Zealand—have inflicted upon the world a system of secret, pervasive surveillance from which there is no refuge. They protect their domestic system from the oversight of citizenry through classification and lies, and shield themselves from outrage in the event of leaks by overemphasizing limited protections they choose to grant the governed…

The keywords and phrases are: **conspiracy**, **secrecy**, **no refuge**, **abuse of oversight**, **exaggeration of limited protections**. Whatever the truth of these charges, the hopeful fact is that all of them are capable of being met, at least to some degree, with the kinds of changes proposed in this study.

As the Privacy Commissioner engages with one of his key strategic privacy priorities—government surveillance—it is hoped that these five identified change factors might play a role.[89]Even as we contemplate the Snowden leaks and what they mean for a Canadian concept of lawful access, new technological challenges continue pile into the debate, including around the problems of encryption and its implications for intelligence and security agencies "going dark" in their hunt for actionable intelligence. One indication of the brooding this has generated among security agency heads was voiced by the RCMP Commissioner, Bob Paulson. In a speech delivered to the annual symposium of the Canadian Association for Security and Intelligence Studies, in January 2016, the Commissioner focused on the investigative challenges presented to the RCMP by the phenomenon of threat-related messaging "going dark" in the broadest meaning of the term. His concern extended beyond the technological challenges of intercepting communications and beyond the encryption problem to the fundamentals of "lawful access," as a product of societal legitimacy. What appeared to concern the Commissioner most was the potential loss of his own organisation's ability to collect even the most basic identification data about people, not because of

[89] OPC Strategic Privacy Priorities 2015–2020, available at: https://www.priv.gc.ca/information/pub/pp_2015_e.pdf

technological constraints but because of societal resistance. Here is how he put it:

> *What has proven difficult is the ability for us, for lawmakers, for society, to reconcile the need to have a robustly Charter-compliant way to access information with the safeguarding of a right to privacy which occupies a place of paramountcy. Today, we will abide nothing that can remotely be seen or understood to threaten our freedom, including our privacy. Privacy has become the crusade of those who would have us live in their textbooks. Privacy is an essential component of our freedom, no question, but I argue our privacy must be thoughtfully balanced against the very communal dimension and nature of our existence. We need to consider to what degree privacy is meant to equal anonymity.*[90]

This portrait of the power of privacy advocates and of the strength of privacy preoccupations may surprise many in today's Canadian society. But what is important in the Commissioner's speech is not his assessment of the strength of privacy concerns but rather his belief that a wide gulf separates privacy protections from communal safety. Again this suggests to me the need for a framework debate.

So, too, do the kinds of new tensions that have appeared, post Snowden, in the already complex world of public-private sector partnerships in surveillance. As the Apple–FBI imbroglio in the United States suggests, the lack of a solid framework for considering lawful access can lead to a calling out of good and bad corporate citizens. Blackberry CEO, John Chen, weighed into the controversy, following media reports about the RCMP having accessed Blackberry BBS messages in an operation against organized crime in Quebec, with this perspective:

> *When it comes to doing the right thing in difficult situations, BlackBerry's guiding principle has been to do what is right for the citizenry, within legal and ethical boundaries. We have long been clear in our stance that tech companies as good corporate citizens should comply with reasonable lawful access requests. I have stated before that we are indeed in a dark place when companies put their reputations above the greater good.*[91]

Good corporate citizens need the same framework for considering lawful access as governments. They too will have to figure out what privacy risks mean, what transparency and accountability demands, what the value proposition for national intelligence means to them, and what the "ethics" of surveillance really come down to.

---

[90] RCMP Commissioner Paulson, speech to the annual CASIS Symposium, January 15, 2016, http://www.rcmp-grc.gc.ca/en/news/2016/15/john-tait-memorial-lecture-canadian-association-security-and-intelliegence-studies

[91] Terry Dawes, "BlackBerry CEO John Chen confirms RCMP Cooperation," April 18, 2016, http://www.cantechletter.com/2016/04/blackberry-ceo-jon-chen-confirms-recmp-cooperation/

For governments these may be old topics under new pressures, but freighted by secrecy and inertia. For their private sector partners, some of the topics are just brand new, not least the value proposition and ethos of intelligence.

## APPENDIX A

## SNOWDEN ARCHIVES ON THE WEB

### Snowden Document General Repositories:

### A. "Snowden Surveillance Archive"

Creator/Research Partners:

Prof. Andrew Clement, University of Toronto, and the Canadian Journalists for Free Expression. Research collaboration involves: The Politics of Surveillance Project, Faculty of Information, University of Toronto; Surveillance Studies Centre, Queen's University; Centre for Free Expression, Faculty of Communications and Design, Ryerson University

Web site:

https://snowdenarchive.cjfe.org

General contents:

Documents published from July 2013 to present
Includes links to source documents and media reporting associated with document

Overview of Contents:

This archive contains approximately 400 documents related to the Snowden leaks. These documents have been published by the variety of publishing partners associated with the Snowden leaks, including Glenn Greenwald's *The Intercept*. The documents have been sourced from a variety of other Snowden archives, including the Electronic Frontier Foundation's NSA Primary Sources, the American Civil Liberties Union's NSA Documents, and the Courage Foundation's Snowden Revelations.

