The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians

This page has intentionally been left blank.

Electronic version first published at www.telecomtransparency.org in Canada in 2015 by the Telecom Transparency Project. The Telecom Transparency Project is associated with the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto.

This research was funded through the Canadian Internet Registration Authority's .CA Community Investment Program. Through the Community Investment Program, .CA funds projects that demonstrate the capacity to improve the Internet for all Canadians. The .CA team manages Canada's country code top-level domain on behalf of all Canadians. A Member-driven organization, .CA represents the interests of Canada's Internet community internationally.

Document Version 1.5

About the Telecom Transparency Project

The Telecom Transparency Project investigates how telecommunications data is monitored, collected, and analyzed for commercial, state security, and intelligence purposes. The Project is associated with the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto. The Citizen Lab focuses on advanced research and development at the intersection of information and communications technologies, human rights, and global security.

Core to the Telecom Transparency Project's work is interrogating the practices of telecommunications service providers (e.g. AT&T, Vodafone, and Bell Canada) that route data traffic between communicating parties and the mechanisms that third parties use to access the digital information that is endlessly flowing through telecommunications service providers' networks. Rendering telecommunications processes transparent will help citizens, politicians, and businesses understand how private or public, and how secure or vulnerable, their communications are to service provider-linked communications interferences and data disclosures.

About the Author

This report was researched and written by Dr. Christopher Parsons.

Dr. Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently a Postdoctoral Fellow at the Citizen Lab, in the Munk School of Global Affairs with the University of Toronto as well as the Managing Director of the Telecom Transparency Project at the Citizen Lab.

Dr. Parsons' research focuses on how privacy is affected by digitally mediated surveillance and the normative implications that corporate and government surveillance has in (and on) contemporary Western political systems. He is currently investigating the rationales, processes, practices, and politics of third-party access to telecommunications data. In addition to publishing in academic journals and presses, he routinely presents findings to members of government and the media. He is also a Privacy by Design Ambassador and a Principal at Block G Privacy and Security Consulting.

Acronyms

3GPP	Third Generation Partnership Program
ADSL	Asymmetric Digital Subscriber Line
API	Application Program Interface
ATIP	Access To Information and Privacy
ATIS	Alliance for Telecommunications Industry Solutions
CALEA	Communications Assistance for Law Enforcement Act
CBSA	Canadian Border Services Agency
CDR	Call Dial Records
CIRA	Canadian Internet Registration Authority
CNA	Customer Name and Address
COL	Condition of License
CRA	Canadian Revenue Agency
CRTC	Canadian Radio-television and Telecommunications Commission
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CWTA	Canadian Wireless Telecommunications Association
DFAIT	Department of Foreign Affairs, Trade and Development
DHCP	Dynamic Host Configuration Protocol
DPI	Deep Packet Inspection
ETSI	European Telecommunications Standards Institute
FCC	Federal Communication Commissioner
GCHQ	Government Communications Headquarters
GPS	Global Positioning System
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP Address	Internet Protocol Address
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU	International Telecommunications Union
LEA	Law Enforcement Agency
LI	Lawful Interception
LTE	Long Term Evolution
MAC Address	Media Access Control Address

MBS	Mobile Broadband Services
Mhz	Mega Hertz
MLAT	Mutual Legal Assistance Treaty
MP	Member of Parliament
OCSEC	Office of the Communications Security Establishment Commissioner
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	Personal Information Protection and Electronic Document's Act
PRG	Pseudo-Random Generator
PSC	Public Safety Canada
PSTN	Public Switched Telephone Network
PTSC LAES	Packet Technologies and Systems Committee Lawfully Authorized Electronic Surveillance
RCMP	Royal Canadian Mounted Police
SCC	Supreme Court of Canada
SGES	Solicitor General's Enforcement Standards
SIGAD	Signals Intelligence Activity Designator
SIGINT	Signals Intelligence
SIRC	Security Intelligence Review Committee
SMS	Short Message Service
TSP	Telecommunications Service Provider
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPD	Vancouver Police Department
W3C	World Wide Web Consortium
WTP	Wireless Telecommunications Provider
WTSC LI	Wireless Technologies and Systems Committee Lawful Intercept

Executive Summary

This report, *The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians*, examines how contemporary telecommunications surveillance is governed. In this report, we ask how much telecommunications surveillance is occurring in Canada, what actors are enabling the surveillance, to what degree those actors disclose their involvement in (and the magnitude of) surveillance, and what degree of oversight is given to the federal governments' surveillance practices. We conclude that serious failures in transparency and accountability indicate that corporations are failing to manage Canadians' personal information responsibly and that government irresponsibility surrounding accountability strains its credibility and aggravates citizens' cynicism about the political process. In aggregate, these failings endanger both the development of Canada's digital economy and aggravate the democratic deficit between citizens and their governments.

Section One identifies key pieces of legislation that have affected, or soon might affect, the magnitude of government agencies' telecommunications surveillance. The section also catalogues surveillance that key federal policing, security, and intelligence agencies currently conduct. **Section Two** explores how such surveillance is possible. We first discuss how lawful interception systems, which are used to provide telecommunications information to domestic policing and security agencies, are architected and then outline Canadian organizations' involvement in North American and European standards bodies that develop these interception standards. We also examine the rules concerning mobile telecommunications surveillance in Canada and discuss how Canada's signals intelligence agency monitors Canadians' domestic communications. **Section Three** shifts to analyze the transparency policies that Canadian telecommunications service providers have adopted. We focus on the transparency reports, data retention period disclosures, and law enforcement guideline handbooks. We also raise questions about these companies' roles in enabling Canada's signals intelligence agency to monitor Canadians' communications. After discussing the extent of telecommunications surveillance, how it is architected, and corporations' roles in facilitating such activity, we turn to the limitations of government oversight and review. **Section Four** explores the roles and limitations surrounding the oversight and review of federal institutions' telecommunications-related surveillance practices. We find that regardless of the positive intentions of the persons working within these oversight institutions, their intentions are diminished by their institutions' mandates, lack of resources, or lack of order-making powers.

In **Section Five,** we discuss the risks that are associated with contemporary telecommunications surveillance. We focus on the harms that can be linked to citizens' inability to know how companies and government are using their personal information. Additionally, we show how oversight deficits and the secrecy surrounding government surveillance activities combine to challenge citizens' ability to see themselves as authors who have authorized Canada's surveillance laws. Finally, we recognize how a lack of knowledge regarding contemporary surveillance activities inhibits citizens' ability to trust their elected representatives to hold government – and its various bodies – to account. In effect, the extent of contemporary surveillance practices combined with the practices' secrecy raise serious concerns for the health of Canada's democracy.

In **Section Six,** we provide a range of recommendations to alleviate the risks associated with contemporary telecommunications surveillance. These recommendations are addressed to corporations and government. At the most basic levels, corporations and governments alike should become more transparent about their receipt of, or request for, telecommunications data. As such, companies ought to release extended transparency reports and governments should update their annual interception reports; together, these recommendations would reveal the amount of telecommunications surveillance that government agencies conduct each year. Corporations and government agencies should also commit to openly developing lawful interception standards and involve Canadians in any technical debates, and governments should meaningfully consult with Canadians before introducing new surveillance legislation. Government should also reinforce ministerial accountability to parliament by (re-)establishing inspectors general to oversee the activities of Canada's policing, security, and intelligence agencies. Furthermore, existing oversight and review bodies should be permitted to work more closely with one another so they can ensure that authorized telecommunications surveillance agencies are operating with the scope of their mandates and the law. Where inappropriate practices are discovered, the oversight agencies should be legally empowered to force surveillance agencies to modify their practices.

Canadians are deeply concerned about their online privacy, and they express such concerns when civil society organizations, the press, and survey research prompt them to do so. They are equally concerned with the secretive natures of contemporary surveillance and how previous and current legislation may lead to an increase in government surveillance. When the failure of corporations and

government to transparently explain the existing state of telecommunications surveillance is combined with citizens' and consumers' concerns, it becomes clear that companies and government must both step out of the shadows to explain how often and for what reasons Canadians' telecommunications data is retained and provided to government. Doing anything less than this will only fuel consumer concern about companies' data management practices and worsen the political cynicism that has taken hold amongst many Canadian citizens and residents.

Introduction

Canadians routinely use digital communications systems to conduct online banking, purchase goods from Internet brokers, find and develop friendships, engage in political action, undertake personal learning, and more. The Canadian Internet Registration Authority (CIRA) found that 87% of Canadian households were connected to the Internet in 2013, with average Canadians visiting more web pages per month than any other nationality.[1] Based on research conducted by the Office of the Privacy Commissioner of Canada (OPC), we know that Canadians are extremely concerned about their privacy and that, in 2014, six in ten people polled agreed that they have little expectation of privacy today because there are so many ways to compromise it.[2] The same OPC report found that 44% of Canadians are very concerned about government surveillance and 34% are somewhat concerned.

Concerns about government surveillance of communications systems are well founded. Accompanying Canadians' adoption of digital communications have been government demands for access to communications data that are either stored or transmitted by private Telecommunications Service Providers (TSP), such as Rogers, Bell Canada, and Shaw. Though the specific policies and laws used to access this data vary, the kinds of data that government can access are sensitive. Access to the content of a communication, such as the text of an email or words spoken during a phone call, can reveal the tenor or emotional charge of a conversation alongside the actual words exchanged between the communicating parties. Access to the 'metadata' pertaining to that conversation or to the data that is used to establish and route the communication, can be equally revealing. Knowing that a person received a call from her family doctor, then placed a call to their romantic partner, then their parents, and then with a planned parenthood clinic provides a strong indication of what the call was about. Similarly, analyzing mobile phone data to determine that two persons are routinely in the same home during the evening hours can be used to derive insights about their relationship status. And, while using a telecommunication device, access to the billing and address information that TSPs retain can be used to link what someone says or does pseudonymously to the person who registered the device.

---

[1] Canadian Internet Registration Authority. (2014). "CIRA Fact Book 2014," CIRA, retrieved February 14, 2015, http://cira.ca/factbook/2014/the-canadian-internet.html.

[2] Office of the Privacy Commissioner of Canada. (2014). "Public Opinion Survey: 2014 Survey of Canadians on Privacy," Government of Canada, retrieved January 19, 2015, https://www.priv.gc.ca/information/por-rop/2015/por_2014_12_e.asp.

In this report, we focus on the extent to which Canadian state authorities can access Canadians' telecommunications data, how such access is affected by standards and standards-setting organizations, and the governance processes that shield Canadians from unwarranted surveillance. Our goal is to contextualize the governance of state surveillance that is conducted on communications carried over mobile or wireline networks and, in the process, understand the potential harms that are linked to such surveillance activities. Throughout, we rely on primary and secondary documents, as well as limited interviews, most of which were conducted either on a background or not-for-attribution basis.

In **Section One,** we provide an overview of key telecommunications-related legislation and regulations, as well as the major federal agencies that are responsible for carrying out telecommunications surveillance. In the process, we also identify many of the kinds of surveillance each of these agencies conduct. **Section Two** discusses the roles of lawful interception standards and the processes by which government and private actors advance and develop them. We also explore what composes the core aspects of 'lawful intercept' standards that apply to Canadian wireless providers as well as the 'standards' that Canada's signals intelligence agency, the Communications Security Establishment (CSE), complies with in relation to its domestic mass surveillance technologies. **Section Three** sees us turn to the significance of corporations' data repositories and the extent to which corporations disclose information about government surveillance activities to the public. This section makes apparent that transparency reports circa 2015, while somewhat helpful for informing public debate, are not comprehensive enough to fully advance public debate around government access to TSP-held or -transited data. In **Section Four,** we discuss limitations concerning the oversight of federal institutions' telecommunications-related surveillance practices; the sophistication and breadth of government telecommunications data surveillance is, arguably, not matched by that of the independent organizations tasked to oversee, review, and investigate such practices. **Section Five** discusses the implications of the extent of government surveillance, overall lack of corporate transparency, and relatively weak oversight and review mechanisms we conclude that these conditions risk affecting how Canadians communicate as well as weaken their trust in government institutions. **Section Six** concludes by offering a series of policy recommendations that, if implemented, would enhance transparency and accountability concerning government access to telecommunications data.

Section One: An Overview of Government Telecommunications Surveillance

This section discusses noteworthy security and intelligence legislation and regulations that either currently enable government surveillance of telecommunications networks, or that are proposed to facilitate or expand such surveillance. It then discusses key federal agencies that conduct such surveillance. We are focused principally on federal security and intelligence agencies' access to telecommunications data vis-a-vis Canadian organizations. As such, we do not focus on the legislation or statutes authorizing non-security agencies' access to telecommunications data, nor on the provincial statutes or laws that authorize provincial and municipal bodies to access such data.

Lawful Access Legislation

Since the Canadian government signed the *Convention on Cybercrime* on November 23, 2001, successive Canadian governments have sought to pass lawful access legislation. Lawful access powers enhance or extend government agencies' search and seizure powers, communications interception powers, and subscriber data production powers. This *Convention* was meant to coordinate international legal codes such that signatory governments can detect, investigate, and prosecute computer-based criminal activities. More specifically, part of the ratification process requires signatories to define "several offences, including unlawful interception, access or interference with a computer system, computer-related forgery and fraud, and offences relating to child pornography and copyright."[3]

Successive rounds of consultations have occurred since 2001, helping the government to understand the positions of various stakeholders while informing a series of legislative proposals that were introduced to ratify elements of the *Convention*. Governments have asserted that the *Convention* had to be ratified in law, with attendant new powers, to protect Canadians from serious crime and terrorist attacks, identify and prosecute pedophiles, catch violent offenders, and

[3] Daphne Gilbert, Ian Kerr, and Jena McGill. (2006). "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," *Criminal Law Quarterly* 51(4), p. 480.

address cyberbullying.[4] The following variety of powers have been attached to successive versions of the legislation:

- TSPs must be able to intercept their subscribers' communications
- Authorities can compel subscriber data from TSPs without a court order
- Mandated creation of new preservation and production orders
- 'Key escrow' system for encrypted communications established
- Government agencies authorized to install malware on location-aware devices, such as smartphone and GPS-equipped devices[5]

Throughout the consultations a common set of actors, including law enforcement organizations, TSPs, civil rights advocates, consumer rights advocates, academics, and members of government, were involved. Canada's lawful access legislation was ultimately passed into law under the guise of combatting cyberbullying. As summarized by McCarthy Tétrault, the final bill included the following powers:

- A new offence of non-consensual distribution of intimate images, along with amendments authorizing the removal of such images from the Internet, the ability to recover expenses for such removals, and forfeiture of property used in committing such a distribution offence
- A preservation demand of computer data on grounds to suspect an offence has, or may, be committed. Such demands are made directly by a public officer to a TSP without first going before a court, with data having to be retained for twenty one days for domestic offences or 90 days when the demand is made pursuant to an international investigation. Preserved data is released to the public officer after they convince a judge that there are reasonable grounds to suspect that the preserved computer data will assist in the investigation of an offence
- A production demand for transmission data, or data that relates to telecommunications functions, such as dialing, signaling, routing, or addressing, where such data is used to identify, activate, or configure a device

[4] Christopher Parsons. (Forthcoming 2015). "Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada," in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: Ottawa University Press.

[5] Christopher Parsons. (Forthcoming 2015). "Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada," in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: Ottawa University Press.

so as to establish or maintain a telecommunications service. Similarly, such data may be generated during the creation, transmission, or reception of a communication. The data could include data fields such as direction, date, time, duration, size, origin, destination, or termination of a communication, and it might specifically include IP addresses of visited websites or mobile phone signaling information

- A tracking data production order that is used to obtain location information associated with a device, such as a cellphone, or a motor vehicle. The collection of this information can be obtained by using a software tool (e.g. installation of malware onto a mobile device or vehicle)
- A company may voluntarily retain and subsequently disclose computer data to a government agent and enjoy both criminal and civil immunity for doing so. Other legislation currently before Parliament (i.e. *Bill S-4, An Act to amend the Personal Information and Electronic Documents Act and make a consequential amendment to another Act*) would also let companies share information about individuals for the purposes of preventing, detecting, or suppressing fraud; protecting victims of financial abuse; investigating the breach of an agreement; or breaking of the laws of Canada or a province
- A set of fines that could be applied to individuals or organizations that refuse to comply with the above-mentioned aspects of the legislation. A person who refuses a preservation demand can receive up to a $5,000 fine and a person or organization that refuses a preservation or production order can receive a fine of up to $250,000 and/or up to six months of jail time[6]

These lawful access powers complement existing telecommunications interception and production powers as well as requirements associated with the *Solicitor General's Interception Standards*. We now turn to those standards.

[6] Sean Griffin, Anne-Elisabeth Simard, and Marianne Bellefleur. (2015). "Bill C-13: Lawful Access and the Relationship Between Organizations, Cyber-bullying and the Protection of Privacy Rights," *snIP/ITs: Insights On Canadian Technology and Intellectual Property Law*, February 25, 2015, retrieved March 13, 2015, http://www.canadiantechlawblog.com/2015/02/25/bill-c-13-lawful-access-and-the-relationship-between-organizations/.

The Solicitor General's Interception Standards

While lawful access legislation was being debated and contested, the federal government moved to implement aspects of the lawful access legislation as part of an Industry Canada wireless spectrum consultation and auction. As part of the consultation, Industry Canada indicated that the Department of Public Safety would propose modifications to the *Solicitor General's Enforcement Standards* (*SGES*). The *SGES* identify how mobile telecommunications companies must configure their networks to facilitate telecommunications interceptions and have existed since the early nineties.[7] Simultaneous to indicating that modifications to the *SGES* were coming, Industry Canada "proposed making all radio-based transmissions subject to interception requirements, whereas previously only circuit-based communications were subject to such requirements."[8]

Members of industry who opposed to lawful access-inspired proposal dominated the consultations. The Canadian Wireless Telecommunications Association (CWTA) warned that:

> there has been no enabling legislation passed by Parliament that would require such services to be intercepted, and submits it is inappropriate for the Department to impose such requirements by COL [Condition of License] — particularly at a time when the Government is engaged in a legislative process covering the lawful access issue at a broader level. The COL should reflect the legislative requirements that exist at the time the licences are issued, and not be crafted in anticipation of legislative requirements that may or may not be in force at some point in the future.[9]

[7] We include a discussion of the particularities of the *SGES* in Section Three.

[8] Christopher Parsons. (Forthcoming 2015). "Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada," in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: Ottawa University Press.

[9] Canadians Wireless Telecommunications Association. (2012). "Re: Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band," Canadian Radio-television Telecommunications Commission, June 22, 2013, retrieved January 27, 2014,

In addition to the wireless industry's questions about the appropriateness of the proposed expansions, there was an internal governmental debate about the appropriateness of the changes. Officials at Public Safety Canada, which is responsible for the *SGES*, believed that revised wording would let the *SGES* apply "more broadly and effectively" and function as "an interim measure until full implementation of the [lawful access] legislation."[10] The actual changes to the *SGES* would be revealed only after the conclusion of the 700 MHz consultation.[11] An analyst who worked for the Canadian Security Intelligence Service (CSIS) questioned the appropriateness of the path taken by Public Safety Canada and Industry Canada, writing:

> I would like to know where this "exercise" is going !!?? What is its overall purpose … my understanding was that we were simply trying to get the wording in the licensing regime changed (& not changing the SGES themselves … do you really want us to re-examine all the standards, etc; up date them to current requirements, [Redacted]?[12]

The government ultimately decided that the "changes would not expand the range or kinds of communications that had to be interceptable" and, instead, maintained that the same kinds of communications that were transmitted using circuit-based connections, such as text messages, faxes, and voice communications, would just need to remain interceptable when individuals communicated using contemporary packet-based radios.[13] Publicly, the government asserted "it never actually had designs on vastly expanding surveillance"[14] and, based on documents released

---

https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/DGSO-002-12-comments-CWTA-submission.pdf/$FILE/DGSO-002-12-comments-CWTA-submission.pdf.

[10] See Access To Information And Privacy document A-2012-00457 released by Public Safety Canada, Pp. 83-84.

[11] See Access To Information And Privacy document A-2012-00457 released by Public Safety Canada, Pp. 324.

[12] See Access To Information And Privacy document A-2012-00457 released by Public Safety Canada, Pp. 30-1.

[13] Colin Freeze and Rita Trichur. (2013). "Ottawa sought broader access to smartphone user data, records show," *The Globe and Mail*, September 13, 2013, retrieved January 6, 2015, http://www.theglobeandmail.com/technology/mobile/ottawa-sought-broader-access-to-smartphone-user-data-records-show/article14343991/.

[14] Colin Freeze and Rita Trichur. (2013). "Ottawa sought broader access to smartphone user data, records show," *The Globe and Mail*, September 13, 2013, retrieved January 6, 2015,

under Access To Information and Privacy (ATIP) legislation, we do not believe that a substantive change to the *SGES* took place.

C-44: Protection of Canada from Terrorists Act

Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts (Protection of Canada from Terrorists Act)*, codifies the Canadian Security Intelligence Service's (CSIS's) authority to operate abroad so long as it receives approval from a federal court. Specifically, the legislation states that:

> Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada.[15]

Bill C-44 also (re)extended the privacy CSIS affords to its confidential informants by providing the informants with equivalent privacy protections as are provided to law enforcement agencies' sources.[16] Though this protection is not absolute — the source's identity can be disclosed where necessary to establish an accused person's innocence — it is less clear whether "the new privilege for CSIS sources will prevail in security-certificate and other immigration cases, since the source-protection exception is confined to criminal prosecutions. Another concern is the potential for the privilege provisions to make terrorism prosecutions more difficult in some cases."[17] Using the powers included in this piece of legislation, CSIS could receive warrants to conduct telecommunications surveillance of Canadians travelling abroad, in addition to otherwise monitoring or acting on persons outside of Canada.

Bill C-51: Anti-terrorism Act, 2015

Bill C-51, An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential

---

http://www.theglobeandmail.com/technology/mobile/ottawa-sought-broader-access-to-smartphone-user-data-records-show/article14343991/.

[15] *Bill C-44: An Act to amend the Canadian Security Intelligence Service Act and other Acts*, s.8(2).

[16] *Bill C-44: An Act to amend the Canadian Security Intelligence Service Act and other Acts*, s. 7.

