# Special Report on the Lawful Access to Communications by Security and Intelligence Organizations

The National Security and Intelligence Committee of Parliamentarians

September 2025

Canada

The National Security and Intelligence Committee of Parliamentarians
Special Report on the Lawful Access to Communications by Security and Intelligence Organizations

CP104-7/2025E-PDF
ISBN 978-0-660-77736-8

P.O. Box 8015, Station T, Ottawa, Canada, K1G 5A6
www.nsicop-cpsnr.ca

# Special Report on the Lawful Access to Communications by Security and Intelligence Organizations

The National Security and Intelligence Committee of Parliamentarians

Patricia Lattanzio, M.P.
Chair

Submitted to the Prime Minister on March 4, 2025
Revised version tabled in Parliament in September 2025

# Revisions

Consistent with subsection 21(2) of the *National Security and Intelligence Committee of Parliamentarians Act* (NSICOP Act), the Committee may submit a special report to the Prime Minister and the ministers concerned on any matter related to its mandate. Consistent with subsection 21(5) of the NSICOP Act, the Prime Minister may, after consulting the Chair of the Committee, direct the Committee to submit to him or her a revised version of the report that does not contain information the Prime Minister believes the disclosure of which would be injurious to national security, national defence or international relations or is information that is protected by solicitor-client privilege.

This document is a revised version of the Special Report provided to the Prime Minister. At that time, the document was classified as "Top Secret//Special Intelligence//Canadian Eyes Only//Law Enforcement Sensitive." Revisions were made to remove information the disclosure of which the Prime Minister believed would be injurious to national security, national defence or international relations or which constitutes solicitor-client privilege. Where information can simply be removed without affecting the readability of the document, the Committee notes the removal with three asterisks (***) in the text of this document. Where information could not simply be removed without affecting the readability of the document, the Committee revises the document to summarize the information that was removed. Those sections are marked with three asterisks at the beginning and the end of the summary, and the summary is enclosed by square brackets (see example below).

EXAMPLE: [*** Revised sections are marked with three asterisks at the beginning and the end of the sentence, and the summary is enclosed by square brackets. ***]

# The National Security and Intelligence Committee of Parliamentarians

## 44th Parliament

Ms. Patricia Lattanzio, M.P., Chair

Mr. Stéphane Bergeron, M.P.

Mr. Don Davies, M.P.

The Honourable Patricia Duncan, Senator

Mr. Darren Fisher, M.P.
(member until December 20, 2024)

Ms. Iqra Khalid, M.P.
(member until September 17, 2023)

The Honourable Marty Klyne, Senator

The Honourable Frances Lankin, P.C., C.M., Senator
(member until October 20, 2024)

Mr. James Maloney, M.P.
(member until September 17, 2023)

The Honourable David J. McGuinty, P.C., M.P.
(Chair from November 6, 2017 to December 20, 2024)

Mr. Rob Morrison, M.P.

Mr. Alex Ruff, M.S.C., C.D., M.P.

Ms. Brenda Shanahan, M.P.

# Table of Contents

# Background

**1.** In July 2023, Statistics Canada reported that 95% of Canadians aged 15 years and older used the Internet, with a growing number of Canadians becoming more acquainted with newer technologies and incorporating them into their daily routine every year.[1] Advancements such as the use of smartphones and instant messaging applications have made communicating with each other easier and instantaneous, and have generated significant economic and social benefits.

**2.** These technologies also generate a significant amount of personal information, which in certain circumstances is of interest to the state. Specifically, Canada's security and intelligence organizations may need to access this information in support of national security investigations, because they are used in the planning, coordination, financing and perpetration of threats to public safety and the national security of Canada, such as terrorism, serious organized crime, and foreign interference.

**3.** The judicially authorized practice of the interception of electronic communications, and the search and seizure of electronic information, is known as lawful access.[2] Canada's security and intelligence organizations state that they have been for some time facing mounting challenges to their ability to employ lawful access techniques. They state that encryption and the increasing volume, variety, and velocity of digitally generated data make it difficult and sometimes impossible to gather the information needed to carry out effective investigations. Additionally, they state that the global nature of the Internet challenges legislation drafted at a time when information and communications service providers (CSPs) largely resided within Canada's borders.