The catalogue of documents appears to be fully comprehensive. It includes additional documents voluntarily published by the US Government. It also includes an unprecedented level of search capability, with the ability to browse by creating agency, publisher, reporter, communications target, and security classification or distribution code. It also can search by keyword in the title or body of the document.

### B. "NSA Primary Sources"

Creator:

Electronic Frontier Foundation

Web Site:

https://www.eff.org/nsa-spying/nsadocs

General Contents:

Documents published from June 2013 to present
Includes links to the documents and associated media reporting

Overview:

The Electronic Frontier Foundation has compiled a long list of documents published by other media sources. The archive is updated regularly, containing documents from June 2013 to present. The site can be sorted by media outlet, and contains links to both the documents and to the original news articles. It is also searchable, but this is limited to the titles of the documents.

---

### C. "NSA Documents"

Creator:

American Civil Liberties Union

Web Site:

https://www.aclu.org/nsa-documents-search

General Contents:

Snowden documents from June 2013 to present. Also includes earlier documents. Most entries include download links for the documents. No links to media reporting.

Overview:

The ACLU's database contains over 600 documents and records of media reports. Entries have basic bibliographic information and a short description. The documents are sortable by a number of different criteria, including release date, type of

document, what sorts of records are collected, and the legal authority under which they are collected. All leaked CSE documents appear to be available. Search function appears to access both titles and the documents themselves.

---

**D. "The NSA Files"**

Creator:

*The Guardian* newspaper

Web Site:

http://www.theguardian.com/us-news/the-nsa-files

General Contents:

Media reporting from June 2013 to June 2015. Documents from June 2013 to December 2013. Small number of documents available for download; substantially more media reporting at the site.

Overview:

*The Guardian* has been a major partner in publishing the Snowden leaks. Its database, however, has only a small collection of actual leak documents. It does have a substantial body of press reporting and opinion pieces, mostly focusing on the US, British, and Australian aspects of the reports. No specific search function for the NSA files, although the search function for the entire site provides some functionality.

---

**E. *The Intercept***

Creator:

Glenn Greenwald

Web Site:

https://firstlook.org/theintercept/documents/

General Contents:

After originally being published through a number of mainstream English-language media partners, including *The Guardian*, *The Washington Post*, *The New York Times,*

and some European publications such as *Der Spiegel*, the Snowden files have subsequently come to be published primarily from *The Intercept*, an online news outlet launched by Glenn Greenwald. It hosts copies of a large number of classified documents produced by various intelligence agencies. It is not immediately clear if all of those documents stem from the Snowden leaks, or if some of them are from other sources.

Overview:

The documents display in reverse chronological order, from the most recent releases, with 10 documents on a page. The search function appears to only search articles posted on *The Intercept*. These articles have direct links to the original Snowden material embedded within them.

---

### F. Cryptome's "Snowden Tally"

Creator:

"Cryptome"

Web Site:

http://cryptome.org/2013/11/snowden-tally.htm

General Contents:
Cryptome houses a large collection of obtained classified documents from a variety of sources. The "Snowden Tally" is an identified sub-set of the overall collection

Overview:

The Cryptome collection is sorted by publication date and media outlet. The documents are available for download as links or zip files. There is no integrated search function, and the labels on the documents themselves are not very specific—particularly on the larger releases.

---

### G. The Courage Foundation, Snowden Documents

Creator:

The Courage Foundation (formerly the Journalistic Source Protection Defence Fund)

Web Site:

https://edwardsnowden.com

General Contents:

A sizeable collection of Snowden documents from 2013 to the present, hosted by a Foundation established to defend Edward Snowden and to fundraise for him

Overview:

The site lists 579 documents in total (as of March 2016) with the most recent dating from January 2016. The documents are listed in chronological order from the most recent, and the original material is attached as an available download. The documents are searchable according to various criteria. Of the 579 documents, 30 are listed as pertaining to Canada and 10 describe CSE material.

---

## Canadian-Specific Snowden materials Repositories

### A. Canada's Snowden Files—CBC

Creator:

Canadian Broadcasting Corporation

Web Site:

http://www.cbc.ca/news/topic/Tag/Canada's%20Snowden%20files

General Contents:

A selection of news stories pertaining to Canadian signals intelligence and the Communications Security Establishment. Documents referred to in the stories are embedded or attached as pdfs. CBC established an exclusive arrangement with Glenn Greenwald to access selected Snowden documents with Canadian content and do joint reporting on them, under a shared byline. The first such story dates to November 2013. The most recent (at time of writing in March 2016) was May, 2015.