[17] Kent Roach and Craig Forcese. (2014). "Putting CSIS surveillance on a firmer legal footing," *The National Post*, October 29, 2014, retrieved January 3, 2015, http://news.nationalpost.com/full-comment/kent-roach-and-craig-forcese-putting-csis-surveillance-on-a-firmer-legal-footing.

amendments to other Acts (Anti-terrorism Act, 2015), is currently before the Canadian Senate at the time of writing. This legislation includes a range of new powers that will ostensibly enhance existing CSIS and other government agencies' power to combat terrorism and serious crimes. The legislation authorizes the arrest of individuals if law enforcement agencies believe that an individual may carry out a terrorist act;[18] it also establishes a terrorism peace bond.[19] Judges would be required to consider imposing other restrictions on the individual, including surrendering their passport, subjecting them to electronic monitoring, or ordering that they cannot leave the country.[20] The legislation would also criminalize the promotion of terrorism[21] and allow court proceedings to be sealed in immigration proceedings at any point during the proceeding; such seals protect investigative techniques and witnesses.[22] In addition, the bill authorizes the government to add anyone to the no-fly list whom it believes might be travelling to engage in terrorism.[23]

While monitoring for the promotion of terrorism, CSIS or other security and intelligence agencies may intercept or analyze Canadian citizens' or residents' communications. Moreover, C-51 would authorize CSIS to disrupt activities linked to threats to Canada and engage in "counter messaging". Past reviews of CSIS activities revealed that the organization has conducted disruption activities, that the Minister of Public Safety was not apprised of such disruption activities, and that

[18] *Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, s. 17.
[19] *Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, s. 24.
[20] *Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, s. 17.
[21] *Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, s. 16.
[22] *Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, s. 22.
[23] *Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, s. 8-9.

disruption was undertaken "in the absence of appropriate guidance."[24] In the context of Bill C-51, academics and researchers have warned that CSIS' use of disruption warrants could endanger Crown prosecutors' abilities to prosecute terrorism-related cases because CSIS' disruption activities may be unlinked from crime investigations and, as such, involve CSIS acting in ways that would bias any subsequent criminal investigations.[25]

Bill C-51 would also let the government order the seizure of terrorist propaganda. Practically, this means that officials could apply to a court for permission to seize or to force a website to remove "any materials that promote or encourage acts of terrorism against Canadians in general, or the commission of a specific attack against Canadians."[26] It remains unclear whether CSIS or another government body would make these requests.

Finally, C-51 expressly states that activities that undermine the security of Canada include interfering with intelligence-gathering practices as well as interfering with the 'global information infrastructure' (i.e. the Internet). Interfering with intelligence gathering may include the use of encryption products that the government cannot decrypt. Interfering with the Internet is also very broadly defined: interference could include 'hacking' a Canadian TSP, knowingly or unknowingly interfering with how data packets are routed online, or otherwise affecting the flow of information between Canadians. In effect, even if authorities cannot monitor a given communication, perhaps because it is encrypted, the very fact that a communication is encrypted could itself potentially be used to justify investigations meant to guarantee or protect national security interests.

[24] Security Intelligence Review Committee (SIRC). (2010). "CSIS's Use Of Disruption to Counter National Security Threats (SIRC Study 2009-05)," Government of Canada, June 2, 2010.
[25] Craig Forcese and Kent Roach. (2015). "Bill C-51 Backgrounder #2: The Canadian Security Intelligence Service's Proposed Power to "Reduce" Security Threats through Conduct that May Violate the Law and Charter," *Canada's Proposed Antiterrorism Act: An Assessment*, February 12, 2015, retrieved February 21, 2015, http://static1.1.sqspcdn.com/static/f/842287/25955621/1423917614487/Final+Backgrounder+on+CSIS+Powers+v1.pdf.
[26] Laura Payton. (2015). "Anti-terrorism powers: What's in the legislation?" *CBC News*, January 30, 2015, retrieved February 15, 2015, http://www.cbc.ca/news/politics/anti-terrorism-powers-what-s-in-the-legislation-1.2937964.

Organizations that Conduct Security and Intelligence Surveillance

The Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), the Canadian Border Services Agency (CBSA), and the Royal Canadian Mounted Police (RCMP) conduct most security and intelligence surveillance in Canada. Other agencies, including the Department of Foreign Affairs, Trade, and Development (DFAIT), Fisheries and Oceans Canada, Canadian Revenue Agency, and others also conduct surveillance. These other agencies are not discussed in this report because no public evidence suggests that these government bodies conduct large volumes of domestic telecommunications surveillance.

Canadian Border Services Agency

The Canadian Border Services Agency (CBSA) was created in 2003 by an order-in-council that amalgamated Canada Customs with border and enforcement officers from the Department of Citizenship and Immigration Canada, as well as those from the Canadian Food Inspection Agency. The order-in-council was followed by the *Canada Border Services Agency Act*, which received Royal Assent on November 3, 2005. CBSA is responsible for border enforcement, immigration enforcement, and customs services. In the course of conducting its operations and in the course of its Inland Enforcement activities, CBSA conducts surveillance along national borders and at entry points.

CBSA enjoys extensive surveillance powers and keeps detailed records about the regularity at which it exercises those powers to conduct surveillance of telecommunications services. In 2012 and 2013, the agency made 18,849 requests for telecommunications information. None of these requests were for real-time access to data and, as such, the agency was not legislatively required to keep these records. CBSA's requests during this period included:

- 63 geolocation requests
- 118 call detail records requests
- 77 text message content requests
- 10 voicemail requests
- 128 cell tower log requests
- 0 real-time intercepts
- 18,729 requests for basic subscriber information

- 113 requests for transmission data
- 78 requests for web sites visited, IP addresses
- 15 requests for other data pertaining to the operation of TSPs' networks and businesses[27]

Only fifty-two of these requests were subject to a court order. No requests were made in exigent circumstances.

CBSA relies on a range of laws to access telecommunications data. The department can receive interception warrants that a justice issues on reasonable grounds to believe that a crime is or will be committed. They can also receive warrants authorizing them to install number dialer recorders, which log the numbers dialed to and from targeted phone numbers or devices and are issued on the standard of reasonable grounds to suspect that an offence under the *Criminal Code* or other act of Parliament has been or will be committed. CBSA can also request tracking warrants that are used to trace the movements of a person whom authorities have linked to a specific device. These sorts of warrants can involve using software, such as malware that is deployed to a targeted device, to conduct the tracking in real-time; alternately, production orders can disclose historical data that a TSP has retained. CBSA can also issue preservation orders and receive production orders for any other kind of data that a TSP transits or stores in the course of its business operations.

Communications Security Establishment

The Communications Security Establishment (CSE) is Canada's foreign signals intelligence agency. It has operated since the Second World War, but it is only since journalists have started to publish stories based on documents provided by Edward Snowden and other whistleblowers that Canadians have paid much attention to the agency's actions. CSE is responsible for fulfilling a series of mandates per s.273.64(1) of the National Defence Act:

- Mandate A: to acquire and use foreign signals intelligence in accordance with the Government of Canada's intelligence priorities
- Mandate B: to help protect electronic information and information

[27] Minister of Public Safety and Emergency Preparedness's Responses to MP Charmane Borg's Q-233 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf.

infrastructures of importance to the Government of Canada

- Mandate C: to provide technical and operational assistance to federal law enforcement and security agencies, including helping them obtain and understand communications collected under those agencies' own lawful authorities

CSE is permitted to collect private communications under signed Ministerial Authorization. Such communications are those that originate or terminate in Canada and where the communications are "attended with a reasonable expectation of privacy."[28] Such communications can be collected only to fulfill CSE's foreign intelligence mandate or information security mandate. To collect Canadians' private communications, CSE must meet the following four conditions: first, the interception must be targeted towards foreign entities located outside of Canada; second, the interception cannot be reasonably obtained by other means; third, the interception must be justified by its expected value; fourth, the privacy of Canadians must "be protected and information retained or used only if it was essential to international affairs, defence or security."[29]

Furthermore, CSE is authorized to intercept Canadians' private communications when a federal law enforcement or security agency requests CSE's assistance in intercepting communications. Such requests (and their fulfillment) are predicated on the requesting agency first receiving a court order that authorizes the interception. CSE provided assistance to the RCMP 85 times and to CSIS 205 times between 2009 and 2012 as part of its assistance mandate.[30] The full extent of CSE's assistance remains unclear though it can include monitoring RCMP or CSIS targets of surveillance when those targets travel abroad. CSIS and CSE work particularly closely with one another, with memorandums of understanding, secondments

[28] Wesley Wark. (2012). "Electronic Communications Interception And Privacy: Can The Imperatives Of Privacy And National Security Be Reconciled?" Government of Canada, March 2012, retrieved February 9, 2015, http://cips.uottawa.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf.

[29] Wesley Wark. (2012). "Electronic Communications Interception And Privacy: Can The Imperatives Of Privacy And National Security Be Reconciled?" Government of Canada, March 2012, retrieved February 9, 2015, http://cips.uottawa.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf.

[30] Colin Freeze. (2014). "Spy agency's work with CSIS, RCMP fuels fears of privacy breaches," *The Globe and Mail*, January 31, 2014, retrieved February 3, 2015, http://www.theglobeandmail.com/news/politics/spy-agencys-work-with-csis-rcmp-fuels-fears-of-privacy-breaches/article16623147/.

between agencies, and policy guidelines authorizing additional and often unwarranted assistance bonding the agencies together.[31]

CSE collects 'metadata' from the Internet or, as CSE's authorizing legislation calls it, the 'global information infrastructure'. Metadata is "information about an electronic or digital record" and can include "the date and time a phone call is made or the location from which an e-mail was accessed,"[32] as well as other data routing information such as IP addresses, communications protocols, message size, transmission originator and recipient, and more. While CSE "cannot and does not single out Canadian metadata for collection" the "complexity of global communications networks means that Canadian communications are commingled with international communications."[33] CSE uses metadata for analyzing foreign communications as well as for data science experiments.[34]

CSE is deeply enmeshed with its other signals intelligence allies in the collection and sharing of both collected signals data as well as analytic tools for parsing that data.[35] Leaked documents from 2008 suggest that CSE was unwilling to share Canadians' data with its allies[36] though it is unclear whether this general prohibition remains.[37] The revelatory nature of metadata and CSE's public assertion that its collection of the metadata of thousands or millions of Canadians doesn't constitute surveillance showcases that CSE regards metadata as having a reduced expectation of privacy — and, correspondingly, might be shared more readily when shared *en*

[31] Justin Ling. (2015). "Secret Documents Reveal Canada's Spy Agencies Got Extremely Cozy With Each Other," *Vice News*, May 20, 2015, retrieved May 20, 2015, https://news.vice.com/article/secret-documents-reveal-canadas-spy-agencies-got-extremely-cozy-with-each-other.

[32] Office of the Privacy Commissioner of Canada. (2014). "Metadata and Privacy: A Technical and Legal Overview," Government of Canada, October 2014, retrieved February 19, 2015, https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.pdf.

[33] See Access to Information and Privacy, A-2014-00059 released by CSE, pp. A009168_4-000026.

[34] Israel, T. (Forthcoming). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." In M. Geist (ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: Ottawa University Press; Access to Information and Privacy, A-2014-00059 released by CSE, pp. A0009162_1-000003.

[35] See: Christopher Parsons. (2015). "Canadian SIGINT Summaries," *Technology, Thoughts, and Trinkets*, retrieved March 15, 2015, https://www.christopher-parsons.com/writings/cse-summaries/.

[36] Unknown Author. (2008 - alleged). "Cheltenham Working Document (Fragments)," April 22-23 (alleged), retrieved January 15, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2014/12/cheltenham-working-document-pieces.pdf.

[37] Unknown Author. (2011). "CASCADE: Joint Cyber Sensor Architecture," Communications Security Establishment, retrieved March 24, 2015, https://www.christopher-parsons.com/writings/cse-summaries/#cse-cascade-joint.

mass — than either private communications or metadata that is knowingly tied to a single identified Canadian.

As will be discussed in Section Two, CSE's capacities may augment those that domestic companies better understand and know about, and which are typically used by government agencies to gain access to telecommunications data. In effect, domestic companies may be largely unaware of CSE's data collection efforts while domestic policing and intelligence agencies are only broadly aware of the specific collections methods, while being much aware of the amount of data accessible vis-à-vis CSE.

The Canadian Security Intelligence Service

CSIS was created in 1984 following the *Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police* (the MacDonald Commission), which reviewed the activities of the RCMP's Security Service. The MacDonald Commission found that the Security Service had engaged in a series of actions that were either not authorized or provided for by law, or, where the activities were lawful, were regarded as inappropriate.[38] The latter included activities such as break-ins, electronic surveillance, mail interception, access to confidential information held by other government departments, and under-cover operations.[39] CSIS was formed to separate Security Intelligence work from RCMP policing and investigation operations; the legislation creating CSIS had the effect of legalizing "those security intelligence activities the legality of which had hitherto been in doubt."[40]

Since 1991, CSIS has largely focused on "counter-terrorism, economic espionage, weapons of mass destructions, and foreign influenced activities deemed

[38] Laurence Lustgarten and Ian Leigh. (1994). *In From The Cold: National Security and Parliamentary Democracy*. Oxford: Clarendon Press.

[39] Peter Gill. (1989). "Symbolic or real? The impact of the Canadian security intelligence review committee, 1984–88," *Intelligence and National Security* 4(3), pp. 550-575; see also: Reg Whitaker, Gregory S. Kealey, and Andrew Parnaby. (2012). *Secret Policing: Political Policing in Canada from the Fenians to Fortress America*. Toronto: University of Toronto Press.

[40] Peter Gill. (1989). "Symbolic or real? The impact of the Canadian security intelligence review committee, 1984–88," *Intelligence and National Security* 4(3), p. 552; see also Reg Whitaker, Gregory S. Kealey, and Andrew Parnaby. (2012). *Secret Policing: Political Policing in Canada from the Fenians to Fortress America*. Toronto: University of Toronto Press and Laurence Lustgarten and Ian Leigh. (1994). *In From The Cold: National Security and Parliamentary Democracy*. Oxford: Clarendon Press.

detrimental to the national interests of Canada."[41] CSIS also plays a role in security screening of immigrants, collaborates with the Canadian Revenue Agency (CRA) to investigate abuses of charitable status by groups affiliated with terrorist organizations, and works to identify some cyber-based threats to domestic critical infrastructure.[42]

Since CSIS' inception, the agency has conducted surveillance on Canadians and collected intelligence pursuant to Canada's national security. Writing in 1986, Murray Rankin acknowledged that:

> [a]gents of C.S.I.S. may open mail, tap telephones, acquire access to medical records and income tax information, surreptitiously enter residences and offices to investigate, plant listening devices, and invoke a long list of other generally framed powers in the [CSIS] act, subject to two conditions: 1 / that the investigation is 'strictly necessary to obtain information and 2 / that the information concerns activities that may 'on reasonable grounds be suspected of constituting threats to the security of Canada.'[43]

Currently, CSIS undertakes such activities as using paid sources and informants, as well as working with Canada's signals intelligence agency, the Communications Security Establishment (CSE), to monitor persons or groups subject to an authorized warrant. Between 2009 and 2012, as an example, CSIS requested assistance from CSE 205 times.[44] In 2013, Justice Richard Mosley challenged CSIS's collaboration with CSE when he rebuked CSIS for not explaining to Mosley that when CSIS approached CSE for assistance, that CSE would subsequently request other Western signal intelligence agencies' help to track the warranted individuals.

---

[41] Martin Rudner. (2002). "Contemporary Threats, Future Tasks: Canadian Intelligence and the Challenges of Global Security," in Norman Hillmer and Maureen Appel Molot (Eds). *Canada Among Nations 2002: A Fading Power*. Toronto: Oxford University Press.

[42] Martin Rudner. (2002). "Contemporary Threats, Future Tasks: Canadian Intelligence and the Challenges of Global Security," in Norman Hillmer and Maureen Appel Molot (Eds). *Canada Among Nations 2002: A Fading Power*. Toronto: Oxford University Press.

[43] Murray Rankin. (1986). "National Security: Information, Accountability, and the Canadian Security Intelligence Service," *The University of Toronto Law Journal* 36(3), p. 256.

[44] Colin Freeze. (2014). "Spy agency's work with CSIS, RCMP fuels fears of privacy breaches," *The Globe and Mail*, January 31, 2014, retrieved December 11, 2014, http://www.theglobeandmail.com/news/politics/spy-agencys-work-with-csis-rcmp-fuels-fears-of-privacy-breaches/article16623147/.

This potentially placed Canadians and Canadian residents at risk of harm linked to the sharing of security information and was also (per Mosley) "a breach of the duty of candour owed by the service and their legal advisers in court."[45] Parliament recently passed into law legislation (Bill C-44, *Protection of Canada from Terrorists Act*) that authorizes CSIS to request CSE's assistance and, in turn, enable CSE to partner with foreign intelligence services to track those persons that CSIS is monitoring.

As noted elsewhere, debates are ongoing about whether to extend CSIS' operational powers under Bill C-51. CSIS already enjoys expanded powers as a result of the lawful access legislation, Bill C-13, which came into force in early 2015. CSIS can also receive interception, production, and number dialer warrants, just as CBSA and the RCMP do. Court orders issued to CSIS may be issued privately per the *Canadian Security Intelligence Services Act*.[46]

Royal Canadian Mounted Police

The Royal Canadian Mounted Police (RCMP) is Canada's federal policing body. The RCMP is mandated to prevent and investigate crime; to maintain peace and order; to enforce laws; to contribute to national security; to ensure the safety of state officials, visiting dignitaries, and foreign missions; and to provide operational support services to other domestic and international police and law enforcement agencies. The RCMP, along with other Canadian law enforcement agencies, has repeatedly called for enhanced intelligence-gathering powers in order to fulfill its mandates.[47]

Journalists, academics, and members of parliament have routinely tried to clarify and tabulate the kinds of surveillance that the RCMP conducts. Despite these groups' interest, the agency has rarely provided extended and holistic responses to

---

[45] Re X, 2013 FC 1275, https://www.canlii.org/en/ca/fct/doc/2013/2013fc1275/2013fc1275.html; see also: *Re X*, 2009 FC 1058, https://www.canlii.org/en/ca/fct/doc/2009/2009fc1058/2009fc1058.html and *Re CSIS Act*, 2008 FC 301, https://www.canlii.org/en/ca/fct/doc/2007/2007canlii62002/2007canlii62002.html.

[46] *C-23: Canadian Security Intelligence Service Act*, s. 27-28.

[47] e.g. Ottawa Citizen. (2007). "Web access powers needed to fight crime: RCMP," *Canada.com*, April 9, 2007, retrieved February 9, 2015, http://www.canada.com/saskatoonstarphoenix/news/national/story.html?id=1d424ebe-2fe9-4e79-bab5-8fd67fd1b441#__federated=1; see also Reg Whitaker, Gregory S. Kealey, and Andrew Parnaby. (2012). *Secret Policing: Political Policing in Canada from the Fenians to Fortress America*. Toronto: University of Toronto Press.

the questions put to it. The following paragraphs include a summary of the kinds of telecommunications records that we know that the RCMP requests and information about where (and why) gaps exist in our knowledge about the kinds of telecommunications data that the RCMP requests from TSPs.

Access To Information and Privacy (ATIP) documents reveal that the RCMP contacted TSPs for customer name and address information at least 28,143 times in 2010. In 93.6% of cases, ISPs voluntarily provided information to authorities whereas in all other cases TSPs demanded a warrant before they would disclose the information.[48] In response to questions issued by a member of parliament in 2014, the RCMP asserted that it did "not maintain a centralized data repository that would allow it to determine the total number of requests to telecommunications service providers for customers' usage of communications devices and services".[49] A separate investigation by the Office of the Privacy Commissioner of Canada (OPC) confirmed that the RCMP lacked a record-keeping system for subscriber data requests.[50] As a result of a decision passed down by the Supreme Court of Canada (SCC) in 2014, which restricted how Canadian authorities could request subscriber records without a court order, the RCMP is presumably receiving fewer subscriber data records when it asks for them without a court order than in years past.[51] The question of the RCMP's (and other LEAs') access to subscriber data records figured prominently throughout the debates and contestations surrounding Canadian lawful access legislation.[52]

The RCMP can avail itself of a range of laws to collect telecommunications data. It can receive interception warrants, which are issued when reasonable grounds for believing that a crime is or will be committed exist. Such interception warrants

[48] See Access to Information and Privacy document released by Public Safety Canada, A-2011-00220.
[49] Minister of Public Safety and Emergency Preparedness's Responses to MP Charmane Borg's Q-233 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf.
[50] Tom J. Fitzpatrick. (2014). "Memorandum: Review of the Royal Canadian Mounted Police — Problems with statistics and identifying warrantless access files," Government of Canada. Released under Access To Information and Privacy by the Office of the Privacy Commissioner of Canada.
[51] *R. v. Spencer*, 2014 SCC 43. Though anecdotal, ATIPs issued to the Halifax and Vancouver police departments revealed that there have historically been warranted and unwarranted requests for subscriber data records. While unwarranted requests have fallen to 0 in the ATIPed departments, warranted requests continue to be issued to TSPs.
[52] Christopher Parsons. (Forthcoming 2015). "Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada," in Michael Geist (Ed.). *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: Ottawa University Press.

authorize the RCMP to receive data in real-time and can apply to telephone conversations, Internet traffic, text messages, and other forms of real-time communications. Other warrants authorize authorities to install number dialer recorders, which log the numbers dialed to and from targeted phone numbers or devices. These warrants are issued on the standard of reasonable grounds to suspect that an offence under the *Criminal Code* or other act of Parliament has been or will be committed. Tracking warrants have an equivalent standard that must be met before a judge will issue them. Alternately, the RCMP can obtain production orders to compel a TSP to disclose historically retained location data. The RCMP can also issue preservation orders and subsequently receive production orders to access telecommunications data that a TSP transits or stores in the course of its operations.[53]

Summary

The federal security, intelligence, and policing agencies of Canada can avail themselves of a diverse set of laws to authorize their telecommunications surveillance. And, legislation that is currently before the Senate may further extend their existent capabilities.

As we discuss in Section Two, these capabilities must be supported at a technical level and often by TSPs' infrastructures. Such support can include the following measures:

- Integrating and deploying 'lawful intercept' capable devices
- Governing agencies support of interception system developments
- Working at international standards organizations to ensure that technology vendors' products meet Canadian interception requirements
- Inserting signals intelligence monitoring networks within domestic companies' telecommunications infrastructures

The ability to use these various technical systems, however, is predicated on the legal and legislative authorities enjoyed by federal institutions as was described in this section.

[53] The RCMP employs a diverse range of other technologies and surveillance systems, such as License Plate Recognition systems in British Columbia and Unmanned Aerial Vehicles by provincial detachments. Many of these technologies and systems have been critiqued and reformed in the light of such critiques but, given that they are not focused on telecommunications data, are not discussed in this report.