**4.** However, privacy advocates, civil society groups, academics, and cyber and legal experts state that the government has not effectively made the case to modernize lawful access for security and intelligence organizations, who, they state, are equally able to benefit from the investigative capabilities provided by new technologies.[3] They also warn that efforts to make it easier for police and intelligence organizations to access or circumvent encrypted communications or data fundamentally weaken cybersecurity overall, erode public trust, and threaten fundamental democratic values.[4]

**5.** In 2011, two competing narratives emerged. One described a "golden age of surveillance" where technological advancements allowed governments to have unprecedented access to information about individuals, as well as the ability to store and mine this information for even more detail than communication content could reveal on its own.[5] The other warned of

1 Statistics Canada, "Canadian Internet Use Survey, 2022," July 7, 2023.
2 Department of Justice (DoJ), Industry Canada, and Solicitor General of Canada, "Lawful Access – Consultation Document," 2002.
3 Benjamin J. Goold, "Lawful Access, Privacy, and Trust – Report for the National Security and Intelligence Committee of Parliamentarians," National Security and Intelligence Committee of Parliamentarians (NSICOP) Commissioned Paper, November 2023.
4 Benjamin J. Goold, "Lawful Access, Privacy, and Trust – Report for the National Security and Intelligence Committee of Parliamentarians," NSICOP Commissioned Paper, November 2023; and Siena Anstis, Ronald J. Deibert, Camila Franco, and Zoe Panday, "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," June 30, 2023.
5 Peter Swire and Kenesa Ahmad, "Encryption and Globalization," Ohio State Public Law Working Paper No. 157, *Columbia Science and Technology Law Review*, Vol. 23, 2012, November 17, 2011.

the phenomenon of "going dark," which security and intelligence practitioners referred to as the widening gap between the legal authority to access electronic communications pursuant to judicial authorization and the practical ability to obtain those communications.[6] Often framed as a zero-sum game, the debate set the government's responsibility to prevent and respond to national security threats against Canadians' right to privacy. The debate has been largely stalled since that time.

**6.** One objective of this review is to move the debate beyond this stalemate and prompt a renewed discussion. Security and intelligence organizations are often reluctant to publicly describe highly sensitive operational vulnerabilities, such as those they say are caused by lawful access challenges, so as not to provide adversaries with more information on how to conceal their activities. The National Security and Intelligence Committee of Parliamentarians (the Committee) has access to this information. This access allows the Committee to examine the degree to which lawful access challenges impede the ability of security and intelligence organizations to fulfil their mandates, and to review the government's efforts to respond to these challenges.

## Scope and Approach

**7.** On August 18, 2022, the Committee announced its review of the legislative, regulatory, policy and financial framework for the lawful access to communications by security and intelligence organizations, the challenges of new and emerging technologies, and any limitations of the current framework, set out in the Terms of Reference found in Annex A.[7] The objectives of this review are to examine:

- The current state of lawful access, including the challenges identified by the national security and intelligence community;
- Concerns and criticisms raised by civil society and privacy experts with respect to modernizing authorities in this area;
- The technological challenges relating to lawful access, including interception of communications and the search and seizure of communications-related data;
- The extent to which the security and intelligence community has mitigated the challenges of "going dark" through technology, policy and cooperation with CSPs; and
- The extent to which gaps remain to address the impact of new and emerging technologies on the lawful access of communications.

6 Federal Bureau of Investigation General Counsel Valerie Caproni, "Statement before the United States House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security," Washington D.C., February 17, 2011.

7 NSICOP, "National Security and Intelligence Committee of Parliamentarians launches review of the Lawful Interception of Communications for Security and Intelligence Activities," Press Release, August 18, 2022.

**8.** This review examined information from January 1, 2012, to January 9, 2025, and included the following organizations:

- Canadian Security Intelligence Service (CSIS);
- Communications Security Establishment (CSE);
- Department of Justice (DoJ);
- Department of Public Safety and Emergency Preparedness (Public Safety); and
- Royal Canadian Mounted Police (RCMP).

**9.** In support of the review, the Committee requested material from CSIS, CSE, DoJ, the RCMP, and PS, and relied on Secretariat briefings and departmental responses to written questions. Senior officials from CSIS, CSE, the RCMP, PS, and DoJ appeared before the Committee, sometimes more than once. In the final stage of its review, the Committee held appearances with the Minister of Justice and the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs. The Committee also sought input from stakeholders outside the federal government, including representatives from CSPs, civil society, and the legal community. The Committee extends its gratitude to Ministers, officials, and all presenters for their time and expertise. The full list of witnesses and participants can be found in Annex B.