Overview:

The CBC has been a major partner in releasing Snowden files relating to Canada. Instead of a formal archive for the documents released, the CBC embeds download

links to the documents in each news article where they are discussed. The database is not directly searchable, although the relatively short list of articles means that it is fairly straightforward to find specific articles. Starting in November 2013, the CBC published 17 distinct stories about CSE operations.

---

### B. "Canadian SIGINT Summaries"

Creator:

Dr. Christopher Parsons

Web Site:

https://www.christopher-parsons.com/writings/cse-summaries/

General Contents:

Canadian documents from the Snowden material, dating from September 2013 to present. Links to media reporting and original documents are provided.

Overview:

Christopher Parsons has compiled a list of documents related to CSE's activities. He has provided a summary of the document itself, along with some context for the signals intelligence programs discussed in the document. He also provides links to the news article where the document was originally published, and a download link for the document itself. There are currently 27 documents in this archive, more than the 9 documents provided in the CBC collection. Parsons also plans on integrating procedural documents and reports from the Office of the CSE Commissioner, the oversight body for CSE. Once this is completed, this archive will present a much more complete view of CSE's activities as a whole. There is no specific search function.

---

## Canadian Blog Posts and Sites Providing Commentary on Snowden and Canadian Material:

### A. "Lux et Umbra"

Creator:

Bill Robinson

Web Site:

http://luxexumbra.blogspot.ca/

General Contents:

Analysis of Snowden leaks from June 2013 to present.
Links to media reporting, documents embedded in blog posts

Overview:

Bill Robinson has been posting on Canadian SIGINT topics since 2005. He has been an avid blogger on topics relating to the Snowden leaks and Canadian intelligence capabilities. His blog contains links to the source material and to media reporting and analysis on each of the leaks. The site is not very easy to search, except chronologically. It contains commentary on very wide range of associated topics, including SIGINT capabilities in the Canadian Armed Forces and CSIS.

---

**B. Professor Craig Forcese, National Security Law Blog**

Creator:

Professor Craig Forcese, University of Ottawa, Faculty of Law

Web site:

http://craigforcese.squarespace.com/national-security-law-blog/

General Contents:

Extensive expert commentary on issues at the intersection of national security law and policy. Blog posts link to media reporting and official documents. Some Snowden-related posts (13 entries in all), mostly for 2013 and 2014

Overview:

A major site for analysis of the impacts of security stories on national security law. The blog posts are designed as a process of updating his book treatment, National Security Law: Canadian Practice in International Perspective.

---

**C. Michael Geist Blog Post**

Creator:

Professor Michael Geist, University of Ottawa, Faculty of Law

Web Site:

http://www.michaelgeist.ca/

General Content:

Some blog posts linked to media reporting on Snowden leaks.

Overview:

Michael Geist is a professor specializing in privacy law at the University of Ottawa. He posts analysis regularly on issues relating to surveillance in Canada, including lawful access. These blogs react to some of the Snowden leaks. These blog posts include links to the media reporting involved in publicizing the leak documents.

---

**D. Canadian Internet Policy and Public Interest Clinic (CIPPIC)**

Creator:

CIPPIC, University of Ottawa, esp. Tamir Israel

Web Site:

https://cippic.ca/
General Contents:

Limited number of news items directly relating to Snowden

Overview:

CIPPIC's web site maintains a section on Electronic Surveillance, where there are a small number of news items relating to the Snowden leaks. Most references to this material appear in reference to a number of potential CSE oversight solutions that have been proposed since 2013. The page also compiles research conducted by CIPPIC, judicial actions relating to surveillance, and PIPEDA complaints lodged by CIPPIC. The site as a whole is searchable, however, there are very few specific references to Snowden or CSE, and no document links provided.

---

In sum, readers looking to explore the available Snowden document data set have a wealth of opportunities available to them from (at present) well-maintained sites. For those wishing to zero in on CSE documents or Canadian related material, there are the very useful web sites maintained by the CBC and by Christopher Parsons. These Canadian sites can be supplemented by an exploration of commentary provided in the web sites maintained by Bill Robinson and Craig Forcese in particular.