Section Two: Lawful Interception of Telecommunications in Canada

A judicial order authorizing lawful surveillance isn't enough to actually conduct telecommunications surveillance; telecommunications providers must engineer their products and infrastructures so communications can be captured and delivered to requesting government agencies. In this section, we first provide a high-level conceptual explanation of how telecommunications networks must be engineered to facilitate government interceptions. Next, we discuss some of the surveillance standards that key international organizations develop and that vendors use to standardize lawful interception capabilities in their products. We then transition to speaking directly about Canadian networks, explaining why mobile telecommunications networks across Canada are required to facilitate interceptions and how wireline systems have been threatened with similar requirements. We conclude by discussing how CSE collects information about Canadians' telecommunications activities; though different in scope from traditional 'lawful interception' equipment, the CSE infrastructure also monitors (and analyzes) Canadians data traffic as it transits to, and from, Canadian TSPs' networks and standardizes how it is captured in order to share information with its intelligence allies.

The Architecture of Lawful Interception

Government agencies that make lawful interception requests of telecommunications data first identify the areas of law they are using to authorize the request and then serve those requests on companies. Interceptions typically must be undetectable to subjects, prevent unauthorized personnel from performing or knowing about lawful interceptions, and prevent different agencies from knowing that they are monitoring the same subject (where that is the case).[54] Moreover, lawful interception infrastructure must often differentiate between Intercept Related Information (IRI), such as routing information or packet headers, and the content of communications, such as the words said in a conversation or the content of an email message. At a high-level conceptual level, we can visualize lawful interception architectures as depicted in Figure 1.

The infrastructure's lawful interception administration area allows a TSP to

[54] Paul Hoffmann and Kornel Terplan. (2006). *Intelligent Support Systems: Technologies for Lawful Intercept*. New York: Auerback Publications. P. 10.

establish the parameters of a given interception thus provisioning the interception. Such parameters may denote the identifiers that are used in targeting a given subscriber or group of subscribers, the duration of the intercept, and the type of content that is to be intercepted. The lawful interception administration area then passes the provisioning information to either the Interception Relay Information Intercept Access Point or Content Intercept Access Point depending on the legal order that the TSP was served. The Mediation Device receives the intercepted information and packages it into a format that the TSP and government agencies have agreed upon, often correlates the formatted data with a specific legal order, and, ultimately, delivers it to the government agency. This conceptual framework applies — with greater degrees of complexity when implemented in practice — for wireline voice and data services, wireless voice and data services, cable-based services, as well as for IP- and satellite-based service.[55]

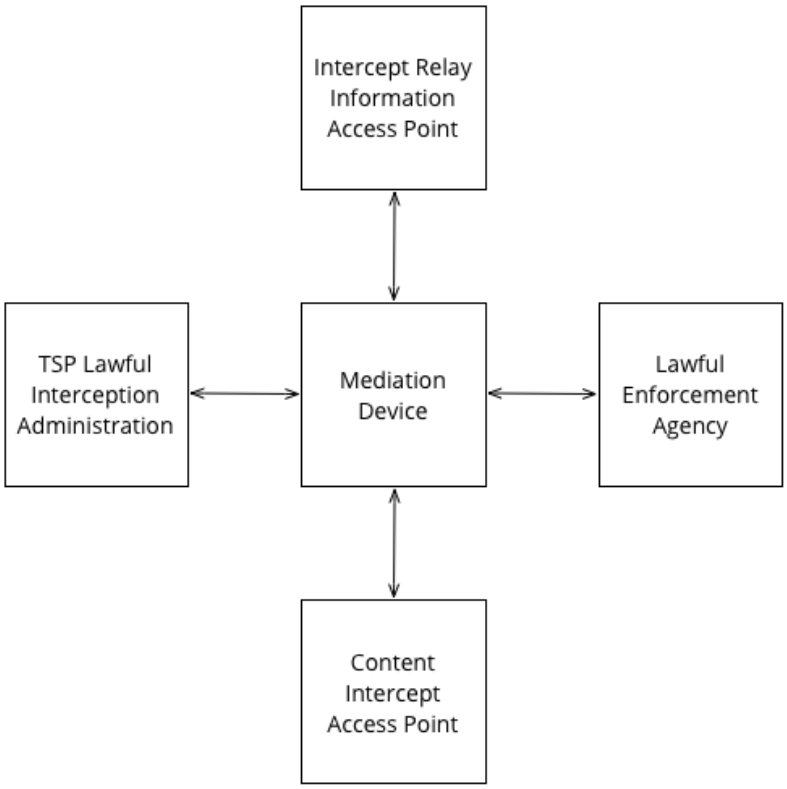

Figure 1: Conceptual Lawful Interception Architecture

Figure 1's basic conceptual model is complicated when accounting for the

[55] Paul Hoffmann and Kornel Terplan. (2006). *Intelligent Support Systems: Technologies for Lawful Intercept*. New York: Auerback Publications. Pp. 20-59.

bureaucratic processes that are associated with private companies intercepting information on behalf of government agencies. Figure 2 reflects this more complicated model, with letters indicating the different stages of the interception process.

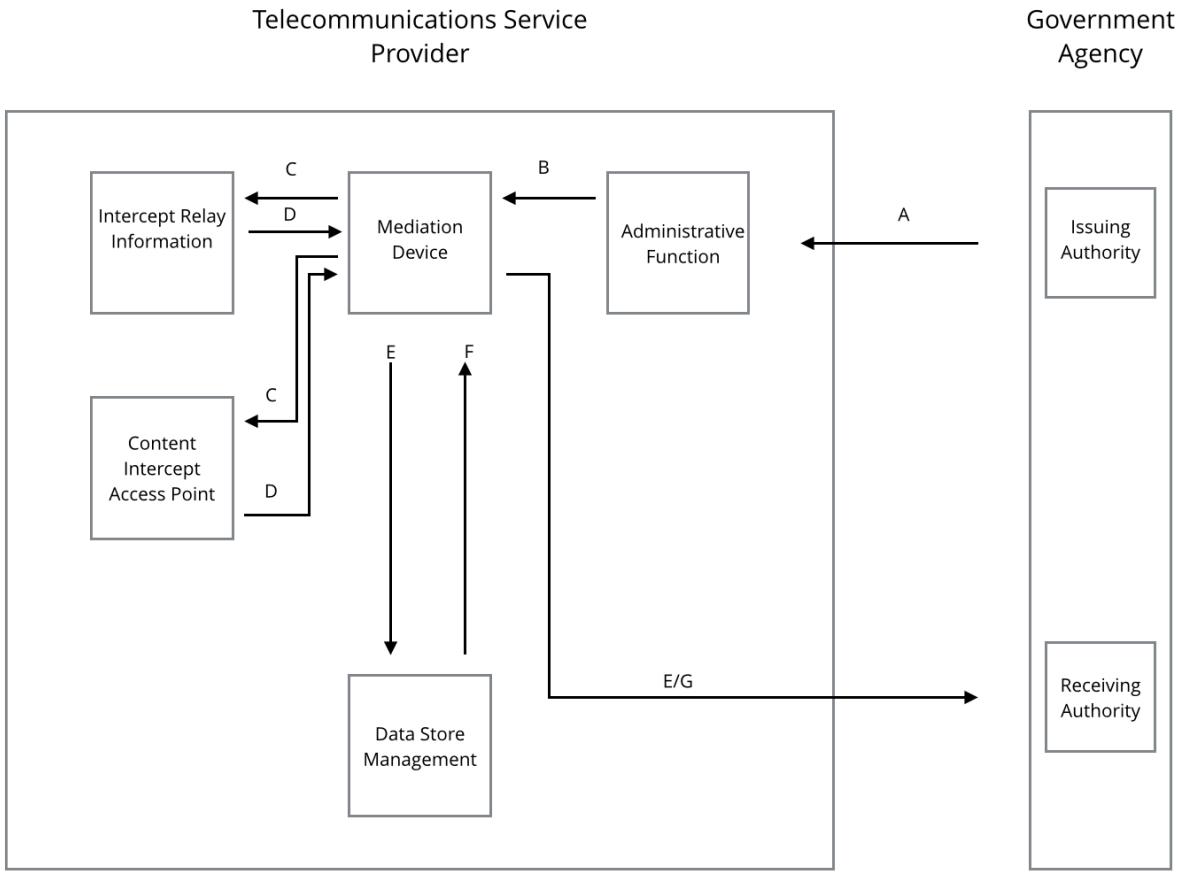

Figure 2: Lawful Interception Architectural Model

In particular, the 'issuing authority' first obtains the legal authorization to request or compel the telecommunications service provider to initiate the request and process the request, using the TSP's administrative functions. Next, the mediation device(s) are activated using the administrative functions to begin the interception of Intercept Relay Information and/or Content. The probes that collect the information then feed it back through the mediation device where collected data is either immediately transmitted to the receiving authority *or* sent to the data store management system. Data may be sent to this management system if a TSP has received a preservation request for telecommunications data but has not yet been served with an accompanying production order. In some jurisdictions, TSPs must retain legislatively mandated data elements in their data store management

systems until either the TSP is permitted to dispose of the data or until it is required to produce it in the course of a government authority's investigation.

Most commonly, a government agency relies on the TSP to perform intermediary functions; the TSP activates and operates the interception equipment and ultimately delivers the intercepted materials to the agency. In some cases, however, TSPs opt to automate a large part of the process. For these TSPs, government agencies can provide a court order electronically and then the IRI or content interception is activated without being scrutinized by the TSP. Intercepted data is then transformed into a data format agreed to by the agency and TSP, after which it is delivered to the requesting agency.[56]

It must be noted that the methods that Canadian TSPs use to collect, analyze, and process court orders can vary significantly; whereas some archive orders in email folders, others retain records in databases customized for holding orders, and still others depend principally on their billing systems for aggregate awareness of the number of orders they receive.[57] Based on interviews, we found an extensive variation in how TSPs received and processed court orders, and in how they recorded the aggregate reception of government requests for subscriber communications or data.

Standards Bodies and Lawful Interception

Standards organizations develop the technical functioning of each of the aforementioned conceptual elements of a lawful interception system in Figure 1 and Figure 2. The Alliance for Telecommunications Industry Solutions (ATIS) and the European Telecommunications Standards Institute (ETSI) are two of the key standards organizations that develop the interception standards that guide how North American TSPs intercept data traffic. Within ATIS, the Packet Technologies and Systems Committee Lawfully Authorized Electronic Surveillance (PTSC LAES) subcommittee develops standards for intercepting wireline TSP data. PTSC LAES typically focuses "in response to, legal and regulatory framework (per USA CALEA law and related FCC regulation, and Canadian regulations)."[58]

[56] Based on interview with former TSP employee.

[57] Based on interview with former TSP employee, current TSP employee, and former security services officer.

[58] Michael Fargano. (2011). "ATIS Lawful Intercept (LI/LAES) Standards Development," Global Standards Collaboration, October 31-November 3, 2011, Canada, Halifax.

Vendors who sell equipment to Canadian TSPs,[59] some Canadian TSPs, and (to a far lesser extent) Public Safety Canada represent Canadian interests at these standards organizations. Industry Canada, which operates spectrum auctions that require wireless providers to be able to intercept their subscribers' communications, is (at best) minimally involved in the North American standards body responsible for lawful interception standards. Specifically, Industry Canada informed us that it has no:

> [c]opies of standards documents, legal opinions, briefing notes, and memos concerning Alliance for Telecommunications Industry Solutions (ATIS) lawful interception standards. Inclusive of January 1, 2011 - November 1, 2014.[60]

ATIS members attempt to proactively support government agencies' requirements while avoiding "crossing the line" of what constitutes reasonable proactive support.[61] ATIS includes the Wireless Technologies and Systems Committee Lawful Intercept (WTSC LI) subcommittee, which coordinates lawful interception activities amongst North American partners, evaluates proposals for lawful intercept capabilities, and interprets the 3G security and lawful interception requirements[62] for the North American market. It also develops and coordinates "appropriate inputs regarding lawful intercept aspects that impact or are impacted" by the International Telecommunications Union's (ITU) third-generation mobile telecommunication standards.[63] The WTSC LI occasionally focuses exclusively on Canadian-related issues, as demonstrated by ATIS-0700009, which concerned Canadian-specific location requirements for lawfully authorized electronic surveillance, and current issue #40, which concerns Canada's implementation of mobile alerts services.[64]

ETSI is the second major telecommunications standards organization that sets a significant number of the lawful interception standards that are integrated into

[59] Based on interview with current TSP employee.
[60] See Access to Information and Privacy document released by Industry Canada, A-2014-00392.
[61] Michael Fargano. (2011). "ATIS Lawful Intercept (LI/LAES) Standards Development," Global Standards Collaboration, October 31-November 3, 2011, Canada, Halifax.
[62] See: 3G security; Lawful interception requirements at http://www.3gpp.org/DynaReport/33106.htm
[63] ATIS. (2015). "WTSC LI: Lawful Intercept," ATIS, retrieved March 14, 2015, http://www.atis.org/0160/li.asp.
[64] ATIS. (2015). "WTSC Issues," ATIS, retrieved March 11, 2015, http://www.atis.org/0160/issues.asp.

technology vendors' products. The main body in ETSI for lawful interception standards development and retained data handover standardization is the ETSI Technical Committee on Lawful Intercept. It became a stand-alone committee in 2002 and is mandated to create standards that let other ETSI standards (e.g. those mandating the operation of LTE or VoIP services) comply with national and international legal requirements. Practically, this committee determines how to integrate the interception and retention requirements of government agencies into technical specifications. The Committee also develops and publishes handover interface specifications and the rules for technology-specific interceptions. Canadian government officials and Canadian TSPs work with European and American partners to develop ETSI's lawful interception standards.

Part of the rationale behind ETSI's (and ATIS') standardization of lawful interception functions is to encourage vendors to produce cheaper products. As technology vendors integrate 'basic' interception functions into their equipment, those basic features become less expensive than featuring demanding high levels of customization in order for the lawful interception equipment to meet more specific national requirements.[65] Core ETSI documents offer guidance to government agencies on how data must be exchanged between TSPs and the agencies,[66] the requirements of how different network functions operate and interoperate (e.g. how network probes operate, how billing systems operate, etc),[67] and the ways that ETSI-covered telecommunications systems interface with one another and with LEA reception systems.[68]

---

[65] ETSI. (2008). "ETSI/TC LI Overview on Lawful Interception and Retained Data Handling," ISS World Europe, October 1-3, 2008, Prague, CZ.

[66] See: ETSI. (2001). "ETSI TS 101 331 v.1.1.1: Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf.

[67] See: ETSI. (2002). "ETSI ES 201 158 v1.2.1: Telecommunications security; Lawful interception (LI); Requirements for network functions," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_es/201100_201199/201158/01.02.01_50/es_201158v010201m.pdf.

[68] See: ETSI. (2006). "ETSI TS 101 671 v2.15.1: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/101600_101699/101671/02.15.01_60/ts_101671v021501p.pdf; ETSI. (1999) "ETSI ES 201 671 v1.1.1: Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_es/201600_201699/201671/01.01.01_60/es_201671v010101p.pdf; ETSI. (2002). "ETSI TR 102 053 v1.1.1: Telecommunications security; Lawful Interception (LI); Notes on

Other standards explain how email should the transmitted from TSPs to government agencies,[69] how TCP/IP, DHCP, and RADIUS information is transmitted,[70] as well as Public Switched Telephone Network (PSTN)/Integrated Services Digital Network (ISDN)[71] and mobile services[72] are transmitted between parties.

Internal ETSI documents that were shown to us reveal Rogers Communications' involvement in discussions around enabling lawfully authorized man-in-the-middle attacks on encrypted communications. Specifically, Rogers Wireless and Alcatel Lucent proposed lawful interception solutions for the 'MIKEY-IBAKE' framework. This framework, which "in addition to providing mutual authentication, eliminates the key escrow problem that is common in standard [Identity-Based Encryption] and provides perfect forward and backward secrecy"[73] should make it be very difficult to intercept and decrypt intercepted communications that are secured using MIKEY-IBAKE. Rogers Wireless and Alcatel responded to the challenge to find a lawful interception solution.

ISDN lawful interception functionality," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_tr/102000_102099/102053/01.01.01_60/tr_102053v010101p.pdf.

[69] See: ETSI. (2007). "ETSI TS 109 232-2 v2.2.1: Lawful Interception (LI); Handover Interface and Service Specific Details (SSD) for IP delivery; Part 2: Service-specific details for E-mail service," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/102200_102299/10223202/02.02.01_60/ts_10223202v020201p.pdf.

[70] See: ETSI. (2011). "ETSI TS 102 232-3 v2.3.1: Lawful Interception (LI); Handover interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/102200_102299/10223203/02.03.01_60/ts_10223203v020301p.pdf.

[71] ETSI. (2007). "ETSI TS 102 232-6 v2.2.1: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/102200_102299/10223206/02.02.01_60/ts_10223206v020201p.pdf.

[72] ETSI. (2012). "ETSI TS 102 232-07 v3.1.1: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services," *ETSI*, retrieved November 11, 2014, http://www.etsi.org/deliver/etsi_ts/102200_102299/10223207/03.01.01_60/ts_10223207v030101p.pdf.

[73] V. Cakulev and G. Sundaram (Alcatel Lucent). (2011). "RFC 6267: MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY)," *IETF*, June 2011, retrieved November 14, 2014, https://tools.ietf.org/html/rfc6267.

Rogers and Alcatel Lucent proposed that "[i]nstead of deploying the true random number generator to create the random secret" that is used to establish an end-to-end encrypted communication, "a pseudo-random number generator (PRG) is deployed in the client application of the user device."[74] The Rogers/Alcatel Lucent solution would let a TSP either decrypt traffic in real time or retroactively decrypt traffic that had been encrypted using the PRG. As such, their proposal would effectively undermine the core security design decisions that were 'baked' into MIKEY-IBAKE.[75]

Other documents further showcase Rogers' contributions to ETSI, including discussions about the extent to which TSPs must integrate lawful interception requirements into cloud services, such as Dropbox-like file services, that they offer to customers. Rogers regarded "the work on [lawful intercept] for the cloud services as an important factor in building a fair competition environment for the 3GPP mobile operators, in the area of cloud services offerings."[76] In a related vein, in 2014, Rogers discussed the extent to which lawful intercept interfaces needed to change as companies like Google moved to increasingly encrypt the Web. Specifically, Rogers questioned whether Google would have to provide interception functionalities (if Google had such obligation), whether a mobile wireless operator carrying Google or other encrypted traffic was obligated to intercept the data, or whether a proxy was required to intercept the material.[77] At the same 2014

[74] Alcatel Lucent and Rogers Wireless. (2012). "Candidate LI solutions for MIKEY-IBAKE based on re-generation of random secret: Discussion and decision," 3GPP TSG-SA3LI, SA3#44LI, January 17-19, 2012, Barcelona, Spain.

[75] Curiously, two years earlier a representative of the British signals intelligence agency, the Government Communications Headquarters (GCHQ), stated that: "An additional concern in the UK is that performing an active attack, such as the Man-in-the-Middle attack proposed in the Lawful Interception solution for MIKEY-IBAKE may be illegal. The UK Computer Misuse Act 1990 provides legislative protection against unauthorized access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material. A Man-in-the-Middle attack causes modification to computer data and will impact the reliability of the data. As a result, it is likely that LEMPFs and PLMNs would be unable to perform LI on MIKEY-IBAKE within the current legal constraints." See: "LI of MIKEY-IBAKE, a UK perspective: Discussion," 3GPP TSG-SA WG3-LI Meeting #38, 7-9 September 2010, Tallinn, Estonia.

[76] Rogers Wireless. (2012). "Scope of work on LI solutions for Mobile Cloud Services," 3GPP TSG-SA3LI, SA3#44LI, January 17-19, 2012, Barcelona, Spain.

[77] Rogers Wireless. (2014). "Web Encryption Discussion," 3GPP TSG-SA3LI, SA3LI #55, October 28-30, 2014, Portland, Or.

meeting, Rogers also discussed the preservation demands included in Canadian lawful access legislation. A Rogers employee noted that preservation processes were "not implemented in the current specification" and that most of the information to be preserved" are stored on Business systems, and no interfaces exist for LI for 3gpp Specification." The Rogers' employee worried that the large volume of data that might be asked to be preserved, such as for cloud data, could take time to retrieve and when delivered to government agencies electronically "may create bottle necks in existing delivery solutions." Though no decision was reached, the author proposed the preservation requirements be considered in the "evolving LI standards."[78]

Separately at ETSI, and also based on documents shown to us, Public Safety Canada (PSC) worried in 2015 that WebRTC could prove resistant to lawful interception. WebRTC is an Application Program Interface (API) that supports browse-to-browser applications for voice calling, video chat, and peer-to-peer file sharing. PSC recognized that WebRTC's security policies were specifically designed "around blocking man-in-the-middle ("The Man"-in-the-middle?) attacks and that the key standards organizations promoting WebRTC, the IETF and W3C, were not "LI friendly."" PSC also noted that the encryption included in WebRTC - perfect forward secrecy - would prevent the lawful interception of the content of communications.[79]

Standards that are developed at ATIS and ETSI are the result of discussions and meetings between vendors, TSPs, and government agencies. The standards are then integrated into both the products developed and sold by vendors and the networking architectures and policies used by TSPs. Similar discussions and standards-setting activities occur at events and proceedings hosted by organizations such as the Internet Corporation for Assigned Names and Numbers, the International Telecommunications Union, CableLabs. Actually using these standards, however, requires both domestic laws that authorize government agencies to make lawful interception requests and domestic regulations or policies that guide TSPs in using lawful intercept-enabled equipment to implement the laws.

Mobile and Wireline Interception in Canada

Canadian mobile lawful interception requirements are outlined in the *Solicitor*

[78] Rogers Wireless. (2014). "Preservation Discussion," 3GPP TSG-SA3LI, SA3LI #55, October 28-30, 2014, Portland, Or.
[79] Public Safety Canada. (2015). "WebRTC Overview," January 29, 2015.

General's Enforcement Standards (*SGES*). The standards were established in the 1990s and have not changed significantly since their inception; Wireless Telecommunications Providers (WTP) are required to agree to - and implement - the SGES as a condition of receiving a spectrum license, which, in turn, is required for a WTP to offer cellular connectivity service in Canada. The *SGES* have historically applied to circuit-based communications, such as faxes, cellular phone calls, and SMS messages. As discussed in Section 1, the government tried to expand the range of communications that WTPs would have to intercept as part of complying with the *SGES*. Those efforts appear to have failed.