**10.** To better understand concerns about lawful access, the Committee commissioned or requested research papers from privacy, legal, and cybersecurity experts further to a call for papers. It wishes to acknowledge and thank Professor Benjamin J. Goold, Professor Vivek Krishnamurthy, Professor Michael Geist, and Professor Ron Deibert of the Citizen Lab for their contributions.[8]

**11.** In examining the material presented over the course of this review, the Committee considered the following questions:

- Are Canada's lawful access challenges for national security investigations as serious as the security and intelligence organizations claim?
- Has the government been effective at mitigating or developing solutions to these challenges?
- How does the government facilitate and enable national security investigations while at the same time protect Canadians' right to privacy?

**12.** This review is ultimately about the exercise of state power. The Committee's mandate narrows its scope to the national security activities of the federal government.[9] While the Committee recognizes that Canadian and foreign commercial entities collect Canadians' personal information online, and that these practices raise important privacy questions for legislators, these issues are beyond the scope of this review.

8 The Committee acknowledges receipt of the following papers: Benjamin J. Goold, "Lawful Access, Privacy, and Trust," November 2023; Siena Anstis, Ronald J. Deibert, Camila Franco, and Zoe Panday, "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," June 30, 2023; Michael Geist, "Lawful Interception of Communication by Security and Intelligence Organization: The Policy and Legal Challenges Posed by Real-Time Messaging on Internet Platforms," NSICOP Commissioned Paper, May 2024; and Vivek Krishnamurthy, "Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws Fit for Purpose?" August 30, 2023.

9 NSICOP Act (S.C. 2017, c 15), sections 8 and 13.

# Chapter 1: Privacy and Security in the Digital World

**13.** The individual right to privacy is fundamental to Canadian society.[10] It ensures that people can go about their lives without being subjected to the scrutiny of others, particularly the government. The government, therefore, has an obligation to protect this right while discharging its responsibility to ensure public safety and protect national security.[11] This is critical because lawful access represents one of the most intrusive powers of the state. Notwithstanding the growing ability of commercial entities to collect personal information, only the state has the power to infringe on an individual's personal liberty, including arrest, detention, prosecution, and imprisonment. This chapter seeks to provide a basic understanding of the concept of privacy in the context of lawful access and the intersection of privacy and security.

## Understanding Privacy

**14.** Privacy is a multifaceted concept with several key principles.[12] In the context of this review, it relates most strongly to informational privacy: a person's right to safeguard their information and assert control over how this information is used by the state. It also relates to expectations of anonymity and confidentiality, emphasizing the protection of an individual's ability to keep personal information hidden from public view.[13]

**15.** Privacy is also highly contextual. The Council of Canadian Academies found that individuals' views and decisions regarding privacy change according to varying factors, including their social, geographic, historical, and cultural circumstances.[14]

**16.** While privacy is often framed in the context of individual rights, privacy has a collective dimension as well:

> Privacy is also important because it provides the foundation for the exercise of other fundamental rights and freedoms, chief among them freedom of expression and freedom of association. By enabling individuals to limit who has access to their communications – and to choose with whom they share their ideas and information – privacy allows for the creation of spaces in which different opinions and beliefs can flourish.[15]

10 Office of the Privacy Commissioner of Canada (OPC), *Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP*, August 2022.
11 Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, 2016; and DoJ, Industry Canada, and Solicitor General of Canada, "Lawful Access – Consultation Document," 2002.
12 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015.
13 *R v Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212.
14 Council of Canadian Academies, *Vulnerable Connections: The Expert Panel on Public Safety in the Digital Age*, March 2023.
15 Benjamin J. Goold, "Lawful Access, Privacy, and Trust – Report for the National Security and Intelligence Committee of Parliamentarians," NSICOP Commissioned Paper, November 2023.

**17.** According to the British Columbia Civil Liberties Association (BCCLA), privacy "is a psychological need and a foundational right that many other key rights rest upon. … Privacy therefore undergirds the fundamental freedoms protected by section 2 of the Charter of Rights and Freedoms: the freedoms of conscience, religion, expression, thought, belief, and opinion that lie at the very heart of liberal democracies like Canada, as well as the liberty rights enshrined in section 7 [of the *Canadian Charter of Rights and Freedoms* (the Charter)]."[16]

**18.** The Supreme Court of Canada has described privacy as a "fundamental consideration in a free society," asserting:

> Though an individual's privacy will be preeminently important to that individual, the protection of privacy is also in the interest of society as a whole. Privacy therefore cannot be rejected as a mere personal concern: some personal concerns relating to privacy overlap with public interests.[17]

The Supreme Court's stance reflects a normative approach to privacy protection. This approach focuses "not just on what privacy is, but what privacy should be," using a "broader lens of how we want to live as a society."[18]