## Appendix B

## List of CSE originated documents in Snowden material:

"Synergising Network Analysis Tradecraft" link to CBC story May 21, 2015 "Spy Agencies Target Mobile Phones"; Chris Parsons doc. #1; Courage Foundation Doc #6

"CSEC SIGINT Discovery: Summary of the Current Effort," Discovery Conference, GCHQ, Nov. 2010, link to CBC story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc. #11; Courage Doc. #1

"Cyber Threat Detection," link to CBC Story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc #6

"CSEC Cyber Threat Capabilities," link to CBC Story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc. #5; Courage Doc. # 3

"Cascade;" link to CBC Story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc. #2; Courage Foundation Doc # 12

"CSEC ITS/N2E Cyber Threat Discovery," Link to CBC Story, "CSE Monitors millions of Canadian emails to Govt," Feb. 25, 2015; Parsons Doc. #4; Courage Foundation Doc #13

"Cyber Network Defence R & D Activities," Link to CBC Story, "CSE Monitors millions of Canadian emails to Govt," Feb. 25, 2015, Parsons Doc. #4

"Levitation and the FFU Hypothesis," Link to CBC Story, "CSE Tracks Millions of Downloads Daily," January 27, 2015; Parsons Doc. #9; Courage Foundation Doc #9

"IP Profiling Analytics and Mission Impacts," Link to CBC Story, "CSEC used Airport Wi-Fi to track Canadian travellers," January 30, 2014; Parsons Doc #19; Courage Foundation Doc #7

"Snowglobe: From Discovery to Attribution," 2011; see *Globe and Mail*, Mar. 21, 2104 "French Spy Software Targeted Canada: Report;" Parsons Doc. #18; Courage Foundation Doc. #10

"Landmark; " see *Globe and Mail*, Aug. 25, 2014, "The Landmark File: Inside Canadian cyber-security agency's 'target the world,' strategy; Lux et umbra, Aug. 17, 2014; Courage Foundation Doc. #8; Parsons Doc. #16

"Pay Attention to that Man behind the Curtain: Discovering Aliens on CNE

infrastructure," SIGDEV conference, NSA June 2010; Link to *Der Spiegel* articles; Courage Foundation Doc. #5; Parsons Doc. #10

"TLS Trends: A Roundtable discussion on current usage and future directions," Link to *Der Spiegel* articles; Courage Foundation Doc. #4; Parsons Doc # 12

"And They Said to the Titans: Watch Out Olympians in the House," see *Globe and Mail*, Oct. 7, 2013; Parsons Doc #24; Courage Foundation Doc #11

**NSA–CSE relationship docs:**

"NSA Intelligence Relationship with Canada's CSEC," Link to CBC Story, "Snowden Document Shows Canada Set Up Spy Posts for NSA," Dec. 9, 2013; Parsons Doc #21

"NSA Lends Support to Upcoming G8 and G20 Summits," Link to CBC Story, "NSA Document Raises Questions about Canada in G8 Spying," Dec 2, 2013; CBC Story "New Snowden Docs show US spied during G20 in Toronto," Nov. 27, 2013; Parsons Doc. #25

"Who Else is Targeting your Target," NSA SID Today article from GCHQ; Parsons Doc# 8

[2nd Scamp at CSEC Process]; NSA doc "Network Tradecraft Advancement Team"; Parsons Doc #14

**GCHQ–CSE relationship docs:**

"Automated NOC detection;" Parsons Doc #13

## APPENDIX C

## Key CSE–Snowden docs on cyber security:

"CSEC SIGINT Discovery: Summary of the Current Effort," Discovery Conference, GCHQ, Nov. 2010, link to CBC story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc. #11; Courage Doc. #1

"Cyber Threat Detection," link to CBC Story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc #6

"CSEC Cyber Threat Capabilities," link to CBC Story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc. #5; Courage Doc. # 3

"Cascade;" link to CBC Story, "CSE Cyberwarfare Toolbox Revealed," March 23, 2015; Parsons Doc. #2; Courage Foundation Doc # 12

"CSEC ITS/N2E Cyber Threat Discovery," Link to CBC Story, "CSE Monitors millions of Canadian emails to Govt," Feb. 25, 2015; Parsons Doc. #4; Courage Foundation Doc #13

"Cyber Network Defence R & D Activities," Link to CBC Story, "CSE Monitors millions of Canadian emails to Govt," Feb. 25, 2015, Parsons Doc. #4

"Pay Attention to that Man behind the Curtain: Discovering Aliens on CNE infrastructure," SIGDEV conference, NSA June 2010; Link to *Der Spiegel* articles; Courage Foundation Doc. #5; Parsons Doc. #10

"NSA Intelligence Relationship with Canada's CSEC," Link to CBC Story, "Snowden Document Shows Canada Set Up Spy Posts for NSA," Dec. 9, 2013; Parsons Doc #21


120 University
Room 5049
Ottawa, Ontario
Canada, K1N 6N5

E-mail: cepi-cips@uottawa.ca
Website: www.cepi-cips.uottawa.ca
Twitter: @uOttawaCIPS
Facebook: www.facebook.com/uOttawaCIPS