The *SGES* outlines the conditions that WTPs must meet so government agencies can successfully receive information from the WTPs' own networks. As a starting point, all 'circuit-based' data that is sent from a mobile device must be interceptable and deliverable to government agencies. Also, the communications of long-term and temporary users of cellular networks must be interceptable. WTP systems must be able to parse the requirements of government agencies so that only the types of communications sought by the agencies are intercepted and only for the period of time the agency is authorized under statute or court order to receive the information. WTPs must also be able to correlate IRI and content so that law enforcement can meet its evidentiary requirements when presenting intercepted material in a court. This requirement means that WTPs must be able to record:

- Signaling of access-ready status
- Called number even if there is not a successful connection to it
- Calling-party number for incoming connections even if there is no successful connection established
- All digits dialed by the target, including post-connection dialed digits (i.e. numbers entered after a successful phone connection)
- Beginning, end, and duration of connection
- Actual destination and intermediate directory numbers if the call is diverted

WTPs also must provide the most accurate geographical information they possess about their subscribers' locations when ordered to do so by government agencies. The locations will often be found by engaging in cell tower triangulation or by evaluating the signal strength of devices connected to cellular towers.

Government agencies also expect WTPs to provide "all information with respect to a target's service, which indicate to us the capabilities the target may have" and that

there be "a real-time, full-time monitoring capacity for the interception of telecommunications. Call associated data should also be provided in real-time."[80] The actual delivery of intercepted materials occurs between handover interfaces; per the *SGES*, "law enforcement would like to see the information available in a non-proprietary format and one that can be easily handled."[81] Similarly, the mode of transmitting material from a WTP environment to a government agency must meet "standard industry accepted formats" and, where WTPs "initiate encoding, compression or encryption of telecommunications traffic," they must be able to provide the intercepted communications in the clear.[82] While end-to-end encryption that subscribers initiate does not need to be decrypted by the WTP, all WTP-initiated encryption must include a backdoor or escrow. All transmissions of intercepted material between WTPs and government agencies must be conducted in a secure fashion; if a WTP meets the required CSIS security level for data transmissions, it automatically meets the RCMP's and other law enforcement agencies' security requirements.

The standards assert that individuals who are subject to interception cannot discover such, "nor any other unauthorized person" of "any changes made to fulfill the interception…no unauthorized personnel are to be made aware of the interception."[83] In order to meet the security criteria associated with conducting interceptions, the service provider must ensure that "procedures and safeguards" are "implemented to prevent improper use of information related to the interception…This necessitates select individuals to be security cleared to the Top Secret level."[84] Included in the secrecy provisions is a prohibition on WTPs: they are to "protect" information about how many interceptions have been, or are being,

[80] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[81] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[82] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[83] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[84] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.

performed and "not disclose information on how interceptions are carried out."[85] Moreover, intercepted data can be delivered only to the agency that requested the information and not to any other; if multiple agencies are monitoring the same subscriber(s) these common actions cannot be disclosed to the various agencies.

WTPs are also sometimes required to provide detailed information about their subscribers, even before they receive a court order for an interception. Specifically:

> Law enforcement requires all pertinent information about the target in question in order to prepare and present the legal authorization document before the courts. This information would also include any services provided to the target such as voice mail, advanced calling features, roaming capability, etc.[86]

Wireless providers must assist government agencies and ensure that the communications being intercepted belong to those of the targeted person. As part of their 'assistance,' WTPs may be required to testify as to the accuracy of the interceptions in court.

Providers are also required to enable a range of different kinds of interceptions, including:

> **Simultaneous targets**: Where a number of targets must be intercepted at the same time, with the total number of possible targets established on a per-switch basis. Here, the maximum number of potential intercepts is what matters to government agencies.
> **Simultaneous multi-agency**: Where multiple agencies can make requests to target multiple persons at the same time. Here, the number of agencies that can be supported is what matters to government agencies.
> **Single target/multi-agency**: Where multiple agencies are able to monitor the same target. Here what matters is that the various agencies

[85] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[86] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.

do not learn that others are monitoring the same target.[87]

While on average, WTPs have three to five days to provision and begin an interception, they must be able to monitor a target's communications much more quickly in exigent circumstances. Throughout the interception period, government agencies require that "the reliability of the services supporting the interception" be at least equal to "the level of reliability of the target services provided to the interception subject" or, in other words, government agencies expect the same caliber of service as those they are monitoring.[88]

Wireline TSPs that provide cable, fibre, or ADSL connectivity do not have to comply with a standards document equivalent to the *SGES* to provide service to their subscribers. The absence of such wireline standards has led the government and private companies to conduct discussions about possible mandated wireline interception standards. Some of these discussions have included proposals that TSPs:

- Be able to operate as many as 200 simultaneous interceptions
- Respond to requests in as little as 30 minutes
- Transmit intercepted data in real-time
- Provide intercepted communications to up to five different government agencies at a time
- Increase the overall number of interceptions that a TSP could conduct beyond the initial simultaneous maximum

Early language about location disclosure requirements and compensation were also discussed.[89]

It should be noted that these discussions occurred during debate of lawful access legislation that predated the 2015 lawful access legislation that was passed into law. However, the discussions highlight the government's interest in mandating interception capabilities that all TSPs must comply with, regardless of the kind of

[87] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[88] Public Safety Canada. (2008). "Solicitor General's Enforcement Standards," November 17, 2008, retrieved January 19, 2014, http://www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[89] See Access to Information and Privacy document released by Public Safety Canada, A-2011-00255.

service that they offer to Canadians.

In an effort to forestall regulation, wireline TSPs have sought to assuage government concerns about their companies' abilities to intercept communications. Specifically, TSPs have "suggested that the proliferation of interception capability legislation and standards, and resulting growth in the marketplace of "built in" interception capacity, eliminates the need for Canada to have a specific interception capability in law…the telecommunications market will soon shift to a point where the interception capability will simply become a standard component of available equipment."[90] Some TSPs have also asserted that certain technologies, such as deep packet inspection, are not required to conform with wireline interceptions[91] and that industry should be left to decide which technology will suit government interception demands.[92] One interviewee conceded that deep packet inspection has come to constitute a threat to the industry that could be imposed upon the industry externally by government.[93] More generally, Canadian TSPs of all stripes have maintained that any new lawful interception requirements should conform with industry norms; 'Canada-specific' requirements should not be included in any law or regulations without appropriate funding from government to offset the costs of 'made-in-Canada' interception requirements.[94]

Analysts working at Public Safety Canada do not agree with the TSPs' assessment that all telecom networks will naturally become intercept capable. One analyst wrote:

> The claim that the telecommunications market will eventually evolve to a point where all service provider networks and equipment will naturally become intercept capable is not supportable. Canadian TSPs can

[90] Public Safety Canada. (2013). "Memorandum For The Minister: The Impact of International Lawful Interception Legislation On Telecommunications Equipment In Canada," Released Under Access to Information Act.
[91] Based on interview with Canadian TSP employee.
[92] Based on interview with Canadian TSP employee.
[93] Based on interview with Canadian TSP employee.
[94] Canadians Wireless Telecommunications Association. (2012). "Re: Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band," *Canadian Radio-television Telecommunications Commission*, June 22, 2013, retrieved January 27, 2014, https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/DGSO-002-12-comments-CWTA-submission.pdf/$FILE/DGSO-002-12-comments-CWTA-submission.pdf; also based on interview with Canadian TSP employee.

> purchase built in interception capability for their telecommunications equipment, but interception is a complex process that requires specific equipment or software, technical expertise, and ongoing operational management … other countries' legislative requirements and standards have no direct impact on the interception capability of Canadian TSPs. In the absence of a legislated requirement for TSPs operating in Canada to build, maintain and manage interception capacity, the ability of law enforcement and national security agencies to investigate serious crimes and gather intelligence on threats through the intersection of communications will continue to decrease year after year.[95]

Despite some companies' (such as Rogers Communications) engagement with standards organizations and Canadian government officials who try to inject Canadian concerns into lawful interception standards being developed at international organizations, it is not evident that these 'soft' efforts to ensure interception equipment will sufficiently meet Canadian government agencies' self-perceived needs. As such, wireline TSPs must continue to worry about mandated interception requirements as well as other regulations, such as the right of government officials to inspect the TSPs' networks for interception compliance or the ability to insert government of Canada-owned equipment in TSPs' networks for interception purposes. Both of these kinds of powers were included in past iterations of lawful access legislation and may return in future legislation.

Signals Intelligence Monitoring in Canada

In addition to government agencies such as the RCMP, CSIS, or CBSA that can lawfully compel TSPs to disclose information, Canada's signals intelligence agency, the Communications Security Establishment (CSE), collects information about Canadians' telecommunications activities. The collection of Canadians' communications occurs at key networking junctions around Canada and, more broadly, throughout the world at Signals Intelligence Activity Designators (SIGADs). SIGADs have programs associated with them that temporarily store all the content or metadata routed through the SIGAD for up to three days for content and thirty days for metadata.[96]

---

[95] Public Safety Canada. (2013). "Memorandum For The Minister: The Impact of International Lawful Interception Legislation On Telecommunications Equipment In Canada," released Under Access to Information Act.

[96] National Security Agency. (2008). "XKEYSCORE," United States Government, retrieved March 21, 2015, http://www.statewatch.org/news/2013/jul/NSA-XKeyscore-program.pdf.

Programs at SIGADs analyze and filter data traffic to pick out what is of value, discarding information that is not expected to contribute to a signals intelligence operation. A Canadian program, EONBLUE, operated at over 200 locations as of November 2010 and was responsible for analyzing the filtered data traffic at each SIGAD in order to identify threats, new targets, and to add metadata and content into other databases.[97] Government of Canada SIGADs have a comparable sensor network associated with them, codenamed PHOTONIC PRISM,[98] though there were plans to dispense with PHOTONIC PRISM and move all of Canada's sensors at SIGADs to EONBLUE-based detection and action systems.[99]

CSE is authorized to monitor Canadian telecommunications so "long as that data wasn't specifically targeted for collection on the basis of its being Canadian or related to a specific Canadian or person in Canada."[100] In the case of EONBLUE, the sensor network uses Deep Packet Inspection (DPI) equipment to analyze and act based on payload and header information of packets in real-time.[101] These conditions let EONBLUE take action on 'public' information (e.g. where a packet is being routed, at what time, etc.) and 'private' information (e.g. who is communicating with whom, what is being communicated, etc.). EONBLUE sensors are designed to extract information about the websites that individuals are visiting, header information that is exchanged between computers that are requesting information from servers, and target tracking information (e.g. cookie information or other user- or device-specific unique identifiers). These sensors may be responsible for a significant portion of the collection of Canadians' metadata that is

[97] Communications Security Establishment. (2009). "Cyber Threat Detection," Government of Canada, retrieved March 29, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-5-cyber-csec-sdf-gchq-nov2009.pdf.

[98] Communications Security Establishment. (2010). "Cyber Network Defence R&D Activities," retrieved March 29, 2015, https://www.christopher-parsons.com/writings/cse-summaries/.

[99] Communications Security Establishment. (2011). "CASCADE: Joint Cyber Sensor Architecture," retrieved March 29, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/cascade-2011-2.pdf.

[100] Bill Robinson. (2015). "EONBLUE: CSE cyber threat detection system "deployed across the globe"," *Lux Ex Umbra: Monitoring Canadian Signals Intelligence (SIGINT) Activities Past and Present*, February 11, 2015, retrieved March 3, 2015, http://luxexumbra.blogspot.ca/2015/02/eonblue-cse-cyber-threat-detection.html.

[101] See: Matthew Braga. (2011). "How Canadian Spies Infiltrated the Internet's Core to Watch What You Do Online," *Motherboard*, February 11, 2015, retrieved February 11, 2015, http://motherboard.vice.com/read/how-canadian-spies-infiltrated-the-internets-core-to-watch-what-you-do-online.

subsequently used in CSE's data science experiments.[102]

EONBLUE has been deployed by CSE and its Australian counterpart, and it interoperates with a range of databases that Australia, Canada, the United States, United Kingdom, and New Zealand signals intelligences agencies rely on to store and analyze the telecommunications data which they collectively capture from around the world.[103] As a result, we can say that EONBLUE is 'standards compliant' insofar as its data analysis and processing models cohere with the global information collection, storage, and analysis architecture of Canada's closest signals intelligence allies.

Some Canadian TSPs have incorporated the EONBLUE family of sensors in their networks. However, it is unclear which TSPs have done so and why they have done so. Some TSPs may have seen ministerial directives that authorize CSE's EONBLUE-based surveillance. Some equipment might have been deployed under a yet-sealed legal authorization. Some TSPs might have willingly incorporated the technologies without being required to do so. Some equipment might have been inserted as a secretive condition of a sale or license agreement. Or, lastly, some other entirely separate reason might exist. No TSP offering wireline, wireless, or satellite services, or which provides interconnection between different telecommunications companies or which carry data traffic using undersea cables have confirmed or denied their incorporation of EONBLUE or EONBLUE-like government sensors in their infrastructures.

Summary

Governmental agencies' abilities to collect telecommunications traffic depends on an infrastructure being in place to carry out such interceptions or produce requested data; law and regulations can impose obligations to assist government but do not dictate the technical standards or processes under which TSPs' data is disclosed to government. The architecture of lawful interception systems must be supported by a network of standards which, when instantiated at a technical level, let TSPs comply with the law.

---

[102] Christopher Parsons. (2015). "Canada has a spy problem," *National Post*, March 23, 2015, retrieved March 23, 2015, http://news.nationalpost.com/full-comment/christopher-parsons-canada-has-a-spy-problem.

[103] Communications Security Establishment. (2010). "CSE SIGINT Cyber Discovery: Summary of the current effort," Government of Canada, November 2010, retrieved January 17, 2015, https://www.christopher-parsons.com/writings/cse-summaries/.

Some Canadian TSPs are seemingly more involved than others to ensure that standards bodies proactively consider Canadian- or carrier-specific issues. This degree of involvement is telling when looking at Rogers Communications' involvement at ETSI. Similarly, some government agencies such as Public Safety are involved in lawful interception issues abroad whereas others, such as Industry Canada, appear to have largely chosen to avoid this particular standards arena.

TSPs have argued to government that TSPs' networks will be more intercept-friendly as more network equipment has lawful interception technologies 'baked in' by default. And they have sought to avoid specialized Canadian lawful interception solutions. Government analysts seemingly disagree that TSPs' networks will become more interception-friendly without legislation that requires their networks to conform to government lawful interception demands. No major TSP seemingly wants to step forward and address the critical question of whether or not it facilitates CSE's EONBLUE surveillance architecture. And no government analyst seems willing to publicly discuss in more depth the extent to which this architecture is used to capture data about Canadians' digital communications. In Section Three, we will more broadly discuss TSPs' transparency about how, how often, and why government agencies request and receive access to TSPs' subscribers' communications and personal information. As a result, we will come to understand the value of transparency efforts thus far and where improvements are still required if Canadians are to understand how TSPs manage their personal information.

Section Three: Corporate Transparency Policies

Canadian academics and civil rights organizations have called for increased transparency into how often, and for what reasons, government organizations request information from TSPs, as well as for information about how TSPs more generally handle their subscribers' personal information.[104] A deliberate effort was undertaken from 2013-2014 to encourage Canadian TSPs to begin releasing transparency reports. That effort involved writing public letters, working with parliamentarians to pressure the federal government of Canada to permit companies to release the reports, developing a right-to-information tool that enabled TSP subscribers to learn what information their TSP retained about them, and filing access to information requests.[105]

This section focuses on the kinds of information that are now publicly available concerning the regularity at which TSPs are asked to disclose information, the periods of time that they retain information, and the significance of TSPs' lack of publicly available law enforcement guidelines. From the information presented in this section, it will become apparent that, despite the extent of the government's legal capacity to request telecommunications data and the technical and standards-based ways to access the data, Canadians generally cannot evaluate or understand the extent of contemporary government telecommunications surveillance or the numbers of persons who are affected by such surveillance.

---

[104] Christopher Parsons. (2014). "Towards Transparency in Canadian Telecommunications" *The Citizen Lab*, January 22, 2014, retrieved March 23, 2015, https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/; Christopher Parsons. (2014). "The Murky State of Canadian Telecommunications Surveillance," *The Citizen Lab*, March 6, 2014, retrieved March 23, 2015, https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance/; Andrew Clement and Jonathan Obar. (2014). "Keeping Internet Users In The Know Or In The Dark: Data Privacy Transparency of Canadian Internet Service Providers," *IX Maps*, retrieved March 11, 2015, http://ixmaps.ca/transparency/img/DataPrivacyTransparencyofCanadianISPs-2013.pdf; Andrew Clement and Jonathan Obar. (2015). "Keeping Internet Users In The Know Or In The Dark: Data Privacy Transparency of Canadian Internet Service Providers: 2014 Report," *IX Maps*, retrieved March 11, 2015, http://ixmaps.ca/transparency-2014.php.

[105] Christopher Parsons. (Forthcoming). "Beyond the ATIP: New methods for interrogating state surveillance," Jamie Brownlee and Kevin Walby (Eds.), *Access to Information and Social Justice*. Arbeiter Ring Publishing.

Transparency Reporting

The efforts of Canadian academics and civil rights organizations to encourage TSPs to release transparency reports have been linked to resistance to proposed federal surveillance powers, such as those in the now-passed lawful access legislation. These critics learned about fragments of government surveillance practices over the course of a decade. TSPs have received so much attention because of their privileged roles in the lives of citizens who, generally, "have come to depend on them to safeguard our personal information and private communications and to prevent that information from falling into the hands of third parties. This [privilege] gives ISPs power and discretion: power to control our online behaviour and discretion to alter our outcomes."[106]

As of the end of 2014, six Canadian TSPs released 'transparency reports'. Two of Canada's largest providers, Rogers and TELUS, disclosed information about how often government requested and received access to subscriber data. One crown corporation, SaskTel, also released a report as did a smaller TSP, TekSavvy. Wind Mobile and MTS Allstream also released reports. All six companies committed to releasing annual reports and Rogers released their 2015 report in April 2015 and TELUS theirs in May 2015. Of the companies, only TELUS requested guidance on releasing transparency reports.[107]

Canadian TSPs receive several different kinds of lawful access requests. Table 1 collates information from the available transparency reports to showcase the extent to which requests are made and the kinds of categories associated with these requests.

[106] Ian Kerr and Daphne Gilbert. (2006). "The Role of ISPs in the Investigation of Cybercrime," in T. Mendina & J. J. Britz (Eds.), *Information Ethics in the Electronic Age: Current Issues in Africa and the World*. Jefferson, North Carolina: McFarland, pp. 164-5.

[107] Amber Hildebrandt. (2015). "Police asked telcos for client data in over 80% of criminal probes," *CBC News*, April 10, 2015, retrieved April 11, 2015, http://www.cbc.ca/news/technology/police-asked-telcos-for-client-data-in-over-80-of-criminal-probes-1.3025055.

	Rogers		TELUS		SaskTel	TekSavvy
Request Category	**Requests in 2013 (in 2014 report)**	**Requests in 2014 (in 2015 report)**	**Requests in 2013 (in 2014 report)**	**Requests in 2014 (in 2015 report)**	**Requests in 2013 (in 2014 report)**	**Requests in 2012 & 2013 (in 2014 report)**
Court Order/Warrant	74,415	71,501	3,922 (Court Order), 393 (Subpoena)	3,500 (Court Order), 453 (Subpoena)	4,139	1
Government Requirement Letter	2,556	2,315	1,343	1,247	233	—
Emergency Requests from Police	9,339	10,016	—	—	—	—
Foreign Requests Through MLAT	40	1	2	2	—	—
Customer Name/Address Checks	87,856	29,438	40,900	30,046	2478	52
Child Sexual Exploitation Assistance Requests	711	384	154	144	49	—
Emergency Responder Requests	55,900	50,439	56,748	61,596	4,711	—
Total Requests	230,817	164,094	103,462	97,938	11,610	53

Table 1: Collated Transparency Report Information

	MTS Allstream		Wind Mobile	
Request Category	**Requests in 2013 (in 2014 report)**	**Requests in 2014 (in 2015 report)**	**Requests in 2013 (in 2014 report)**	**Requests in 2014 (in 2015 report)**
Court Order/Warrant	9,200	Not reported yet	646*	2,989*
Government Requirement Letter	197	Not reported yet	646*	2,989*
Emergency Requests from Police	---	Not reported yet	---	---
Foreign Requests Through MLAT	---	Not reported yet	---	---
Customer Name/Address Checks	2,726	Not reported yet	6,445	3,845
Child Sexual Exploitation Assistance Requests	100	Not reported yet	---	---
Emergency Responder Requests	1,632	Not reported yet	5,965	7,822
Total Requests	13,855	Not reported yet	13,056	14,296

Table 2: Collated Transparency Report information for MTS Allstream and Wind Mobile

* Wind Mobile does not differentiate between court ordered and government requirement letter demands[108]

Court orders and warrants run the gamut from interception warrants to production

[108] In a prior version of this report (1.4) we mistakenly left out this table. We apologize for this error.

orders and number dialer recorder orders. Thus, while the 'Court Order/Warrant' category indicates the regularity at which TSPs are served with orders authorized by a judge, it does not reflect the different kinds of surveillance that might be entailed by different types of orders. In contrast, government requirement letters compel TSPs to disclose information according to statute; when relying on a statute, government authorities are not typically required to obtain court authorization before compelling TSPs to release information. Emergency requests from police involve authorities demanding information from TSPs in cases where, if the authorities had to first receive a judicial order, it would endanger the investigation or put individuals at severe risk. Foreign requests through Mutual Legal Assistant Treaties (MLAT) refers to situations where authorities in a foreign jurisdiction request information from a TSP through a formal government-to-government data request process. Customer Name/Address Checks are a contentious category because in addition to a person's name and where they live the requests may sometimes ask for more detailed subscriber billing information. Canadian TSPs as an industry have not clearly differentiated which Customer Name/Address Check request require basic or more detailed information to be returned to authorities. Rogers and TELUS have stopped fulfilling these requests without first receiving a court order or being satisfied that the information must be released in an emergency situation.

Child sexual exploitation assistance requests almost always involve a TSP providing a customer's name and address after receiving a warrantless request from law enforcement; such requests often ask a TSP to correlate an IP address with a TSP's billing information. Post-*Spencer*, many Canadian ISPs have stopped this practice save for in exigent circumstances. It should be noted that former telecommunications executives for Rogers[109] and Bell Canada[110] both assert that 'subscriber data' requests were always meant to be isolated to child exploitation investigations. However, the definition of such requests in Rogers' and TELUS' transparency reports seems at odds with their industry group's report that the TSP industry received were over 1.1 million requests for subscriber records in 2011

[109] Kenneth Engelhart. (2014). "Regulatory Blockbuster Panel," Canadian Telecommunications Summit. June 2, 2014.

[110] Suzanne Morin. (2015). "R v Spencer "lawful authority to obtain" (or not)," *LinkedIn*, April 15, 2015, retrieved April 17, 2015, https://www.linkedin.com/pulse/r-v-spencer-lawful-authority-obtain-suzanne-morin?trk=prof-post.

alone.[111]

Emergency responder requests refer to cases where emergency responders require information to either prevent or react to cases where a person's life may be in imminent danger.