**19.** Defining what the norms related to privacy should look like has become increasingly challenging. Research suggests conceptions and expectations of privacy are evolving as digital technology[19] reshapes Canadians' day-to-day lives.[20] While the degree of adoption and use may differ among individuals, the Canadian Council of Academies argues that the ubiquity of digital technologies is such that everyone in Canada can be considered "digital-by-default."[21] With growing amounts of personal information being collected by a host of entities, each with their own approach to protecting this data,[22] considerations about privacy no longer centre on keeping information secret. Rather, they have expanded to include "regulating the flow of information to some, restricting it from some, and opening it up to others."[23]

## Balancing Privacy and Security

**20.** Law enforcement and security agencies are tasked with safeguarding national security and public safety.[24] To do this effectively, they may need to access private communications. Collection and surveillance techniques may generate leads, uncover threats, and help

16 BCCLA, NSICOP appearance, October 1, 2024.
17 *Sherman Estate v Donovan*, 2021 SCC 25, [2021] 2 S.C.R. 75.
18 Ann Cavoukian, "Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy Makers," August 2011.
19 Digital technology refers to use of digital systems, tools, and devices that process, store, and transmit data in electronic form, as distinct from analogue technologies that preceded it.
20 Council of Canadian Academies, *Vulnerable Connections: The Expert Panel on Public Safety in the Digital Age*, March 2023.
21 Council of Canadian Academies, *Vulnerable Connections: The Expert Panel on Public Safety in the Digital Age*, March 2023.
22 Michael Geist, "Lawful Interception of Communication by Security and Intelligence Organizations: The Policy and Legal Challenges Posed by Real-Time Messaging on Internet Platforms," NSICOP Commissioned Paper, May 2024.
23 Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age*, 2018.
24 Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, 2016.

identify and investigate individuals or groups involved in threats such as terrorism, serious organized crime, espionage, and foreign interference.[25] This access necessarily interferes with an individual's right to privacy.[26]

**21.** The collection of personal information by the state differs from the collection of personal information by commercial entities because of the coercive powers of the state, and because electronic surveillance conducted by national security and intelligence organizations happens mostly in secret.[27] In addition to the privacy rights engaged directly by lawful access activities such as electronic surveillance, lawful access may lead to other intrusive or coercive state activities, such as the search and seizure of property, and the sharing of information with other states. In most likeminded democracies, such infringements must be prescribed by law, serve a legitimate purpose, and be necessary and proportionate.[28] (Canada's legal framework for lawful access will be described in the following chapter.)

**22.** Whether such intrusion is appropriate, and if so to what extent, is a matter of fierce debate, often reducing the tension between privacy and security to a zero-sum game. Some argue that such powers should not exist at all; others accept the powers but emphasize the need for robust safeguards on their use.[29] Some also challenge the notion that judicial authorization for lawful access sufficiently addresses privacy concerns. Professor Goold notes,

> While important, legal accountability via judicial oversight only goes part of the way towards ensuring that the police are properly subject to the rule of law. In addition, there needs to be transparency around the range of powers and investigative techniques available to them.[30]

All sides have called for more nuance to the debate, arguing that both privacy and security are integral to Canadian democracy and that there are ways to respect both concurrently.[31]

**23.** According to the BCCLA, the judicial authorization of lawful access is crucial yet not enough, particularly with respect to CSIS investigations where "the possibility remains that CSIS may not be sufficiently candid with the Court to allow full protection of the rights" when seeking a warrant.[32] This concern stems from a landmark Federal Court decision in 2016 which ruled that CSIS had breached its duty of candour when seeking warrants in numerous warrant applications.[33] In a subsequent decision, the Federal Court noted that repeated breaches suggested "a degree of institutional disregard for – or a the very least – a cavalier institutional approach to – the duty of candour and, regrettably, the rule of law."[34] CSIS notes that it has since adapted its practices with the Federal Court to better satisfy duty of candour obligations and believes that trust has been restored with the Federal Court.[35]

25 DoJ, Industry Canada, and Solicitor General of Canada, "Lawful Access – Consultation Document," 2002.
26 DoJ, Industry Canada, and Solicitor General of Canada, "Lawful Access – Consultation Document," 2002.
27 BCCLA, NSICOP appearance, October 1, 2024.
28 Council of Europe Commissioner of Human Rights, "Highly intrusive spyware threatens the essence of human rights," January 2023.
29 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015.
30 Benjamin J. Goold, "Lawful Access, Privacy, and Trust – Report for the National Security and Intelligence Committee of Parliamentarians," NSICOP Commissioned Paper, November 2023.
31 OPC, NSICOP appearance, June 18, 2024.
32 BCCLA, NSICOP appearance, October 1, 2024.
33 2016 FC [Federal Court] 1105, public version.
34 2020 FC 616, public version.
35 CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.