There are discrepancies across the different data types, arguably because TSPs have not yet developed a common standard for reporting. Moreover, Canadian TSPs have thus far not adopted the standard reporting format used in American and other foreign jurisdictions. Specifically, TSPs in those other jurisdictions routinely include the type or category of request, the number of that kind of request, and the numbers of subscribers affected. Canadian TSPs tend not to break out requests in this format, either conjoining requests and subscribers (e.g. Rogers/TekSavvy) or indicating the number of requests but not the number of affected subscribers (e.g. SaskTel/TELUS).

Data Retention Practices

TSP transparency reports have contributed information about the regularity at which government authorities request data from these corporations. However, the number of times that data is requested does not reveal the extent of the data accessed; while one request could be for a single data record created yesterday, that request could also encompass all subscriber data records that were created over many years. Disclosing the number of requests, then, does not reveal the amount of data that is collected. To fully understand the extent of government data access requests, we need additional information about how long the TSPs retain personal information records.

We worked throughout 2014 and early 2015 to learn more about how long Canadian TSPs retain data. This research involved sending public letters to the TSPs that inquired about their data governance practices. Additionally, we developed and deployed a tool that let Canadians obtain basic information about their own TSP's data collection, use, retention, and disclosure practices. In their response to the public letters, TSPs generally declined to explain what kinds of data they

[111] Gowlings, for the Canadian Wireless Telecommunications Association. (2011). "Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members," Gowlings. December 11, 2011.

collected, processed, or retained. For example, the responses from Bell Aliant,[112] Bell Canada,[113] Cogeco,[114] Eastlink,[115] Rogers,[116] TELUS,[117] or Videotron[118] failed to comprehensively explain how long they collected their customers' personal information. Only TekSavvy provided a fulsome response to the letter issued to them.[119] Most responsive companies did, however, affirm their commitment to Canada's commercial privacy legislation, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[120]

Principle 4.9 of *PIPEDA* gives individuals the right to make requests of companies that retain their personal information. Individuals who make such requests "shall be informed of the existence, use, and disclosure of his or her personal information and be given access to that information"[121] upon making a request to a company

[112] Bell Aliant Privacy Office. (2014). "RE: Questions Concerning Disclosure of Telecommunications Information to Government Authorities," personal email, March 3, 2014, retrieved October 5, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Bell-Alliant.pdf.

[113] Bell Canada. (2014). "Inquiry concerning lawful access and other disclosures to government," March 3, 2014, retrieved October 14, 2015, https://citizenlab.org/wp-content/uploads/2014/03/Bell-Canada-Lawful-Access-Request- Letter.pdf.

[114] Cogeco Cable Inc. (2014). "Request for information - Cogeco Cable," March 3, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Cogeco-Cable-March-3-2014.pdf..

[115] Eastlink. (2014). "RE: Questions Concerning Disclosure of Telecommunications Information to Government Authorities," personal email, March 3, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Eastlink.pdf.

[116] Rogers Communications. (2014). Untitled, February 27, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Rogers.pdf.

[117] TELUS. (2014). "Re: Data Retention and Sharing Policies of TELUS," March 5, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/TELUS-Response-to-Parsons-et-al-Letter-20-Jan-2014.pdf.

[118] Videotron. (2014). "Demande d'informations," March 3, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/QuebecorVideotron.pdf.

[119] TekSavvy. (2014). "Re: January 20 Data Request (items 1-10); May 1 Personal Information Template," *TekSavvy*, June 4, 2014, retrieved June 4, 2014, www.teksavvy.com/Media/Default/Citizen Lab/TekSavvy to Citizenlab - 2014-06-04.pdf.

[120] Christopher Parsons. (2014). "The Murky State of Canadian Telecommunications Surveillance," *The Citizen Lab*, March 6, 2014, retrieved February 15, 2015, https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance/.

[121] Office of the Privacy Commissioner of Canada. (2013). "Interpretation Bulletin: Access to Personal Information," Government of Canada, last modified May 16, 2013, retrieved September 23, 2014, https://www.priv.gc.ca/leg_c/interpretations_05_access_e.asp.

with a substantial commercial connection to Canada.[122] Individuals can also mount a challenge if they believe that information provided is inaccurate or incomplete.[123] "[G]iven the relative opacity of companies' terms of service and accompanying privacy policies, these access and correction rights can also be used by individuals to learn more about a company's handling of personal information … [A]nd when groups of individuals collaborate and share the responses they receive from companies within the same industry type, such as telecommunications, the public collectively can render transparent the industry's data handling practices."[124]

We enabled this type of public collaboration by publishing a template for an access letter that was based on Principle 4.9 of PIPEDA and, subsequently, developing a web browser-based tool to let Canadians request their personal information from their TSPs. The template letter was accessible from the Citizen Lab's website and individuals could copy and paste it into a word processor, customize it, and then send it to their TSP.[125] The web tool, in contrast, was developed by Open Effect under its Digital Stewardship Initiative. It let individuals rapidly generate and send their requests either by printing it and delivering it by letter mail or sending the request directly to their TSP's privacy officer using email.[126] We then sought samples of responses from various TSPs around Canada to better understand TSPs' data collection, retention, processing, and disclosure policies. The following tables indicate the periods of time that different kinds of data are retained by some Canadian TSPs based on responses to Canadians' PIPEDA requests. We required access to at least three separate persons' primary documents in order to validate the responses that the telecommunications companies issued; as a result, a summary of all TSP responses that we have seen is not included in the following tables.

---

[122] Colin J. Bennett, Christopher Parsons, and Adam Molnar. (2014). "Real and Substantial Connections: Enforcing Canadian Privacy Laws Against American Social Networking Companies," *Journal of Law, Information & Science* 23(1).

[123] Office of the Privacy Commissioner of Canada. (2013). "Interpretation Bulletin: Access to Personal Information," Government of Canada, last modified May 16, 2013, retrieved September 23, 2014, https://www.priv.gc.ca/leg_c/interpretations_05_access_e.asp.

[124] Andrew Hilts and Christopher Parsons. (2014). "Enabling Citizens' Rights to Information in the 21st Century," *The Winston Report*, Fall 2014.

[125] Christopher Parsons. (2014). "Responding to the Crisis in Canadian Telecommunications," *Citizen Lab*, May 1, 2014, retrieved October 14, 2014, https://citizenlab.org/2014/05/responding-crisis-canadian-telecommunications/.

[126] Andrew Hilts and Christopher Parsons. (2014). "Enabling Citizens' Rights to Information in the 21st Century," *The Winston Report*, Fall 2014.

Data Type	Retention Period for Mobile/Wireless Service	
	Bell	**Rogers**
Call Records	Unknown	7 years
Voicemail	Unknown	Unknown
SMS Content / Metadata	Unknown / Unknown	0 / 13 Months
Device Internet Protocol (IP) Logs	Unknown	Unknown
Device Media Access Control (MAC) Address	Unknown	Unknown
Visited Website IP Logs/Uniform Resource Locators (URLs)	Unknown / Unknown	Unknown / Unknown
Geolocation: Global Positioning System	Unknown	0 Months
Geolocation: Wifi	Unknown	0 Months
Geolocation: Cell Tower Logs	Unknown	Unknown
Subscriber Records	Unknown	Unknown
Customer Service Records	Unknown	Unknown
Billing Records	Unknown	7 Years

Table 3: Comparative Mobile/Wireline Retention Periods

Data Type	Retention Period - Home Phone Service		
	Bell	**Rogers**	**TekSavvy**
Call Records	Unknown	7 Years	Indefinite (TekTalk and Home Phone)
Voicemail	Unknown	Unknown	14 Days (TekTalk) and Unknown (Home Phone)
Subscriber Records	Unknown	Unknown	Unknown (Intend to Store for 2 Years)
Customer Service Records	Unknown	Unknown	Unknown

Data Type	Retention Period - Home Phone Service		
	Bell	**Rogers**	**TekSavvy**
Billing Records	Unknown	Unknown	Unknown

Table 4: Comparative Home Phone Retention Periods

Data Type	Retention Period - Home Internet Service		
	Bell	**Rogers**	**TekSavvy**
Device Internet Protocol Logs	Unknown	Unknown	30 Days
Device Media Access Control (MAC) Address	Unknown	Unknown	30 Days
Visited Website Internet Protocol (IP) Logs/Uniform Resource Locators (URLs)	Unknown / Unknown	Unknown / Unknown (Must be at least 31 days)	0 / 0 Days
Subscriber Records	Unknown	Unknown	Unknown (Intend to Store for 2 Years)
Customer Service Records	Unknown	Unknown	Unknown
Billing Records	Unknown	Unknown	Unknown

Table 5: Comparative Home Internet Service Retention Periods

TSPs routinely provided ambiguous responses to the requests they received. One part of the requests asked for "[a]ll logs of IP addresses associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names or sites I visit and the times, dates, and port numbers." All TSPs must retain information about the IP addresses their subscribers visit, and that are assigned to their devices, for at least some period of time in order to provide Internet services. However, Fido states that it did not "collect" the IP addresses or domain names of websites visited,[127] and TekSavvy stated they did not "log" this information;[128] the latter company instead retains it for brief periods of time and subsequently disposes of it. Fido subsequently clarified that while the

[127] Fido response to a subscriber's *PIPEDA* request.
[128] TekSavvy response to a subscriber's *PIPEDA* request.

company does temporarily "collect" information for technical reasons, it does not "retain" associations between customer information and visited IP addresses.[129] The lack of clarity in the TSPs responses represents a non-standardized way of describing activities and has the effect of making comparisons between company responses more challenging when consumers compare multiple companies' responses.

In other situations, TSPs would provide only general statements in response to questions. When asked, NorthwesTel acknowledged that it retained IP addresses linked with a requestor's device, but the TSP failed to state for how long this association was maintained.[130] In a related vein, responses from Shaw simply did not address whether it kept records of the visited sites or about the full ranges of information the TSP stores; it only provided the requestor's current IP address.[131]

In many cases, TSPs asserted that subscribers would have to pay significant costs before the TSPs would respond to requests:

> Fido invited the subscriber to inquire about costs, as did Rogers. In both cases fees for providing text message metadata and call logs ran as high as five thousand dollars. Similarly, a subscriber of Koodo reported that the company would levy a twelve hundred dollar free to provide historical IP address logs associated with her mobile device, a fee that was nearly double what the subscriber had paid as a customer of the company.[132]

Other TSPs simply declined to meaningfully respond to subscribers' requests at all. "Bell Canada failed to address the request for historical IP address records and consequently also failed to disclose information about its retention schedules for these records. Furthermore, Bell did not mention its capacity or willingness to provide this information for a fee."[133]

The *PIPEDA* requests followed a common structure, which we hoped would help us identify when companies failed to address one or more of the specific questions

[129] Fido clarifying response concerning a subscriber's *PIPEDA* request.
[130] NorthwesTel response to a subscriber's *PIPEDA* request.
[131] Shaw response to a subscriber's *PIPEDA* request.
[132] Andrew Hilts and Christopher Parsons. (2014). "Enabling Citizens' Rights to Information in the 21st Century," *The Winston Report*, Fall 2014.
[133] Andrew Hilts and Christopher Parsons. (2014). "Enabling Citizens' Rights to Information in the 21st Century," *The Winston Report*, Fall 2014.

that they were asked. Several companies provided item-by-item responses to the requests but still failed to comprehensively explain data collection or retention policies or periods. The result is that while this method did expand the amount of information concerning TSP data retention and handling practices, the available data is partial at best.

Law Enforcement Guideline Handbooks

Government agencies turn to TSPs when conducting investigations and access telecommunications data in the course of up to 80% of their investigations.[134] Canadian companies already have processes and policies to respond to state agencies' requests for assistance or stored data. Bell Canada's lawful access group vets all such requests,[135] TELUS and Rogers both challenge overly broad requests,[136] SaskTel has a dedicated unit to handle data requests from government agencies,[137] and TekSavvy carefully evaluates all requests that they receive.[138] Moreover, companies such as Bell Canada led the way in standardizing the regime which let law enforcement make requests for subscriber data without warrant.[139] As of May 2015, however, no Canadian TSP has publicly released their internal policies or the guidelines that Canadian authorities must comply with before a

[134] Amber Hildebrandt. (2015). "Police asked telcos for client data in over 80% of criminal probes," *CBC News*, April 10, 2015, retrieved April 11, 2015, http://www.cbc.ca/news/technology/police-asked-telcos-for-client-data-in-over-80-of-criminal-probes-1.3025055.

[135] Bell Canada. (2014). "Inquiry concerning lawful access and other disclosures to government," March 3, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Bell-Canada-Lawful-Access-Request-Letter.pdf.

[136] TELUS. (2014). "Re: Data Retention and Sharing Policies of TELUS," March 5, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/TELUS-Response-to-Parsons-et-al-Letter-20-Jan-2014.pdf; Rogers Communications. (2014). Untitled, February 27, 2014, retrieved October 14, 2014, https://citizenlab.org/wp-content/uploads/2014/03/Response-from-Rogers.pdf. See also: Rogers Communications. (2015). "2014 Rogers Transparency Report," *Rogers Communications*, Retrieved April 2, 2015, http://www.rogers.com/cms/pdf/en/2014-Rogers-Transparency-Report.pdf; TELUS. (2015). "2014 TELUS Sustainability Report," *TELUS*, retrieved May 12, 2015, http://sustainability.telus.com/content/pdf/2014_Sustainability_Report_EN.pdf.

[137] SaskTel. (2014). "2013 Transparency Report," *SaskTel*, retrieved March 3, 2015, https://www.sasktel.com/wps/wcm/connect/019634af-8378-432a-b6bf-3c47fe2e8d55/Transparency+Report_NR_Sep14.pdf?MOD=AJPERES.

[138] TekSavvy. (2014). "Re: January 20 Data Request (items 1-10); May 1 Personal Information Template," *TekSavvy*, June 4, 2014, retrieved June 4, 2014, www.teksavvy.com/Media/Default/Citizen Lab/TekSavvy to Citizenlab - 2014-06-04.pdf.

[139] Suzanne Morin. (2015). "R v Spencer "lawful authority to obtain" (or not)," *LinkedIn*, April 15, 2015, retrieved April 17, 2015, https://www.linkedin.com/pulse/r-v-spencer-lawful-authority-obtain-suzanne-morin?trk=prof-post.

given TSP will disclose its subscribers' information.

Law enforcement guideline handbooks "include the detailed procedures government agencies must follow to request corporate-held data, the kinds of identification government agencies must present before information will be disclosed, the time it takes for corporations to process requests, and the costs agencies must pay for the requests to be processed."[140] When these handbooks are public, less confusion exists amongst government agencies about what kinds of data the company stores, for how long, and under what terms it can be (and is) released. Moreover, subscribers can better understand exactly how a TSP handles their personal information — in excess of generic privacy policy and terms of service assurances that a TSP only discloses subscriber information in compliance with the law — when presented with different kinds of court orders.

Law enforcement guideline handbooks that foreign companies have released routinely provide detailed information about what authorities must do to receive information from the company in question. The handbooks often begin by outlining how a government authority can serve a data request on a TSP and how different kinds of requests (e.g. emergency versus subpoena) must be served to the company. For each kind of request there are explanations of what legal bars, if any, must be met and the kinds of information a government official must provide to prove their employment with a government agency.

Foreign companies' law enforcement guideline handbooks also outline the kinds of data that each type of legal request can elicit from the company and specify the kinds of data the government authority must first provide so the company can find the customer's information in their databases (e.g. a subscriber's email address, IP address, phone number, credit card number, etc.). Handbooks may also explain how the company must process foreign authorities' requests for company-held data, identify whether customers are notified of either domestic or foreign authorities' requests, outline the period of time the company can take to respond to requests, and state whether costs incurred in fulfilling the government request must be compensated or not.

Canadian TSPs have not released their law enforcement guideline handbooks

[140] Christopher Parsons. (2015). "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," *Social Sciences Research Network*, last revised January 14, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

though some have provided information concerning the costs of some interception and disclosure activities; comparable information is often included in foreign companies' handbooks. While SaskTel asserts that it "does not receive compensation for providing information to government agencies," it does "recover the cost" of performing some lawful interception services.[141] Their CRTC-approved tariff rates are divided between information lookups and interceptions of private communications. 'Non-confidential' lookups contain information that is "published in the Company's directories or listed in the Company's Directory Assistance records"[142] whereas 'confidential lookups' include information consisting of "names, addresses and telephone numbers of customer whose listings are not published in directories or listed in SaskTel's Directory Assistance records."[143] Requests for confidential information are billed at a rate of $50/hour (minimum ½ hour and billed in 15-minute increments) in excess of the customer-name and address (CNA) information charges denoted in Table Five. This charge applies when SaskTel retrieves customer record information, call details, or copies of customer bills for the requesting agency.[144] Past tariffs filed by Bell Canada in 2002[145] and TELUS in 2006[146] also showed costs of processing CNA information requests, as noted in the

[141] SaskTel. (2014). "Requests for customer information. (Transparency Report 2013)," *SaskTel*, retrieved April 10, 2015, https://www.sasktel.com/wps/wcm/connect/019634af-8378-432a-b6bf-3c47fe2e8d55/Transparency+Report_NR_Sep14.pdf?MOD=AJPERES.

[142] SaskTel. (2010). "General Tariff — Basic Services: Customer Information Requests and Wiretap Services," *SaskTel*, March 19, 2010, retrieved April 10, 2015, http://www.sasktel.com/wps/wcm/connect/afd85294-2b3c-476c-a9fd-75869c23537a/110-16.pdf?MOD=AJPERES.

[143] SaskTel. (2010). "General Tariff — Basic Services: Customer Information Requests and Wiretap Services," *SaskTel*, March 19, 2010, retrieved April 10, 2015, http://www.sasktel.com/wps/wcm/connect/afd85294-2b3c-476c-a9fd-75869c23537a/110-16.pdf?MOD=AJPERES.

[144] SaskTel. (2010). "General Tariff — Basic Services: Customer Information Requests and Wiretap Services," *SaskTel*, March 19, 2010, retrieved April 10, 2015, http://www.sasktel.com/wps/wcm/connect/afd85294-2b3c-476c-a9fd-75869c23537a/110-16.pdf?MOD=AJPERES.

[145] Bell Canada. (2002). "General Tariff — Miscellaneous Services, Item 2175. Customer Name and Address," *Bell Canada*, September 10, 2002, retrieved March 20, 2015, http://www.bce.ca/assets/Tariffs/bellcanada/GT/2/2175.pdf; Bell Canada. (2002). "General Tariff — Miscellaneous Services, Item 2177. Service Provider Identification Service," *Bell Canada*, March 17, 2002, retrieved March 20, 2015, http://www.bce.ca/assets/Tariffs/bellcanada/GT/2/2177.pdf.

[146] TELUS. (2006). "General Tariff — Features and Optional Services: Law Enforcement Agencies (LEA) Services," *TELUS*, March 12, 2006, retrieved March 20, 2015, http://about.telus.com/servlet/JiveServlet/previewBody/2607-102-1-2606/item313.pdf.

following table.[147]

LEA Service	Bell Canada	TELUS	SaskTel (Non-Confidential)	SaskTel (Confidential)
CNA Request by Telephone Number				
- Verbal	$9.65	$9.85	$3.00	$3.00
- Facsimile	$2.80	$6.45		
- Electronic file transfer	$1.20	$1.50		
Request by Address	$15.40	$13.50	$10.00*	$10.00*
Name/Address Lookup				
Service Provider Identification Service Request by Telephone Number				
- Each number found	$1.50	$2.95	—	—

Table 6: Comparative TSP Lawful Interception Fees

* SaskTel charges this rate when responding to requests based on an address *or* when responding to requests based on a person's name

SaskTel's general tariff filings show that the company is authorized to recover the costs of performing communications interceptions. There is a one-time service charge for the first connection, which can range from $200 for major cities to $400 for a remote location plus $250 for each additional connection made during the

[147] An RCMP ATIP (A-2014-02766) further indicates Rogers', Bell's, TELUS', SaskTel's, Wind's, and other carriers' law enforcement authority service charges. However, given the lack of specificity or context (e.g. p. 720 of the ATIP) we have opted to not try and integrate these charges into Table 5. See also: ha
Ling. (2015). "The RCMP Spent $1.6 Million to Run an Unconstitutional Spying Program," *Vice News*, January 20, 2015, retrieved March 25, 2015, http://www.vice.com/en_ca/read/the-rcmp-spent-16-million-to-run-an-unconstitutional-spying-program-239.

same field visit to the remote location. Cellular wiretap rates are much higher; there is a one-time charge of $850 plus a connection charge of $200 for each month that the wiretap is active. There is also a $100/number search tariff where authorities request SaskTel to conduct specific, or verbatim, searches of toll events.[148]

Considerable variation exists in the compensation or reimbursement schedules used by Canadian TSPs. In the transparency report it released in 2014, TekSavvy stated that it has not received compensation for disclosing subscriber and subscriber-related data to government authorities;[149] only TekSavvy's and SaskTel's transparency reports clearly state the compensation the companies have or can receive: all other companies' transparency reports only provide general information. Rogers notes that it assumes all costs for court-ordered demands for subscriber information though for some cases the company charges "a minimal fee to recover our costs based on the work required".[150] TELUS is similarly ambiguous in the transparency report it published in 2014, explaining that the company "bears most of the cost of complying with the types of requests."[151]

When responding to the Privacy Commissioner of Canada, through the Canadian Wireless Telecommunications Association (CWTA), Canadian TSPs were more forthcoming than in their transparency reports. Eight of the nine responsive companies stated that they did seek reimbursement for complying with some requests made by authorities. Some companies required compensation for customer name information and lawful interceptions, others requested reimbursement only for lawful intercepts, and still other companies wanted compensation only when costs were significant. Companies also differed on how public their tariff rates were; three stated only that they had tariffs and complied with them pursuant to CRTC policies, two did not make the tariffs available to the

[148] SaskTel. (2010). "General Tariff — Basic Services: Customer Information Requests and Wiretap Services," *SaskTel*, March 19, 2010, retrieved April 10, 2015, http://www.sasktel.com/wps/wcm/connect/afd85294-2b3c-476c-a9fd-75869c23537a/110-16.pdf?MOD=AJPERES.

[149] TekSavvy. (2014). "Re: January 20 Data Request (items 1-10); May 1 Personal Information Template," *TekSavvy*, June 4, 2014, retrieved June 4, 2014, www.teksavvy.com/Media/Default/Citizen Lab/TekSavvy to Citizenlab - 2014-06-04.pdf.

[150] Rogers Communications. (2015). "2014 Rogers Transparency Report," *Rogers Communications*, Retrieved April 2, 2015, http://www.rogers.com/cms/pdf/en/2014-Rogers-Transparency-Report.pdf.

[151] TELUS. (2014). "TELUS Transparency Report 2013," *TELUS*, retrieved April 2, 2015, http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf.

general public, and one only made its schedule of tariffs available to "Enforcement and Government Agencies."[152]

Ultimately, the cost of providing interceptions composes just one of many parts of an effective law enforcement guideline handbook. And despite many Canadian TSPs having divisions that receive and respond to requests from law enforcement and receiving requests often enough that they can see compensation for the requests, few have made these policy documents available to the public. Without these handbooks, in tandem with transparency reports and data retention schedules, politicians, citizens, and policy analysts cannot genuinely understand the body of law and the accompanying policies that govern access to the data that TSPs collect, process, and retain.

TSPs and Signals Intelligence Surveillance

News organizations around the world have been publishing stories about how signals intelligence agencies, including the Communications Security Establishment (CSE), have been involved in collecting information from the Internet in bulk for extensive analysis and long-term data retention. CSE accesses at least some data collected by its closest intelligence allies and has also deployed its own sensor systems around the world to collect information for its own databases.

As of 2011, CSE had two core classes of sensors. It operated the PHOTONIC PRISM sensor system to monitor government of Canada systems[153] and the EONBLUE system. The latter is used to collect 'full-take' data, as well as to conduct signature- and anomaly-based detections on the networks in which it was deployed.[154] Within Canada, PHOTONIC PRISM systems were deployed in selected government networks and other sensors with EONBLUE capabilities were deployed in

[152] Gowlings, for the Canadian Wireless Telecommunications Association. (2011). "Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members," Gowlings. December 11, 2011.

[153] Communications Security Establishment. (2010). "Cyber Network Defence R&D Activities," Government of Canada, retrieved March 29, 2015, https://www.christopher-parsons.com/writings/cse-summaries/.

[154] Communications Security Establishment. (2011). "CASCADE: Joint Cyber Sensor Architecture," Government of Canada, retrieved March 24, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/cascade-2011-2.pdf; Communications Security Establishment. (2009). "Cyber Threat Detection," Government of Canada, retrieved March 29, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-5-cyber-csec-sdf-gchq-nov2009.pdf.

commercial networks. For example, the CSE deployed the CRUCIBLE system, which has similar capabilities as EONBLUE, domestically at gateways between domestic and international network domains.[155] Other sensors that were deployed domestically include a metadata production and processing program, THIRD-EYE, which operated at selected new sites and an unclassified sensor which was designed to track targets and be deployed in non-highly secured locations (i.e. not in Sensitive Compartmentalized Information Facilities).[156] As of 2011, CSE had 100% EONBLUE coverage of all traffic on international Internet links between Canada and the rest of the world.[157]

Canadian TSPs are likely challenged in their knowledge of, and ability to disclose, CSE's operation within or alongside their networks. In the United States and United Kingdom, companies have tried to avoid acknowledging the presence of signals intelligence equipment in their networks even when the existence of such equipment has been made public. Companies may be limited in their ability to disclose that they *do* have such equipment in their networks but, in their transparency reports, they could clearly state that CSE equipment is *not* in their networks and could go so far as to state that *no* government equipment exists in their networks. Alternately, a given TSP could include a disclaimer in their law enforcement guidance handbook about how the company responds to requests to insert government-owned or –purchased surveillance equipment in its networks, indicating how the TSP deal with this often secretive aspect of government surveillance.

The absence of such a statement could not be taken as evidence or proof that a company's network had equipment from the signals intelligence agency in it, but statements denying the presence of the equipment would further expand Canadians' understanding of how their personal information is handled and who

[155] Communications Security Establishment. (2011). "CASCADE: Joint Cyber Sensor Architecture," Government of Canada, retrieved March 24, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/cascade-2011-2.pdf.
[156] Communications Security Establishment. (2011). "CASCADE: Joint Cyber Sensor Architecture," Government of Canada, Retrieved March 24, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/cascade-2011-2.pdf.
[157] Communications Security Establishment. (2011). "CASCADE: Joint Cyber Sensor Architecture," Government of Canada, retrieved March 24, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/cascade-2011-2.pdf.

(and how) TSPs make it available to government authorities.[158]

Summary

The limits of current transparency reporting, most TSP's failure to clearly and comprehensively outline their data retention schedule to subscribers, and the current failure to release law enforcement guidance handbooks are all practices that companies can improve upon. They can develop and release more meaningful transparency reports. They can perform internal audits of their data management practices and publicize the results of those audits. And they can publish their law enforcement handbooks and polices on their websites or with their transparency reports. Ascertaining how to explain or describe their existing or potential relationships with Canada's signals intelligence agency could be more challenging, but this work could be accomplished by adding small modifications to transparency reports or disclosures in government access handbooks.

Corporate disclosures will, first and foremost, render transparent the extent of government surveillance of telecommunications subscribers and their communications. But such disclosures will not, on their own, force agencies to be more accountable to Canadians, nor will they ensure that agencies are acting within the scope of their mandates or the law. Government oversight of government agencies, however, has the potential to limit improper surveillance requests and to ensure that Canadian TSPs are not inappropriately asked to disclose subscribers' information and, where such request are inappropriate, subsequently correct procedures and ensure that similar actions are not repeated. However, as discussed in Section Four, there are severe limitations concerning contemporary governmental review and oversight of telecommunications surveillance; the result is that Canada's intelligence and security agencies' surveillance activities are minimally monitored by independent branches of government.

[158] In some respect, this proposal parallels 'warrant canary' warnings that some American TSPs use to indicate whether they have been forced to disclose their subscribers' information after receiving a national security letter. For more, see: Naomi Gilens, "The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures," *Social Science Review Network*, last revised April 2014, retrieved November 14, 2014, http://ssrn.com/abstract=2498150.

Section Four: Limits of Government Oversight and Review

Corporate transparency reports, no matter how useful or informative, are not a replacement for strong government oversight. While corporations have considerable insight into the regularity at which, and rationales for, government access to telecommunications data, they cannot oversee the ways that government agencies actually use the data they access. Nor can corporations conduct investigations of government practices; all corporations can do (at best) is challenge perceived overreaches.

This section examines the limitations concerning the oversight and review of federal institutions' telecommunications-related surveillance practices. As a point of clarity, whereas review describes after the fact analysis, oversight entails supervision that may include ongoing activities.[159] The section begins by critiquing the interception reports that the federal and provincial governments of Canada must table by law. Next, it discusses the roles and limitations of key independent oversight, review, or complaints bodies, namely the Security Intelligence Review Committee (SIRC), Office of the Privacy Commissioner of Canada (OPC), and the Office of the Communications Security Establishment Commissioner (OCSEC). Ultimately, regardless of the positive intentions of the persons working within these institutions, their intentions are diminished either by their institutions' mandates or lack of resources or lack of order-making powers.

Interception Reports

Canadian governments must produce annual reports that detail the regularity at which they intercept Canadians' telecommunications. This reporting requires that authorities disclose the number of individuals affected by the interceptions, average duration of the surveillance, type of crimes investigated, number of cases brought to court, and the number of individuals notified that the surveillance had taken place.[160] Comparisons of interception reports from 1975 and 2010 reveal that the number of requests made by federal authorities for surveillance have decreased from almost 1,200 in 1975 to under 200 in 2010, though there has been

[159] M. Caparini, in Peter Gill (2002). "Democratic and Parliamentary Accountability of Intelligence Services After September 11th," Workshop on Democratic and Parliamentary Oversight of Intelligence Services, Geneva, October 3-5, 2002.
[160] *Criminal Code*, 1985, s.195.

a 50% increase in the number of persons notified; whereas in 1977 roughly 800 people were notified compared to roughly 1,200 in 2010.[161] Thus, though fewer interceptions warrants are issued to authorities now, they encompass roughly 50% more people per warrant than in the 1970s. Ultimately, the federal reports only tell a partial story: they fail to account for provincial interceptions, fail to encompass more commonly used telecommunications surveillance practices, and do not include government agencies' requests for 'subscriber' or 'customer name/address' information.

An Access to Information and Privacy (ATIP) request that was filed by a journalist revealed, that overall, TSPs in Canada received at least 6,000 interception orders that applied to wireline, wireless, and Internet communications in 2011.[162] The bulk of these requests were made by provincial and municipal agencies, not agencies associated with the federal government of Canada. For example, the Vancouver Police Department averaged 54 interceptions per year between 2011 and 2013[163] and Halifax Regional Police approximately 20 per year over the same period of time.[164] Larger policing bodies, including Toronto Police, failed to comply with access to information laws and did not provide information we requested from them in a timely fashion. Though all provincial governments are required to table equivalent reports to the federal government's interception report, provinces are largely reticent to make the reports public. The result is that researchers, including us, have been stymied in conducting cross-national comparisons of the interceptions conducted by federal *and* provincial agencies. Regardless of which government institution makes an interception request, the individuals affected are ultimately notified that a specific government agency had monitored their communication(s) .

While the federal interception reports provide considerable detail about specific modes of surveillance, the kinds of telecommunications surveillance that are used

[161] Nicholas Koutros and Julien Demers. (2013). "In Big Brother's Shadow: Historical Decline of Electronic surveillance by Canadian Federal Law Enforcement," *Social Sciences Research Network*, last revised March 15, 2013, retrieved December 2, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220740.

[162] Matthew Braga. (2014). "New Documents Show Thousands of Unreported Wiretaps by Canadian Cops," *Motherboard*, November 20, 14, retrieved November 26, 2014, http://motherboard.vice.com/en_ca/read/new-documents-show-thousands-of-unreported-wiretaps-by-canadian-cops.

[163] Records Request to Vancouver Police Department, completed December 30, 2014.

[164] FOIPOP # 14-187 provided by Halifax Regional Police, completed January 23, 2015.

most often by government agencies do not have to be statutorily recorded or reported to legislative assemblies, nor are those subjected to these kinds of surveillance typically notified. One such type of unreported surveillance includes number dialer warrants, which are issued on the standard of "reasonable grounds to suspect that an offence under this or any other Act of Parliament has been or will be committed."[165] These recorders log the numbers dialed from, and dialed to, a targeted phone number or device. No government agency is required to record the number of times it files for, or receives, a number dialer warrant, nor is it required to record the number of persons who the surveillance affects; individuals are unlikely to learn of the surveillance unless it is included as evidence during trial.

An ATIP document that was re-released in 2014 revealed that Canadian TSPs had received approximately 12,000 number dialer warrants in 2011.[166] ATIPs issued to police agencies across the country could not substantiate that approximation for one of two reasons: either the agencies failed to respond to the ATIPs or they noted that they did not track these kinds of requests. When asked to provide information about number dialer warrants, Halifax Regional Police stated that it "does not record or track the number of times individual investigators obtain production orders as part of their investigations" but that "it is not uncommon for investigators to require CDR information to be seized as evidence related to specific investigations."[167] The Vancouver Police Department (VPD), in contrast, asserted that, "[t]his information was not tracked by the VPD in the years of the request. We simply do not have this information to provide. The VPD will be centralizing the service of all Production Orders to the Covert Interception Unit to permit tracking beginning January 2015."[168] When a member of parliament asked the RCMP to provide this information, the agency replied that it,

> does not maintain a centralized data repository that would allow it to determine the total number of requests to telecommunications service providers for customers' usage of communications devices and

[165] *Criminal Code*, 1985, s.492(1).
[166] Matthew Braga. (2014). "New Documents Show Thousands of Unreported Wiretaps by Canadian Cops," *Motherboard*, November 20, 14, retrieved November 26, 2014, http://motherboard.vice.com/en_ca/read/new-documents-show-thousands-of-unreported-wiretaps-by-canadian-cops.
[167] FOIPOP # 14-187 provided by Halifax Regional Police, completed January 23, 2015.
[168] Records Request to Vancouver Police Department, completed December 30, 2014.

services.[169]

Between 2001 and 2015, following the passage of the lawful access legislation mentioned in Section One, a number of contentious debates focused on the ease at which government agencies accessed 'subscriber data'. Such data was defined differently across successive pieces of legislation and consultations and, in aggregate, included the following types of data: name, address, telephone number, subscriber's email address, as well as Internet protocol number, mobile identification numbers, electronic serial numbers, local service provider identifiers, international mobile equipment identity numbers, and subscriber identity module cards associated with accounts.[170] Some versions of the lawful access legislation would have compelled TSPs to provide this information, without warrant, upon the request of a government agent. Other versions included a reporting feature that required federal and provincial agencies to record and disclose the regularity at which they requested this information from TSPs.[171] In addition to comprehensive disclosers of subscriber records, government agencies have also requested 'tombstone data' when they issued Customer Name and Address (CNA) requests.

Authorities routinely requested, and received, subscriber and CNA information from Canadian TSPs. The RCMP made at least 28,143 requests for these types of records in 2010.[172] According to the Canadian Wireless Telecommunications Association's (CWTA) data, at least 1,193,630 requests, which affected at least 784,756 accounts, were made to their members in 2011.[173] The CWTA information came to public light only after the OPC released the information to curious

[169] Minister of Public Safety and Emergency Preparedness's Responses to MP Charmane Borg's Q-233 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher-parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf.

[170] Christopher Parsons. (2011). "The Anatomy of Lawful Access Phone Records," *Technology, Thoughts, and Trinkets*, November 21, 2011, retrieved December 2, 2014. https://www.christopher-parsons.com/the-anatomy-of-lawful-access-phone-records.

[171] Philippa Lawson. (2012). Moving Towards a Surveillance Society: Proposals to Expand "Lawful Access" in Canada. Vancouver, BCCLA, pp. 33.

[172] Christopher Parsons. (2012). "Canadian Social Media Surveillance: Today and Tomorrow," *Technology, Thoughts, and Trinkets*, May 12, 2012, retrieved November 26, 2014, https://www.christopher- parsons.com/canadian-social-media-surveillance-today-and-tomorrow/. The RCMP's data is incomplete and did not include information on how provincial deployments of the policing agency requested subscriber records.

[173] Gowlings, for the Canadian Wireless Telecommunications Association. (2011). "Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members," Gowlings. December 11, 2011.

journalists - just as it was about to be released to an academic who had filed an ATIP for the information.

Significantly, the RCMP maintains that, despite releasing ATIPs containing information about their collection of subscriber records and requirements to provide interception information as part of complying with s.195 of the *Criminal Code*, they have no records concerning:

> [B]usiness notes, memos, or policy docs showing the number of times that a) 'subscriber data' was requested from Canadian telecommunications service providers; b) wiretaps initiated under court order; c) Call Detail Records were obtained from January 1, 11-Nov 1, 14.[174]

Of note, the RCMP maintains records of the costs for gaining access to subscriber records, conducting wiretaps or interceptions, and compelling TSPs to operate number dialer programs.[175] These records were not only 'missed' when the RCMP replied to our ATIP, but they were not provided to the OPC when it conducted an investigation into the RCMP's accessing of TSP subscribers' records.[176]

Following the Supreme Court of Canada's ruling on *Spencer*, which established restrictions on warrantless access to subscriber records and CNA information, public agencies now must serve a court order on companies or rely on statutory powers to collect this information in non-emergency circumstances. Current and past telecommunications executives have previously asserted that they understood these warrantless requests had purely pertained to child abuse investigations.[177]

---

[174] See Access to Information and Privacy document released by the Royal Canadian Mounted Police, A-2014-08371.

[175] See Access to Information and Privacy document released by the Royal Canadian Mounted Police, hosted at https://www.scribd.com/doc/253197072/RCMP-Access-to-Information-Request.

[176] Office of the Privacy Commissioner of Canada. (2014). "2013-2014 *Privacy Act* Annual Report to Parliament: Transparency and Privacy in the Digital Age," Government of Canada October 2014, retrieved January 17, 2015, https://www.priv.gc.ca/information/ar/201314/201314_pa_e.asp#heading-0-0-4.

[177] Kenneth Engelhart. (2014). "Regulatory Blockbuster Panel," Canadian Telecommunications Summit. June 2, 2014; Suzanne Morin. (2015). "R v Spencer "lawful authority to obtain" (or not)," *LinkedIn*, April 15, 2015, retrieved April 17, 2015, https://www.linkedin.com/pulse/r-v-spencer-lawful-authority-obtain-suzanne-morin?trk=prof-post.

Despite the ongoing, extensive, attention given to telecommunications surveillance practices that are or are believed to be conducted by Canadian security, policing, and intelligence agencies, no new kinds of surveillance must be reported yearly. No new statutes have been passed that would expand the types of information contained in the interception reports so they account for contemporary means of monitoring or intercepting communications and communications traffic. While the current interception reports provide granular information about federal interceptions, they do not account for what is a numerically larger amount of surveillance practices, such as requests for subscriber data, production orders, and number dialer orders. Moreover, the failure of all Canadian provincial governments to make their interception reports available online limits researchers and policy analysts from ascertaining the extent of even interception-based surveillance in Canada. Together, the failure to update the reports to account for contemporary surveillance practices and the failure of all governments to make their (limited) interception reports available mean that the reports are severely limited in their ability to communicate to the public, parliamentarians, and policy analysts of the annual amount of government-conducted surveillance.

Security Intelligence Review Committee and the CSIS Inspector General

The Security Intelligence Review Committee (SIRC) was created to provide external review of CSIS and was complemented by the Inspector General of CSIS. This latter body was to review the operational policies and activities of CSIS and certify its satisfaction with the annual reports that CSIS submitted to its minister.[178] The Inspector General functioned as an "internal auditor to review the operations of the Service and to monitor compliance with ministerial directives and statue[s]"[179] to the effect of enabling "the Minister to be kept reliably informed, so that he can effectively control the CSIS and, being accountable for the Service, also discharge his responsibilities to parliament."[180] SIRC sometimes tasked the Inspector General

[178] Laurence Lustgarten and Ian Leigh. (1994). *In From The Cold: National Security and Parliamentary Democracy*. Oxford: Clarendon Press.
[179] Martin Rudner. (2002). "Contemporary Threats, Future Tasks: Canadian Intelligence and the Challenges of Global Security," in Norman Hillmer and Maureen Appel Molot (Eds.). *Canada Among Nations 2002: A Fading Power*. Toronto: Oxford University Press.
[180] Joseph F. Ryan. (1989). "The Inspector General of the Canadian Security Intelligence Service," *Conflict Quarterly*, Spring (1989), p. 43.

to carry out reviews.[181] Most importantly, the Inspector General operated as a kind of early warning system; it was to "get in there and identify the problems and point them out to the minister and say 'You have to fix this before it becomes an issue for the public.'" [182] In contrast, the SIRC functions predominantly as a public place for people to complain about CSIS's activities and to publicize problems. Despite the valuable contributions of the Inspector General it was dismantled in 2012 as part of a federal budget implementation bill.[183]

SIRC is composed of a three- to five-person committee along with a support staff. In addition to reviewing CSIS's actions, SIRC acts as a complaints tribunal that considers citizens' complaints about CSIS's activities and all complaints concerning federal security clearance matters. SIRC's committee members' part-time status is intentional; while long-term insiders of the intelligence community might have greater insight into the CSIS's activities, parliament worried that full-time committee members were more likely to be co-opted by the intelligence community.[184] Moreover, at SIRC's inception, the government worried that it would be unable to pay full-time salaries for qualified members and, further, that "a part-time review committee, albeit with full-time staff, might also be seen as less of an imposition by CSIS itself".[185] Historically, SIRC has used its influence strategically and, some have argued, effectively: it developed techniques that compelled CSIS to reveal information about its activities in excess of information that SIRC itself had access to and also led CSIS to dissolve its Counter-Subversion Branch, integrating that Branch's members into other CSIS Branches.[186] Its early effectiveness waned, however, as its committee members become less 'activist' in nature over the course

[181] Peter Gill. (1989). "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984-88," *Intelligence and National Security* 4:3.
[182] The Canadian Press. (2012). "Axing CSIS watchdog 'huge loss" says former inspector general," *CBC News*, August 10, 2012, retrieved March 13, 2015, http://www.cbc.ca/news/politics/axing-csis-watchdog-huge-loss-says-former-inspector-general-1.1143212.
[183] Government of Canada. (2012). "Bill C-38: An Act to implement certain provisions of the budget tabled in Parliament on March 29, 2012 and other measures," Assented to June 29, 2012.
[184] Peter Gill. (1989). "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984-88," *Intelligence and National Security* 4:3, p. 558.
[185] Peter Gill. (1989). "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984-88," *Intelligence and National Security* 4:3, p. 558.
[186] Peter Gill. (1989). "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984-88," *Intelligence and National Security* 4:3, pp. 558; Laurence Lustgarten and Ian Leigh. (1994). *In From The Cold: National Security and Parliamentary Democracy*. Oxford: Clarendon Press.

of the 1990s.[187]

SIRC has been challenged to provide effective oversight of CSIS for a variety of reasons. First, there have been numerous issues with members of its committee over the past several years; it has had four different chairs and seen two committee members retire before the end of their regular terms between April 2011 and March 2014.[188] These organizational disruptions have affected the availability of committee members to conduct work and have led SIRC to reassign "workload to remaining Members who worked to will in the gaps" and increase "scheduling flexibility for its meetings in order to ensure quorum."[189] Second, CSIS has delayed providing information or has provided incomplete information to SIRC, which has negatively affected the timeliness of reviews; as a result, SIRC has recently been forced to increase the "frequency and formality" of its communications with CSIS and invoke its authority to produce special reports to the Minister of Public Safety.[190] These special reports are "prompted by high-profile events or serious concerns which the Committee believes warrant attention."[191] Third, SIRC is limited in its ability to identify how CSIS-gathered information might be used after it is shared outside of CSIS; a previous SIRC chair, Chuck Stahl, stated in 2013 that,

> the trail is not going to stop nicely and neatly at CSIS's door … Other agencies … are working closely with CSIS, and increasingly we're going to need some way of chasing those threads. Otherwise, we'll have to tell parliamentarians that, as far as we can tell, everything looks great in CSIS country, but we don't know what happened over that fence; you're on

[187] Peter Gill and Mark Phythian. (2012). *Intelligence In An Insecure World*. Malden, MA: Polity Press. P. 185.
[188] Security Intelligence Review Committee. (2014). "2013-14 Department Performance Report," Government of Canada, October 24, 2014, retrieved October 30, 2014, http://www.sirc-csars.gc.ca/opbapb/dprrmr/2013-2014/index-eng.html.
[189] Security Intelligence Review Committee. (2014). "2013-14 Department Performance Report," Government of Canada, October 24, 2014, retrieved October 30, 2014, http://www.sirc-csars.gc.ca/opbapb/dprrmr/2013-2014/index-eng.html.
[190] Security Intelligence Review Committee. (2014). "2013-14 Department Performance Report," Government of Canada, October 24, 2014, retrieved October 30, 2014, http://www.sirc-csars.gc.ca/opbapb/dprrmr/2013-2014/index-eng.html.
[191] Security Intelligence Review Committee. (2012). "Section 54(2) Reports," Government of Canada, October 22, 2012, retrieved March 15, 2015, http://www.sirc-csars.gc.ca/nwsspr/bkgdci/s54rpt-eng.html.

your own.[192]

Forth, as a review organization first-and-foremost, SIRC is tasked with legitimizing CSIS's activities. While critical reports can cast doubts on the actions of CSIS, those doubts are not meant to short-circuit activities as they are being undertaken. With a more aggressive oversight role, SIRC could flag problems more prominently but, even still, issues of resources, provision of information, and legal restrictions on what the review committee can evaluate limit any such oversight role barring significant amendments to the SIRC's mandate and powers.