**24.** The Privacy Commissioner has stated that transparency about how security and intelligence agencies consider privacy concerns can act as an "accelerator" of trust in government institutions.[36] In other words, if these agencies put in place mechanisms and practices to demonstrate how they put privacy at the forefront of their deliberations and actions, the public is more likely to trust the necessity of the proposed investigative authorities and tools. This in turn fosters public consent and legitimacy when it comes to actions that may interfere with Canadians' Charter rights.

**25.** As such, some privacy advocates have called for increased transparency by law enforcement and security agencies in carrying out lawful access activities.[37] Transparency mechanisms include regular reporting on government requests and access to personal information, a greater involvement of privacy protection organizations in the development of lawful access capabilities, and legally mandating privacy impact assessments.[38]

**26.** Professor Goold cautions against linking trust and transparency in this way:

> [While] the promotion of trust serving as a justification for greater transparency – might appear to be unproblematic, the assumption that more transparency is always and inevitably a good thing is one that deserves further examination. This is particularly true when it comes to the use of surveillance technologies by the police and security services. Although transparency is often cited as a necessary prerequisite for institutional accountability, it can also play a role in the normalization of activities that should be seen as exceptional.[39]

**27.** Similarly, Professor Goold calls for a shift in the way the government initiates legislative reform to address lawful access challenges so that Canadians who are concerned about privacy do not feel they need to "be on the defensive."[40] He argues the government needs to better justify the need for expanded surveillance powers and tools in a more transparent way.[41] This is particularly important because once privacy is ceded as a consequence of new authorities or the adoption of a new technology, that ground is rarely ceded back:

> Once granted, powers conferred to agents of the state like the police are rarely withdrawn or curtailed, and while we may not be concerned about the misuse of such powers in the current political climate, circumstances can change. Similarly, before expanding the surveillance capacities of the state to allow the police and security services to use [On-Device Investigative Tools or] ODITs or other forms of lawful hacking, lawmakers and the public should consider the risk that such capacities may be misused in the future.[42]

**28.** The Committee intends to address these risks and those raised by the security and intelligence community in this report.

---

36 OPC, *Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP*, August 2022.
37 OPC, NSICOP appearance, June 18, 2024.
38 OPC, NSICOP appearance, June 18, 2024.
39 Benjamin J. Goold, "Lawful Access, Privacy, and Trust – Report for the National Security and Intelligence Committee of Parliamentarians," NSICOP Commissioned Paper, November 2023.
40 Benjamin J. Goold presentation to NSICOP, May 21, 2024.
41 Benjamin J. Goold, "Lawful Access, Privacy, and Trust – Report for the National Security and Intelligence Committee of Parliamentarians," NSICOP Commissioned Paper, November 2023.
42 Benjamin J. Goold, "Lawful Access, Privacy, and Trust – Report for the National Security and Intelligence Committee of Parliamentarians," NSICOP Commissioned Paper, November 2023.

# Chapter 2: Canada's Legal Framework for Lawful Access

**29.** Lawful access refers to the judicially authorized interception of electronic communications, and the search and seizure of electronic information, in accordance with Canada's legal framework.[43] This chapter describes some of the rights and freedoms guaranteed in the Charter, the authorities provided in the *Criminal Code*, the C*anadian Security Intelligence Service Act* (CSIS Act), the *Communications Security Establishment Act* (CSE Act), other relevant legislation, and how Canada compares with likeminded international partners in responding to these challenges. Jurisprudence has also played an important role in shaping the use of lawful access tools and techniques by law enforcement and security agencies. This chapter describes how Supreme Court decisions in 2014 (*R v Spencer*) and 2024 (*R v Bykovets*) shaped lawful access.