Office of the Privacy Commissioner of Canada

The Office of the Privacy Commissioner of Canada (OPC) is mandated to oversee compliance with the *Privacy Act* and the *Personal Information and Electronic Documents Act* (*PIPEDA*). The former addresses how the federal government and its departments must handle Canadians' personal information and the latter how private companies collect, process, retain, disclose, and use Canadians' personal information. The OPC exists independently of government and investigates complaints about how government agencies and private companies alike (mis)handle the personal information that they collect.

The OPC operates as an ombudsperson as opposed to a regulator. In this role, the Commissioner's Office tends to adopt the roles of educator, policy adviser, and negotiator. As an educator, the OPC produces its own materials, explaining to businesses how they can comply with *PIPEDA*. This material includes a guidebook for businesses and organizations. In addition, the Office helps businesses understand what their accountability obligations include. The Office has also produced documents for federal institutions, explaining what ought to be included in a privacy impact assessment and what constitutes a complaint investigation under the *Privacy Act*. Resources are also available for individuals. The OPC engages in public outreach activities, explaining how new and emerging practices challenge Canadians' privacy and what actions they can take to defray harm linked to those practices.

In its role as a policy advisor, the OPC frequently provides testimony to Parliament

[192] Chuck Stahl. (2013). "The Standing Committee on National Security and Defence: Evidence," *Parliament of Canada*, December 9, 2013, retrieved March 15, 2015, http://www.parl.gc.ca/content/sen/committee/412%5CSECD/51109-E.HTM.

about privacy-impacting legislation, including proposed security- and intelligence-related bills. In this role, the OPC also receives and analyzes federal institutions' privacy impact assessments. Institutions produce such assessments when they are planning to initiate a program that could affect Canadians' privacy rights or interests. The assessments are evaluated for their cohesion with existing best practices and interpretations of the *Privacy Act*; the OPC does not authorize or validate any given submission and only offers advice on what is submitted.

In its role as an ombudsperson, the OPC is tasked with attempting to find a negotiated settlement between private parties involved in a dispute concerning a privacy matter. Only when a negotiated settlement cannot be reached does the OPC formally investigate the alleged problematic practice, ultimately issuing a decision about the legitimacy of a person's complaints. Such decisions, however, are not binding and do not carry a fiscal penalty. In order for decisions to be enforced, the OPC must go to a federal court and successfully win its case before the courts.

The OPC has repeatedly sought to understand and investigate the extent of telecommunications surveillance in Canada. The Office has previously asked the Canadian Wireless Telecommunications Association (CWTA) to outline the regularity at which government agencies access telecommunications data and how Canadian wireless companies managed these requests.[193] The OPC has also audited the RCMP's collection of subscriber data, only to learn that "based on our review of statistics and interviews with senior officials at the RCMP we were unable to rely upon the numbers provided for warrantless access requests, nor was there any linkage between reports of such requests and the actual operational files containing such requests."[194] The OPC cannot force another government agency to change its activities. While federal agencies sometimes update their practices to reflect the Commissioner's recommendations, they are not legally required to do so. As a result, regardless of the effectiveness of an investigation, the OPC is limited in its ability to enforce its decisions.

The Privacy Commissioner also examines and comments on the activities of other

[193] Gowlings, for the Canadian Wireless Telecommunications Association. (2011). "Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members," Gowlings. December 11, 2011.
[194] See Access to Information and Privacy document released by Public Safety Canada, A-2011-00255.

security and intelligence agencies, such as CBSA, CSIS, and CSE. The Office has previously warned that CBSA's information-sharing practices need to be carefully monitored in light of tragic consequences of Canadian agencies sharing citizens' information with foreign agencies, which has led to a Canadian being tortured by foreign governments. The OPC also recommended that the CBSA secure its computer systems that hold sensitive personal information while, at the same time, tailoring its privacy management framework to account for the Agency's obligations under Canadian law.[195] The OPC has called on CBSA to conduct privacy impact assessments prior to implementing new programs.[196] The Privacy Commissioner has also raised warnings in relation to proposed new powers for CSIS. According to the Privacy Commissioner, the information-sharing provisions in Bill C-51, the *Anti-Terrorism Act, 2015*, would cause an "excessive" loss of privacy by making available "potentially all personal information that any department may hold on Canadians." Further, the Commissioner found that "17 government institutions involved in national security would have virtually limitless powers to monitor and, with the assistance of Big Data analytics, to profile ordinary Canadians, with a view to identifying security threats among them."[197] Per C-51, government agencies can share information that they receive in the course of their regular business operations (e.g. tax information collected by Canadian Revenue Agency) as well as information collected pursuant to a court order, such as an interception, number dialer, or other telecommunications-related order. In addition to warning about CBSA and CSIS activities, the Privacy Commissioner periodically reviews CSE's activities as they pertain to the collection of Canadians' personal information.

Most problematic, however, is how the *Privacy* Act limits the OPC's mandate. Specifically, the Office can examine only personal information according to the *Privacy Act*; the OPC "does not have jurisdiction to examine in general the

[195] Office of the Privacy Commissioner of Canada. (2006). "Audit of the Personal Information Management Practices of the Canada Border Services Agency: Trans-Border Data Flow," Government of Canada, June 2006, retrieved March 14, 2015, https://www.priv.gc.ca/information/pub/ar-vr/cbsa_060620_e.asp#015

[196] Office of the Privacy Commissioner of Canada. (2014). "Appearance before the Standing Senate Committee on National Security and Defence on Canda Border Services Agency (CBSA) border security measures," Government of Canada, April 28, 2014, retrieved March 14, 2015, https://www.priv.gc.ca/parl/2014/parl_20140428_cb_e.asp.

[197] Office of the Privacy Commissioner of Canada. (2015). "Bill C-51, the *Anti-Terrorism Act, 2015*: Submission to the Standing Committee on Public Safety and National security of the House of Commons," Government of Canada, March 5, 2015, retrieved March 15, 2015, https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp.

lawfulness of the activities of national security agencies."[198] The limitations of the *Privacy Act* also mean that "no judicial recourse" exists for complainants to the OPC "in cases involving improper collection, use, disclosure or retention of personal information."[199] Furthermore, the OPC cannot effectively liaise with SIRC or the Office of the Communications Security Establishment Commissioner (OCSEC), and the OPC has stated that under the *Privacy Act*, "there are no provisions for joint audits or investigations with other like bodies, even in an era where information-sharing has increased greatly."[200]

Limitations in mandate and resources prevent the OPC from discerning the full extent of government agencies' telecommunications surveillance or the processes that private corporations undertake when agencies request subscriber information. Even when the OPC discovers that a federal agency is conducting an inappropriate, personal information-based activity, it cannot necessarily stop the activity using the powers afforded to the Office under the *Privacy Act*. And, while the OPC can carry out investigations in response to complaints of private companies' practices, the OPC cannot compel a company to modify its practices without appealing to the federal courts.

Office of the Communications Security Establishment Commissioner

The Office of the Communications Security Establishment Commissioner (OCSEC) is mandated to review the CSE's activities, determining whether the CSE's actions comply with law, investigating written complaints about the CSE, and informing the Minister of National Defence and the Attorney General of Canada of CSE activities that the Commissioner believes are unlawful. Each year the CSE Commissioner

[198] Office of the Privacy Commissioner of Canada. (2015). "Bill C-51, the *Anti-Terrorism Act, 2015*: Submission to the Standing Committee on Public Safety and National security of the House of Commons," Government of Canada, March 5, 2015, retrieved March 15, 2015, https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp.

[199] Office of the Privacy Commissioner of Canada. (2015). "Bill C-51, the *Anti-Terrorism Act, 2015*: Submission to the Standing Committee on Public Safety and National security of the House of Commons," Government of Canada, March 5, 2015, retrieved March 15, 2015, https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp.

[200] Office of the Privacy Commissioner of Canada. (2014). "(Special Report to Parliament) Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance," Government of Canada, January 28, 2014, retrieved March 15, 2015, https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp.

tables a report as a result of examining and evaluating some of CSE's activities for the previous year. All of the CSE Commissioner's review personnel "hold security clearances to allow full access to the classified holdings, facilities and personnel of the intelligence agency being reviewed. This also allows review personnel to acquire expertise about CSE activities"[201] and to conduct in-depth investigations. Since the Office was created in 1996, it has never found that CSE behaved unlawfully.

As noted in the Commissioner's 2003-04 report, the assessment that CSE has behaved lawfully "should not be taken to mean that I am certifying that all CSE's activities in 2003-2004 were lawful. I cannot make this assertion, because I did not review all their activities—and no independent review could."[202] Moreover, the assertion of lawfulness is predicated on evaluating CSE's activities "in light of the Department of Justice interpretation of the applicable legislative provisions."[203] These interpretations, however, have caused concerns for successive CSE Commissioners; since 2001 with the passage of Part 1 of the *National Defence Act* Commissioners have applied an interim "solution of assessing compliance based on the government's interpretation".[204] As a result, there is an element of ambiguity to all assurances by the CSE Commissioner that CSE behaves lawfully: such assurances are predicated on the government's interpretation of CSE's core authorizing Act and which is not available to the public. As summarized by independent researcher Bill Robinson, it is extremely challenging and unlikely that the CSE Commissioner would declare any CSE activity unlawful because,

> the Commissioner would have to choose to examine the activity, sufficient records would have to exist to support a compliance judgement, the Commissioner would have to conclude that the activity violates the law, CSE and the Department of Justice would have to agree

[201] Office of the Communications Security Establishment Commissioner. (2014). "Frequently Asked Questions," Government of Canada, last updated December 8, 2014, retrieved March 15, 2015, http://www.ocsec-bccst.gc.ca/new-neuf/faq_e.php.
[202] Office of the Communications Security Establishment Commissioner. (2004). "Communications Security Establishment Commissioner Annual Report, 2003 – 2004," Government of Canada, retrieved March 15, 2015, http://www.ocsec-bccst.gc.ca/ann-rpt/2003-2004/activit_e.php#4
[203] Office of the Communications Security Establishment Commissioner. (2006). "Communications Security Establishment Commissioner Annual Report, 2003 – 2004," Government of Canada, retrieved March 15, 2015, http://www.ocsec-bccst.gc.ca/ann-rpt/2005-2006/activit_e.php#5
[204] Bill Robinson. (2015). "Does CSE comply with the law?," *Lux Ex Umbra: Monitoring Canadian Signals Intelligence (SIGINT) Activities Past and Present*, March 14, 2015, retrieved March 15, 2015, http://luxexumbra.blogspot.ca/2015/03/does-cse-comply-with-law.html.

> with that conclusion, CSE would have to affirm, or the Commissioner would have to demonstrate, that the activity was authorized by the agency, CSE would have to declare that it intends to continue doing it, and the government would have to refuse to promise to amend the law (at some undefined point in the future) in order to permit the activity. If all those conditions were met, and the Commissioner subsequently reported the issue to the Attorney-General, and no promise (sincere or otherwise) to change either the activity or the law were forthcoming following that step, then and only then would he report to the public that CSE was not in compliance with the law.[205]

In addition to having difficulties reviewing CSE's self-directed actions, the CSE Commissioner suffers from the same limitations as SIRC and the Office of the Privacy Commissioner of Canada, namely that the CSE Commissioner cannot work with other oversight and review bodies. Consequently, the CSE Commissioner cannot adequately 'track' information that the CSE collects as part of its assistance to other agencies, nor is the Commissioner necessarily privy to the full uses of the shared information. In addition, the Office cannot collaborate with foreign oversight and review agencies that monitor British, American, Australian, or New Zealand signals intelligence agencies, despite the fact that these signals intelligence agencies work intimately with the CSE. And, given the CSE Commissioner's inability to comprehensively review all, or even most, of CSE's activities, it is impossible to assure Canadians that all of CSE's activities are lawful.

The limitations of the CSE Commissioner's office were made clear following revelations that CSE massively collects the metadata associated with Canadians' electronic devices. In response to statements that CSE's collection of such metadata "would not be unlawful, under current Canadian law, under our Charter, under [CSE]'s mandates"[206] along with political outcry,[207] the CSE Commissioner found

---

[205] Bill Robinson. (2015). "Does CSE comply with the law?," *Lux Ex Umbra: Monitoring Canadian Signals Intelligence (SIGINT) Activities Past and Present*, March 14, 2015, retrieved March 15, 2015, http://luxexumbra.blogspot.ca/2015/03/does-cse-comply-with-law.html.

[206] Greg Weston, Glenn Greenwald, and Ryan Gallagher. (2014). "CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden document," *CBC News*, last updated January 31, 2014, retrieved March 15, 2015, http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881.

[207] Trinh Theresa Do. (2014). "Liberals call for parliamentary oversight of CSIS, CSEC," *CBC News*, February 4, 2014, retrieved March 15, 2015, http://www.cbc.ca/news/politics/liberals-call-for-parliamentary-oversight-of-csis-csec-1.2522578.

that:

> [based] on our inquiry and on our accumulated knowledge and expertise from reviewing CSE's metadata and network analysis activities over a period of eight years, we concluded that this CSE activity does not involve "mass surveillance" or tracking of Canadians or persons in Canada; no CSE activity was directed at Canadians or persons in Canada.[208]

The language adopted by the CSE Commissioner reflects that of the CSE itself. "Directed at" has a specialized definition for intelligence agencies and is used to refer to cases where an agency is intentionally targeting known and specific individuals. So long as CSE was not collecting Canadian metadata for this purpose (and there is no evidence that this was the specific rationale for the metadata collection), the CSE Commissioner's statement is accurate. However, at the same time, the statement does not reflect what most Canadians would consider mass surveillance, which is a government agency's effort to collect information that could identify and track individuals if the information was analyzed. Such limitations in the Commissioner's analyses and public statements, combined with the previously mentioned limitations, reveal why the OCSEC's review functions are insufficient to satisfy critical questions of the appropriateness of CSE's activities.

Summary

The executive and staff of Canada's review and oversight organizations attempt to fulfill their organizations' mandates and, by most appearances, are committed to their respective organizations' goals. However, good intentions and commitment aside, these organizations mandates need to be updated to reflect the contemporary surveillance and intelligence collection landscape. The *Privacy Act* along with authorizing legislation for SIRC and OCSEC are insufficient to guarantee to Canadians that federal agencies are not inappropriately intruding on citizens' and residents' privacy. Moreover, statutory reporting of surveillance activities, as demonstrated in the Interception Reports, simply does not capture the range and magnitude of contemporary government surveillance activities.

As we discuss in the next section, the current state of telecommunications

[208] Office of the Communications Security Establishment Commissioner. (2014). "Frequently Asked Questions," Government of Canada, last updated December 8, 2014, retrieved March 15, 2015, http://www.ocsec-bccst.gc.ca/new-neuf/faq_e.php.

surveillance governance in Canada threatens to delegitimize the surveillance-related activities that the federal and provincial governments of Canada undertake lawfully. The extent of contemporary government surveillance, limits in corporate transparency, and subtle manipulation of technologies to facilitate government surveillance, combined with limited government review and oversight, have created a situation where citizens cannot understand the ramifications of currently legislated surveillance laws or of those which are proposed in provincial and federal legislation. The result is that, without changes to the current status quo, Canadians cannot meaningfully debate or determine the appropriateness of current surveillance practices regardless of whether they are citizens or (non-Ministerial) members of parliament or legislative assemblies.

Section Five: Risks Posed By Contemporary Telecommunications Surveillance

This report's preceding sections showcased the extent of contemporary government-driven telecommunications surveillance, how technical systems are architected to facilitate such surveillance, the limitations of corporate transparency efforts, and the limitations placed upon federal bodies that are responsible for overseeing and reviewing surveillance activities conducted by Canada's policing, intelligence, and security agencies. In this section, we discuss the harms that arise from the aforementioned telecommunications surveillance activities. Specifically, we focus on harms linked to citizens' inabilities to know how companies and government use their personal information, on how oversight deficits combined with government surveillance-activity secrecy effects citizens' ability to see themselves as authors of laws that authorize surveillance, and on how an unfamiliarity with contemporary surveillance activities hinders citizens' ability to trust their elected representatives to hold government – and its various bodies – to account.

How Is Personal Information Used and Disclosed?

Telecommunications Service Providers (TSPs) provide access to the services that bind our digital lives together; without the spectrum, fiber, copper, and cable infrastructures operated by these companies, it would be functionally impossible for Canadians to communicate using digital technologies. Given these companies' role in the ways Canadians conduct their daily lives, it is imperative that these companies transparently disclose the kinds of information they collect, process, retain, and disclose, especially when their customers specifically ask for this information.

Most major Canadian TSPs have failed, to differing degrees, to meaningfully or comprehensively explain their collection, processing, and storage policies concerning their subscribers' telecommunications data. Sometimes, TSPs have refused to respond to specific questions that subscribers have asked; in other cases, they have provided misleading or incorrect responses. Given these companies' stature in the Canadian economy, it is shocking that they have, in some

cases, failed to develop systems to track how they collect and use their subscribers' personal information. These companies should be able to account for how, and why, they use this information if they genuinely integrate core principles of *PIPEDA*, Canada's commercial privacy legislation, into their operations. In particular, principle five of *PIPEDA* asserts that corporations must limit their use, disclosure, and retention of personal information, and principle eight states that corporations must be open about their practices and policies "relating to the management of personal information."[209] Combined, these principles mean that companies should, first, know what data they collect about Canadians, and second, they should be forthright about what data they collect and how they use this data. Despite the principles establishing what TSPs should do, very few have comprehensively explained their data management practices to their subscribers.

We have documented throughout this report that Canadian TSPs have often responded poorly to Canadians who have inquired about TSPs' data management practices. This extends beyond how companies retain and process data to how often, and for what reasons, they disclose information to other parties. Efforts by independent officers of parliament, Canadian academics, and civil society organizations have routinely met with obfuscation or incomplete explanations of why and how often subscribers' information has been disclosed to government agencies. While some TSPs have begun releasing transparency reports, the data that they have provided does not always indicate how many subscribers have been subject of government surveillance. No TSP has committed to notifying their subscribers of government surveillance or taken a public policy position that subscribers *should* be notified after being the target of government surveillance. Since only communications interceptions are disclosed to subscribers, except when targets of other modes of surveillance have the surveillance findings used against them in court, most TSP subscribers remain oblivious that their TSP has been compelled to disclose the subscribers' information or conducted surveillance of he subscriber. TSPs arguably have a fiduciary duty to their subscribers[210] but few, it seems, have rigorously adopted such a duty into their routine business practices. Consequently, Canadians must partner with TSPs to gain access to the opportunities that the Internet makes possible, but the TSP partners do not

[209] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.
[210] Daphne Gilbert, Ian Kerr & Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," (2006) 51:4 *Criminal Law Quarterly*.

necessarily watch out for Canadians.

Severely Limited Functions of 'Oversight' and 'Review'

Corporations are not the only institutions that are failing Canadians. Federal and provincial governments have passed legislation that expands government agencies' surveillance capabilities without ensuring that oversight and review bodies, independent information and privacy commissioners, or inspectors general can monitor government agencies that conduct telecommunications surveillance. The Canadian Border Services Agency (CBSA) is to be praised for maintaining excellent records about how it uses telecommunications surveillance, but it lacks an inspector general and is not required to account for all the ways that it monitors Canadians. As such, CBSA's record keeping can change at any time without any legal penalty and to the detriment of Canadians who want to understand how the agency requests information from TSPs. The Canadian Security Intelligence Service has had its inspector general office dissolved. At the same time, the Service has obstructed its review body's ability to evaluate its compliance with federal law. And the Office of Communications Security Establishment Commissioner cannot comprehensively monitor Canada's signals intelligence agency and is unlikely to ever find that the agency has behaved unlawfully. While many Canadians might expect the Office of the Privacy Commissioner of Canada (OPC) to 'step in' to supplement the oversight and review functions of other government bodies, the Office's own mandate under the *Privacy Act* limits the OPC to focusing on how personal information is used by the federal government. Moreover, supposing the OPC found inappropriate behavior, it cannot legally compel government agencies to fix their practices.

Even the statutory reporting mechanisms that are meant to clarify the extent of government surveillance are unnecessarily limited. The content of annual interception reports has not kept pace with the multitude of government surveillance techniques; the reports now principally reflect past positive legislative intentions while providing an appearance of transparency concerning government surveillance. To go beyond appearances, the reports would have to include the modes of surveillance – such as access to subscriber records, number dialer records, and access to stored data – that make up the majority of government telecommunications surveillance. While some members of parliament have demonstrated an interest in privacy and data management practices, either by

introducing legislation meant to enhance oversight of Canada's signals intelligence agency or by asking questions of the intelligence and security agencies, these members represent an extreme minority of parliament. No party leader or deputy leader, or groups of back benchers has advanced the issue of making the government accountable for telecommunications surveillance to the top of their long- or medium-term policy or legislative agendas. No parliamentarian in recent years has publicly suggested expanding the reporting functionality of the annual interception reports.

The severe lack of government accountability for its surveillance practices prevents parliamentarians from carrying out their full duties. Members of parliament are elected to represent their constituents' interests and to hold the government accountable. With regard to the latter, members lack sufficient information to know whether the government is judiciously exercising its surveillance powers, whether the exercised powers are effectively addressing social ills, or whether the powers and their associated practices represent a good investment of taxpayer money. Without adequate and critical oversight and review, Parliament cannot know whether Canada's security, intelligence and policing agencies are operating within the scope of their respective mandates, or whether the agencies are appropriately interpreting the scopes of those mandates. Without understanding the extent of federal agencies' activities, it is functionally impossible for members of parliament to represent their constituents' interests. Their constituents cannot *know* whether government surveillance activities are appropriate or excessive, whether these activities offer good fiscal value, or whether they are effective or ineffective. Consequently, constituents are severely limited in their abilities to communicate specific worries, concerns, or questions about telecommunications surveillance. With these limitations, Canadians' members of parliament cannot fully represent their constituents' interests.