## *Canadian Charter of Rights and Freedoms*

**30.** The Charter[44] enshrines and protects Canadians' individual rights against undue interference by the government.[45] A part of the Constitution, the Charter reigns supreme: all laws in Canada must be consistent with the rules or principles it sets out.[46] In the context of lawful access, one Charter right is particularly salient: section 8, which states that "Everyone has the right to be secure against unreasonable search or seizure." Section 8 has been held to safeguard one's reasonable expectation of privacy.[47] Activities by law enforcement and security agencies must comply with section 8 or they may be subject to challenges in court.[48] Section 8 requires that intrusions on an individual's reasonable expectation of privacy have some form of legal authority, which is typically commensurate with prior judicial authorization.[49]

**31.** Section 8 of the Charter protects Canadians and persons in Canada from *unreasonable* searches by government investigators. Soon after the coming into force of the Charter, the Supreme Court ruled that section 8 is meant to prevent unreasonable searches before they occur, making a warrantless search presumptively unreasonable.[50] A few years later, the Supreme Court ruled that a search not authorized by law was unreasonable.[51] Statutes that authorize electronic surveillance generally require government investigators to obtain judicial authorization prior to conducting the search; this is the case for the warrant

43 DoJ, Industry Canada, and Solicitor General of Canada, "Lawful Access – Consultation Document," 2002.
44 *Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the *Canada Act 1982*, 1982, c 11 (U.K.).
45 Henri Brun, Guy Tremblay & Eugénie Brouillet, *Droit constitutionnel*, 5th edition, 2008.
46 Henri Brun, Guy Tremblay & Eugénie Brouillet, *Droit constitutionnel*, 5th edition, 2008.
47 Steve Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" *Supreme Court Law Review*, 2014.
48 Henri Brun, Guy Tremblay & Eugénie Brouillet, *Droit constitutionnel*, 5th edition, 2008.
49 Henri Brun, Guy Tremblay & Eugénie Brouillet, *Droit constitutionnel*, 5th edition, 2008.
50 *Hunter v Southam*, [1984] 2 SCR 145.
51 *R v Collins*, [1987] 1 SCR 265.

powers in the *Criminal Code* and the CSIS Act.[52] The threshold required to obtain judicial authorization generally depends on the level of intrusion into one's reasonable expectation of privacy, with a higher threshold required for more serious intrusions.

**32.** A search is an investigative technique that infringes on an individual's reasonable expectation of privacy.[53] If an investigative technique does not infringe on a reasonable expectation of privacy, then it is not a search.[54] A search is lawful if it is reasonable under section 8 of the Charter.[55] According to the Supreme Court, "A search will be reasonable if it is authorized by law, if the law itself is reasonable and if the manner in which the search was carried out is reasonable."[56]

## *Criminal Code*

**33.** The RCMP investigates offences in Canada and abroad related to national security, transnational and serious organized crime, financial crime, and cybercrime.[57] The RCMP relies on provisions in the *Criminal Code* to authorize its lawful access activities. All law enforcement in Canada can obtain a judicial authorization for the interception of private communications, more commonly known as a wiretap, by filing an application as set out in Part VI of the *Criminal Code* with the assistance of Crown counsel.[58] Police may be authorized by a judge to intercept private communications without the consent or knowledge of the parties to the communication, provided that the application meets the criteria and complies with the safeguards outlined in the authorization.[59]

**34.** It is important to note that Part VI of the *Criminal Code* applies to prospective interceptions of communications in real time, rather than retrospective searches of stored communications. As described by Professor Krishnamurthy,

> This reflects the former technological reality whereby intercepting communications in real time, such as by conducting a wiretap, was a very different act than obtaining records of past communications, such as by searching a suspect's home for incriminating letters. Part VI subjects real-time interceptions of communications to stringent safeguards on the theory that such interceptions are the most serious invasion of privacy imaginable by the state in the exercise of its criminal law enforcement power.[60]

52 According to CSIS, the Federal Court has found s.12 of the CSIS Act to provide reasonable authority for searches that minimally intrude on privacy interests. CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.
53 Steve Coughlan, *Criminal Procedure*, 3rd edition.
54 Steve Coughlan, *Criminal Procedure*, 3rd edition.
55 Steve Coughlan, *Criminal Procedure*, 3rd edition.
56 *R v Collins*, [1987] 1 SCR 265.
57 Section 18 of the *Royal Canadian Mounted Police Act* and the common law authorize the RCMP to prevent and investigate crime, while Section 6(1) of the *Security Offences Act* makes the RCMP the primary police agency for criminal activities that are a national security threat as defined in section 2 of the CSIS Act.
58 *Criminal Code*, RSC 1985, c C-46, Part VI (Invasion of Privacy).
59 There are other wiretap applications that are available in Part VI, e.g., one-party consent applications.
60 Vivek Krishnamurthy, "Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws fit for Purpose?" NSICOP Commissioned Paper, December 2023.

**35.** In light of the high threshold imposed for seeking a wiretap, law enforcement will generally seek other orders first to collect the information and evidence they need to meet that threshold. For example, they may first seek a transmission data recorder warrant, which permits the collection of information about communications (i.e., transmission data, sometimes informally referred to as metadata), but not the content of the communication itself.[61]

**36.** Additionally, the complexity of some investigative tools and techniques may require law enforcement to obtain multiple authorizations involving several provisions of the *Criminal Code* to deploy them. For example, to deploy an ODIT could require several different authorizations, including a wiretap authorization, a transmission data recorder warrant, and a general warrant.[62] Advances in communication technologies can also often result in law enforcement seeking additional judicial authorizations under the *Criminal Code* to deploy the investigative tool or technique in question. These could include an assistance order to compel a person or company to assist law enforcement in the execution of an authorization or warrant,[63] or a preservation order to compel a person or company to keep electronic evidence until an appropriate warrant is obtained.[64]

## *Canadian Security Intelligence Service Act*

**37.** Under section 12 of the CSIS Act, CSIS is responsible for investigating, collecting, and analyzing information on activities suspected of constituting threats to the security of Canada.[65] These are defined in the Act as espionage or sabotage, foreign-influenced activities, terrorism, and subversion.[66] CSIS is also authorized to assist the Minister of National Defence or the Minister of Foreign Affairs in the collection of information and intelligence on foreign states or actors within Canada under section 16 of the CSIS Act.

**38.** To support its intelligence collection mandates, CSIS may seek warrants[67] from the Federal Court under section 21 of its Act to conduct electronic surveillance, known informally as section 12 or section 16 warrants, depending on whether they are acting pursuant to their section 12 or section 16 mandate. In June 2024, *An Act Respecting Countering Foreign Interference* amended the CSIS Act to include new authorities related to lawful access.[68] This included a specific warrant to obtain information, records, and documents, and an ability for CSIS to seek production orders. Prior to these amendments, CSIS only had one warrant authority under the Act to authorize privacy intrusive activities, regardless of the actual impact of the investigative tool or technique on one's reasonable expectation of privacy.

**39.** In order to obtain a warrant, CSIS provides the Federal Court an affidavit that sufficiently describes "the nature and background of the particular threat, the course of the investigation to date, and the purpose for which the intrusive powers are being sought."[69] CSIS must also demonstrate to the judge that the criteria in the CSIS Act to issue the warrant are satisfied.

---

61 *Criminal Code*, RSC 1985, c C-46, s 492.2.
62 RCMP, "On-Device Investigative Tool (ODIT) Technical Description: Draft for Project," August 2022.
63 *Criminal Code*, RSC 1985, c C-46, s 487.02.
64 *Criminal Code*, RSC 1985, c C-46, s 487.012 and s 487.013.
65 CSIS Act, RSC 1985, c C-23, s 12.
66 CSIS Act, RSC 1985, c C-23, s 2.
67 The Federal Court has found that sections 12 and 16 constitute reasonable lawful authority for minimally intrusive searches. CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.
68 *Countering Foreign Interference Act*, SC 2024, c 16 (assented to June 20, 2024).
69 Murray Segal, *Review of CSIS Warrant Practice*, December 2016.

Unlike warrants sought under the *Criminal Code*, CSIS warrant applications do not generally face the same level of public scrutiny and legal challenges by interested parties given that there is no notification to those individuals who are subject to interception under the warrant. This is primarily because CSIS' objective is to collect intelligence and not evidence for eventual use in a prosecution; this approach also reflects the sensitivity of the information included in warrant applications and of the underlying investigations.[70] For this reason, a range of administrative and executive safeguards, such as approval by the Minister, are required for each application.[71]

## *Communications Security Establishment Act*

**40.** CSE is Canada's foreign signals intelligence agency. Under the CSE Act, CSE is responsible for collecting "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security."[72] CSE is prohibited from directing its foreign intelligence activities at Canadians and it must put in place appropriate measures to protect the privacy of Canadians when it incidentally acquires information related to them.[73] CSE does not have any domestic lawful access authorities of its own.[74]

**41.** Section 20 of the CSE Act provides a mandate for CSE to assist federal law enforcement and security agencies.[75] Accordingly, when the RCMP and CSIS have obtained the appropriate authorization to carry out lawful access activities, they may request that CSE assist with conducting operations, including by designing technical capabilities or intercepting communications.[76] When providing technical and operational assistance, CSE is bound by all of the restrictions and conditions imposed on the RCMP or CSIS in carrying out the activity.[77]

## Other Relevant Legislation

**42.** Certain provisions of the *Canada Evidence Act* and Canada's privacy legislation, which includes the *Privacy Act*, are also relevant when considering Canada's legal framework for lawful access.