It is not just members of parliament who are limited in their abilities to monitor and safeguard Canadians' interests. While Ministers of the government may receive more information about the activities taken by policing, security, and intelligence services than their less-privileged peers, they lack the 'sensors' needed to detect inappropriate behaviours. Specifically, without inspectors general, the government lacks its own internal watchdogs to monitor these agencies. Inspectors raise alerts to their Ministers when they identify agencies that are operating beyond or outside of their mandates that are engaged in potentially unlawful practices. While currently proposed legislation, such as Bill C-51, would radically expand the extent of information-sharing throughout the federal government, the legislation does not

meaningfully expand oversight, review, or other accountability features for the agencies that will soon receive – and release – Canadians' personal information. Such personal information may include telecommunications data that government agencies have collected in either the course of their regular activities or in the course of some kind of investigation. The consequence is that Canadians, their members of parliament, and government ministers alike will, at best, be uncertain about how extensively Canadians' personal information is being disclosed throughout government and, at worst, will have no idea whatsoever.

Implications of Contemporary Canadian Telecommunications Surveillance

The secrecy concerning the extent and modes of telecommunications surveillance restricts public debate concerning the appropriateness, legality, and constitutionality of government-mandated surveillance practices. It also fails to address the risks that are linked to the lawful interception systems that telecommunications companies install or the harms that are connected to using signals intelligence systems to capture massive amounts of information about Canadians.

The secrecy that surrounds surveillance creates a chilling environment in which Canadians will avoid saying, doing, or associating with a specific person, activity, or place solely because such an association could place them under government surveillance. Such an environment threatens democratic governance for at least three reasons. First, such activities rest on laws or interpretations of law that a majority of the public cannot reasonably be believed to have legitimated; without knowledge of the implications of law, citizens cannot be said to have reasonably approved a law vis-à-vis their political representatives. As a result, opaque or secretive government telecommunications-surveillance activities function outside of the scope of citizen-authorization and separate the government's actions from the actions of citizens. Instead of citizens being at the center of democratic power, they become serfs who are protected by their government. Second, secretive telecommunications surveillance has a discouraging effect on the population, straining citizens' willingness to take part in 'risky' political debate that might – or might not – be monitored by government agencies. Moreover, given the breadth of telecommunications surveillance in Canada, the extent to which Canadians are monitored appears to be extensive. No state that genuinely supports democratic norms vis-à-vis strong rights of speech, association, or freedom from unwarranted

searches can be expected to thrive under such conditions. Finally, Canadians currently learn about the extent of government surveillance through corporate generosity, foreign whistleblowers, and the occasional revelatory question that members of parliament ask the government or that an access to information and privacy request brings to light. While each of these actions have afforded some insight into how federal and provincial governments gain access to telecommunications data, they are not sustainable. All telecommunications services companies do not release transparency reports, law-breaking cannot be regarded as a legitimate primary or secondary mechanism to inform citizens about their governments' actions, leadership can muzzle political representatives from asking surveillance-related questions, and delays, redactions, or legislative curtailments can render access to information requests ineffective.

Beyond the sinister effects of government surveillance are unsettling reactions that are based on how unauthorized non-governmental third parties can use Canadian companies' surveillance architectures to illegally intercept Canadians' information. The development and deployment of lawful interception systems are predicated on an understanding that authorities require these systems to identify and respond to suspicious or illegal activities. Wiretaps, number dialer recorders, and access to stored telecommunications information are all used in the course of contemporary governmental investigations. While these modes of surveillance are useful in bringing the law to bear on criminals, they can also be used by unauthorized parties or avoided by the targets of such surveillance. Past research has shown how Cisco systems' and NICE Systems' lawful interception equipment could be remotely activated by an unauthorized third-party,[211] how Greek and Italian lawful interception systems were accessed by unauthorized parties,[212] how the NSA has

[211] Tom Cross. (2010). "Exploiting Lawful Intercept to Wiretap the Internet," Blackhat DC, Washington, DC, retrieved May 1 2015, https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-Lawfull-Intercept-wp.pdf; Johannes Greil, Stefan Viehböck. (2014). "Root Backdoor & Unauthenticated access to voice recordings," *SEC consult Vulnerability Lab*, May 28, 2014, retrieved May 1, 2015, https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20140528-0_NICE_Recording_eXpress_Multiple_critical_vulnerabilities_v10.txt.

[212] Vassilis Prevelakis and Diomidis Spinellis. (2007). "The Athens Affair," *IEEE Spectrum*, June 29 2007, retrieved May 1, 2015, http://spectrum.ieee.org/telecom/security/the-athens-affair; Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. (2014). "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping the Internet," *Northwestern Journal of Technology and Intellectual Property* 12(1).

raised concerns about vulnerabilities in lawful interception architectures,[213] and how the NSA itself has exploited vulnerabilities in lawful interception equipment.[214] Moreover, in some cases where interception systems are inappropriately activated by third-parties, the auditing and other accountability functionalities can be disabled, thus hiding those responsible for illegally activating the systems.[215] Other research has shown that evading lawful interception systems is feasible for technically astute targets.[216] Even the databases that record who was targeted for interceptions, and when, have been successfully targeted: Google, Yahoo!, Microsoft, and other major telecommunications companies were allegedly targeted by the Chinese government in the past.[217] The agreement between society and its government that sanctions the idea that interceptions are needed, must be limited in use, and carefully restricted to authorized persons tends to elide the risks associated with installing interception systems into the communications networks that we rely on to carry out our daily lives.

Beyond the telecommunications surveillance systems and processes that domestic agencies use are those that Canada's signals intelligence agency, the Communications Security Establishment (CSE) have created and deployed. CSE has deployed the EONBLUE packet analysis system throughout Canadian companies' networks. As of 2011, all of the data traffic that was transmitted outside of, and into, Canada's borders could be captured or analyzed by CSE. In 2014, Canadians

---

[213] Susan Landau. (2013). "The Large Immortal Machine and the Ticking Time Bomb," *Journal on Telecommunications and High Technology Law* 11(1).

[214] Ryan Devereaux, Glenn Greenwald, and Laura Poitras. (2014). "Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Phone Call in the Bahamas," *The Intercept*, May 19, 2014, retrieved May 1, 2015, https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

[215] Tom Cross. (2010). "Exploiting Lawful Intercept to Wiretap the Internet," Blackhat DC, Washington, DC, retrieved May 1 2015, https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-wp.pdf.

[216] Romanidis Evripidis. (2008). "Lawful Interception and Countermeasures," Masters of Science Thesis, KTH Information and Communciation Technology, Stockholm, Sweden; Felix "FX" Lindner. (2014). "CounterStrike: Lawful Interception," 30c3, retrieved May 1, 2015, http://phenoelit.org/stuff/CSLI.pdf.

[217] Kenneth Corbin. (2013). "'Aurora' Cyber Attackers Were Really Running Counter-Intelligence," *CIO*, April 22, 2013, retrieved May 1, 2015, http://www.cio.com/article/2386547/government/-aurora--cyber-attackers-were-really-running-counter-intelligence.html; Ellen Nakashima. (2013). "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say," *The Washington Post*, May 20, 2013, retrieved May 1, 2015, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

learned that CSE could, and has, collected domestic Canadian metadata that is geographically associated with airports, coffee shops, businesses, libraries, and universities. Canadians' information was used as part of a CSE experiment, turning the Canadian citizenry into 35 million Canadian lab rats — none of whom consented to having their personal information collected, tracked, and experimented on by their signals intelligence agency. Whether it was EONBLUE that CSE used to collect our information or another program, the federal agency is aggressively hoarding Canadians' personal information for its own secretive purposes. The CSE also tracks the files that Canadians download and has provided questionably-legal assistance to other security agencies when they have wanted to track Canadians. Since Edward Snowden's revelations began in 2013, it has become apparent that Canada's foreign signals intelligence agency is committed to tracking domestic Canadians. Such activities may accelerate as CSE increases the assistance it provides to other federal agencies and as CSIS and CSE, in particular, continue to strengthen their close working relationship. In the United States, the extent of domestic security agencies' surveillance activities and those of the National Security Agency have affected the speech and activities of Americans. It is reasonable to assume that similar effects are being realized amongst Canadians.

In aggregate, telecommunications surveillance establishes chilling conditions that are accentuated by poorly implemented or limited transparency efforts by corporations combined with weak government accountability practices. Moreover, research on lawful interception systems showcases how these systems' vulnerabilities can threaten the privacy of telecommunications customers. Thus, while lawful interception and lawful disclosure of telecommunications information to government agents may be helpful in collecting evidence against suspected criminals, it also is useful in enabling telecommunications surveillance for third-parties who, without the lawful interception architectures, might be unable to as effectively conduct unauthorized surveillance. These chilling effects are accentuated by the CSE's mass collection of data about Canadians' telecommunications.

Summary

Contemporary telecommunications surveillance risks and government's failure to account for transparently explain the processes through which it practices surveillance threaten to distance the electorate from its government. And the distance threatens to widen. Having companies, vendors, and government involved in quietly developing surveillance standards and influencing surveillance products outside of the public eye continues to inhibit citizens' willingness to exercise their

rights on the basis that they cannot know whether, how, or why they might be spied upon. Further, even elected members of parliament cannot hold the government to account because they cannot know what surveillance is occurring. Worse, these systems introduce vulnerabilities into communications networks that unauthorized parties can exploit to the detriment of Canadians' privacy. Such problems are accentuated by CSE's mass surveillance architecture, which is designed to collect data about Canadians' communications within and beyond Canada's borders.

Surveillance by the police, security agencies, or intelligence agencies, can serve a useful function in maintaining order and social peace. But secretive surveillance practices, regulations, and activities can undermine that same order and social peace. In Section Six, we provide recommendations to telecommunications service providers and government. If adopted, these recommendations would mitigate some of the harms caused by contemporary corporate data management practices and secretive government surveillance. If transparency isn't applied to such handling and surveillance practices, however, corporations and government alike will not just maintain a democratically-harmful status quo: they will compound the cynicism that many Canadians feel towards telecommunications companies, government authorities, and politicians, all of whom play essential roles in telecommunications surveillance governance.

Section Six: Recommendations To Alleviate Surveillance-Related Risks

The preceding sections have discussed the extent to which government agencies can, and do, conduct telecommunications surveillance and the technical and legal infrastructures that authorize such surveillance. Although transparency reports that Canadian telecommunications service providers (TSP) are releasing shed some light on the extent of government surveillance, the existing reports can be improved, and more companies must release them for the public to be able to understand the extent to which government agencies request access to corporate-stored or –transited information. Improved reports are especially needed when we consider the limitations that independent commissioners and organizations that oversee, review, and remediate government agencies' surveillance activities work within. Ultimately, a failure to limit government surveillance, significantly extend corporate transparency, or improve governmental oversight, review, and remediation functions will accentuate the surveillance-related harms that Canadians experience.

In this section, we provide recommendations for improving the governance of telecommunications surveillance. Recommendations have been divided between those for TSPs and government agencies. While implementing all of the recommendations would best defray the surveillance governance-related harms experienced by Canadians today, the implementation of *any* of the recommendations will constitute a positive shift in how telecommunications surveillance is governed in Canada.

Policy Recommendations for Telecommunications Service Providers

Recommendation 1: All Telecommunications Service Providers Should Publish Transparency Reports

Per Canada's federal privacy legislation, Canadian businesses must explain to customers how they handle customers' personal information. One aspect of these explanations ought to include the frequency and reasons that information is shared with government agencies. Another aspect of these explanations should include the length of time that companies retain their subscribers' information. An ideal way of communicating these explanations is by releasing annual transparency reports. Federal ministers have asserted that companies are permitted to release such

annual reports so long as they do not indicate to specific individuals that they were targets of government surveillance. Given that companies must provide explanation of how they handle personal information, and that federal ministers have authorized the release of annual reports, all Canadian TSPs should release transparency reports so Canadians can understand how these companies handle their personal information.

Recommendation 2: Standardize Transparency Reports Across the Industry

Canadian TSPs' transparency reports are currently unregulated in terms of the content that they include, how content is presented, and how requests for and disclosures of subscriber information are expressed. Standardization would enhance the effectiveness of reports by making them directly comparable. Without such standardization, the effectiveness of the reports for public policy decision-making is diminished. As such, TSPs should commit to a series of multi-stakeholder meetings, including people from academia, civil societies, government, and the corporate sector, at which they develop standardized transparency reports.

Recommendation 3: Publish Data Retention Periods for All Products

Canadians have a right to understand how their information is collected, processed, and disclosed as part of Canada's federal commercial privacy legislation. Efforts by individuals to understand data retention periods have led to thousands of legally compelling requests being sent to Canadian TSPs since mid-2014. TSPs should commit to publicly disclosing their data retention periods for all of their products so customers can understand how their personal information is handled and so the companies can defray the costs that arise from responding to individuals' questions about their data retention policies.

Recommendation 4: Publish Law Enforcement Guidelines

Canadian TSPs are asked to provide information about their subscribers in up to 80% of investigations. Large companies, such as Rogers and TELUS, and presumably others including Bell Canada and Shaw, receive hundreds of thousands of requests from law enforcement each year. Moreover, companies that receive requests in such large numbers have processes and policies in place to manage the reception of, and response to, these requests. Companies should commit to publishing their law enforcement guidelines in order to reduce the confusion that government agencies may have concerning what data is stored, for how long, and

under what terms it is released. Publishing these guidelines would also strengthen the public's trust that there are practices and policies in place to restrict government agencies' often overbroad or inappropriate requests for subscribers' personal information.

Recommendation 5: Publish Compensation Guidelines

Canadian TSPs are sometimes compensated for collecting or disclosing stored subscriber information to government agencies. Documents provided to the Office of the Privacy Commissioner of Canada demonstrate that many of Canada's largest companies have compensation tariffs in place, though few make them available to the public. These tariffs should be published so that government agencies and the public can understand the costs of contemporary surveillance practices and to begin to understand what the cost of conducting such surveillance is to taxpayers.

Recommendation 6: Develop a 'Government Equipment' Clause

Canadian TSPs have historically opposed federal legislation that would let government agencies install their equipment in TSPs' networking infrastructures. Leaked Snowden documents reveal, however, that the Communications Security Establishment either is installing, or has installed, EONBLUE surveillance systems in at least some TSPs' networks. While companies may be prohibited from disclosing that government networking equipment has been installed in their networks, they could state in their transparency reports, sustainability reports, or in another corporate document that such equipment *has not* been installed. Such a clause could comfort Canadians, confirming that their chosen TSP is responsible for the process of collecting information about its subscribers when the law requires.

Recommendation 7: Commit to Multi-Stakeholder Interception Standards Process

The development of interceptions standards at international organizations is predicated on being invited to what are typically closed-door meetings. As a result, decisions are made about how technologies will be subjected to surveillance and the rationales for such surveillance without true public participation. Canadian TSPs which operate at these organizations and should work to get civil society members invited to these events so they can participate in the development of standards that impact communications privacy and security.

Recommendation 8: Commit to a Lawful Interception Database Breach Notification Process

Various Canadian TSPs possess lawful interception databases, which retain information about who has been subject to government surveillance, when the surveillance took place, and for what reasons. Unauthorized parties could intrude into these databases. In the United States, Google, Yahoo!, and other large Internet companies' lawful interception databases were breached by alleged Chinese hackers. Canadian TSPs should commit to making any such breach public – to Public Safety Canada and to the Privacy Commissioner of Canada – and their annual transparency reports should note whether their lawful interception database were accessed by any unauthorized party.

Policy Recommendations for the Governments of Canada

Recommendation 9: Expand Statutory Reporting of Surveillance Techniques

Current interception reports provide useful information about governmental communications interception, but most government surveillance involves accessing stored information. As a result, the bulk of government surveillance is not accounted for in these reports. Several government agencies have noted that they are not statutorily required to keep records of, let alone report on, their non-interception modes of telecommunications surveillance. Given the shift of government agencies' surveillance techniques toward those favoring access to stored communications databases, access to non-content information, and agencies' failure to proactively disclose their techniques and the regularity at which they use these techniques, Parliament should amend the *Criminal Code* to require all government agencies to record and publicly report their use of non-interception modes of telecommunication surveillance. For example, amendments could explicitly require government agencies to disclose the following modes of surveillance: the use of number dialers, access to subscriber and customer name/address records, tower dumps, use of malware, use of tracking warrants, and use of IMSI catchers.

Recommendation 10: Publish All Government Interception Reports Online

The federal government of Canada currently publishes its interception reports

online, but the same is not true of provincial governments. By amending federal legislation, by passing provincial legislation, or by simply modifying provincial practices, all interception reports should be published online. Publication should include copies of previously completed reports as well as moving forward from 2015.

Recommendation 11: Clarify Whether Order Paper Questions Compel Responses from CSIS and CSE

In the wake of a Parliamentarian's questions about federal agencies' telecommunications surveillance, CSIS asserted that, based on s.19 of the *CSIS Act,* it was largely not required to respond to the questions. CSE also asserted that it was precluded from responding to the Parliamentarian's questions. The federal government of Canada should publicly clarify when, and for what reasons, CSIS and CSE can refuse to respond to a Parliamentarian's questions. Moreover, the government should commit to ensuring that CSIS and CSE always provide the maximal, as opposed to minimal, amount of information to a sitting Parliamentarian's formal questions.

Recommendation 12: Commit to Publicizing and Publicly Updating the Solicitor General's Enforcement Standards

The *Solicitor General's Enforcement Standards* (*SGES*) dictate how mobile communications operators must design their networks to facilitate lawful government interception of mobile communications traffic. In the past, Public Safety Canada has suggested it would secretly modify the *SGES* to expand the breadth of communications that would have to be intercepable without significant consultation with industry and no consultation with civil society, parliament, or the public. The federal government should commit to making the current *SGES* public and to engaging in public consultations prior to updating the Standards.

Recommendation 13: Re-Establish the Inspector General of CSIS

The Inspector General of CSIS provided information about CSIS' activities directly to the Minister and alerted the Minister to wrongdoing or inappropriate interpretations of CSIS's mandate, of Ministerial Authorizations, or of Ministerial Directives. The Inspector General should be re-established to ensure that the Minister receives all of the information required to perform his or her ministerial duties to Parliament.

Recommendation 14: Expand Collaboration Between Oversight and Review Bodies

Canada's oversight, review, and independent review bodies have repeatedly stated that their inability to coordinate and collaborate with one another is hampering their abilities to ensure that the government agencies they monitor are complying with the law. As such, federal legislation should be introduced and passed that would enable the Security Intelligence Review Committee (SIRC), Office of the Communications Security Establishment Commissioner (OCSEC), and Office of the Privacy Commissioner of Canada (OPC) (at a minimum) to share information with one another.

Recommendation 15: Expand Government Agencies That Are Subject to Oversight and Review

Most federal agencies that conduct telecommunications-based surveillance do not have a dedicated independent body that is responsible for ensuring that such surveillance complies with the law. Either dedicated review or oversight bodies should be established for these non-overseen federal agencies or an existing agency such as the SIRC or OPC should be given an expanded mandate and accompanying powers to effectively ensure that all federal agencies' telecommunications surveillance is lawful and appropriate.

Recommendation 16: Commit to Multi-Stakeholder Meetings Before Introducing New Surveillance Powers

Canadians are demonstrably concerned about their privacy and the potential consequences of new surveillance legislation. The government should commit to holding multi-stakeholder meetings with members of law enforcement, civil society, industry, and other interested parties prior to introducing legislation that would extend current surveillance legislation or create new powers. A summary of the meetings should be published before introducing the legislation and the subsequent legislation should reflect the outcome of the consultations.

Recommendation 17: Publish Ministerial Authorizations, Directives, and Memorandums of Understanding Pertaining to CSE and CSIS

CSE and CSIS both receive Ministerial Authorizations and Directives. Authorizations contain conditions pertaining to the actions of these agencies, such as how they can use, retain, or disclose information, whereas Directives establish directions

pertaining to how an agency ought to operate. These authorizations and directives identify the broad contours of what practices and activities Canada's security and intelligence agencies can undertake. Both authorizations and directives should be disclosed to the public - either in a summary or minimally redacted form — within three years of having been established. The delay between issuing the authorizations and directives to the agencies and revealing them to the public would mitigate security concerns that legitimate government surveillance targets could alter their behavior if they learned of the contours of government national security policies. The delay would also provide sufficient transparency to the public and parliamentarians alike and they could express their support for the government's decisions in the parliament and at the ballot box if desired.

Recommendation 18: Provide Appropriate Power for the Office of the Privacy Commissioner of Canada

The Office of the Privacy Commissioner of Canada has a limited mandate under the *Privacy Act* to ensure that federal agencies are effectively safeguarding Canadians' privacy. Moreover, under *PIPEDA,* the Office cannot enforce their decisions without first appealing to the federal courts. The Privacy Commissioner's government- and commercial-mandates are inappropriately restrictive given contemporary data-sharing realities in the private sector and federal government. Consequently, the *Privacy Act* should receive a comprehensive review with the aim of understanding how the Commissioner's mandate should be undertaken. Any reasonable recommendations from this review should be implemented. Moreover, the Commissioner should receive order-making powers equivalent to those enjoyed by many of the Commissioner's provincial counterparts, which allow them to enforce recommendations.

Recommendation 19: Create a Parliamentary Committee That Is Responsible for Overseeing Security and Intelligence Agencies

Parliament should form a national security oversight committee and task it to oversee and report on the adequacy, efficiency, and efficacy of the security and intelligence services' budgetary practices. This committee need not engage in daily oversight. The Committee should also be notified of significant changes to national security policies or novel practices that are about to be undertaken, so members of parliament can genuinely represent their constituents' interests and be able to task review bodies to produce special reports are required. Such a committee would work to ensure that the intelligence and security services provide good value for the tax dollars invested in them and that they are behaving appropriately. Such

parliamentary oversight would assure Canadians that their security and intelligence agencies are operating both within the letter and spirit of the law.

Conclusion

Canadians regularly reveal in surveys, in their personal actions, and in their comments about politics that they are deeply concerned with their online privacy and how commercial actors and government monitor Canadians' online activities. The recommendations that we have presented do not pretend to comprehensively address or respond to the full range of corporate or government modes of collecting, processing, disclosing, and analyzing Canadians' personal information. However, our recommendations would alleviate many of the concerns linked to companies that provide Internet and phone services, and the means by which government agencies routinely monitor such services and their subscribers. Both companies and government must become more accountable for their co-operations with one another and for managing Canadians' personal information, which is collected by or disclosed to policing, security, and intelligence services. If the companies and government fail to do so, they will be viewed only with further suspicion and doubt. For companies, such suspicion will translate into mistrust and doubt about new products and services, which could affect their potential profitability. For governments and their representatives, it will mean that the electorate remains distant, distrustful, and disdainful of persons who are genuinely attempting to maintain order and good government. Companies and governments can reverse these attitudes and the implications they hold for corporate activity and governmental legitimacy. It is well past time for each of them to demonstrably act in the best interests of all Canadian consumers and citizens.