**43.** ***Canada Evidence Act***: Sections 37 and 38 of the *Canada Evidence Act* establish a regime for the government to object to the disclosure of sensitive or injurious information in a legal proceeding. Under Section 37, the government can seek to prevent the disclosure of information relating to a sensitive law enforcement investigative tool or technique, including lawful access techniques. Section 38 permits the government to withhold access to information that is sensitive or injurious to Canada's international relations, national defence

70 Craig Forcese and Leah West, *National Security Law*, 2020; and CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.
71 National Security and Intelligence Review Agency (NSIRA), *NSIRA Review arising from Federal Court's Judgment in 2020 FC 616*, 2022.
72 CSE Act, SC 2019, c 13, s 2.
73 CSE Act, SC 2019, c 13, s 24.
74 Craig Forcese and Leah West, *National Security Law*, 2020.
75 CSE Act, SC 2019, c 13, s 20.
76 CSE Act, SC 2019, c 13, s 20; and CSE, *Assistance to federal partners*, April 2021.
77 CSE, *Assistance to federal partners*, April 2021.

or national security, which can also apply to tools and techniques developed and used by security and intelligence organizations. When an agency invokes a privilege, the question of whether the public interest in preventing injury (i.e., by maintaining secrecy) outweigh the interests of the party seeking disclosure is considered by the applicable court.[78] In criminal trials, courts can order disclosure where they determine that the balance falls in favour of the accused. The Crown will then have to decide whether to disclose the information to the defence, refrain from using the information, or stay the charges.

**44.** ***Privacy Legislation***: The *Privacy Act* sets out the law as it relates to the information-handling practices of personal information by federal government departments and agencies, including how it can be collected, used, or shared.[79] The *Personal Information Protection and Electronic Documents Act* governs the collection, use, and disclosure of personal information by private-sector organizations in Canada.[80]

## Notable Jurisprudence

**45.** Jurisprudence plays a significant role in informing the boundaries of Canada's legal framework. Most notably, several key decisions of the Supreme Court have shaped the understanding of what constitutes a reasonable expectation of privacy. The jurisprudence is such that law enforcement and intelligence agencies are generally required to obtain prior judicial authorization to collect a broad array of information related to communications in the context of investigative and information-gathering activities.

**46.** ***Reasonable Expectation of Privacy***: Over the last decade, the Supreme Court has significantly expanded the scope of what gives rise to a reasonable expectation of privacy in the digital age. In *R v Spencer* (2014), the Supreme Court unanimously determined that the link between the identity of individual internet users and their use of the internet gives rise to privacy interests and that internet users have a reasonable expectation of privacy. Specifically, the Court found that basic subscriber information (BSI) based on a known internet protocol (IP) address provided insights into the personal life of internet users that they would reasonably expect to be private.[81] As such, the Court determined that a request for BSI amounts to a search and thus requires prior judicial authorization.

**47.** More recently, in *R v Bykovets* (2024), a 5-4 split decision of the Supreme Court determined that there is also a reasonable expectation of privacy associated with a person's Internet Protocol (IP) address, and a request to a private company, such as a CSP, to obtain this identifier amounts to a search. Accordingly, law enforcement requires prior judicial authorization to obtain this information.[82]

**48.** ***Disclosure in Criminal Matters:*** The Supreme Court has long since established the obligation of the Crown to disclose all relevant and material information, except that which is privileged, to the defence so that accused persons may make full answer and defence to any charges brought against them.[83] However, this legal duty to disclose can become a challenge in the context of national security criminal investigations, a problem generally

78 *Canada Evidence Act*, RSC, 1985, c. C-5; and Craig Forcese and Leah West, National Security Law, 2020.
79 *Privacy Act*, RSC 1985, c P-21.
80 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.
81 *R v Spencer*, 2014 SCC 43.
82 *R v Bykovets*, 2024 SCC 6.
83 *R v Stinchcombe*, [1991] 3 S.C.R. 326.

known as the intelligence and evidence dilemma.[84] This dilemma is particularly acute in circumstances in which a shared sensitive tool or technique has been used to gather evidence, such as text messages among suspects who allegedly planned an attack.

## Canada's Approach to Intercept Capability

**49.** In the context of lawful access, the interception of private communications, such as phone calls and emails, often requires the cooperation of one or more CSPs. CSPs are entities that "offer telecommunications services or some combination of information and media services, content, entertainment, and application services over networks."[85] In order to execute a warrant from CSIS or the RCMP, some CSPs rely on tools built into their telecommunications system or network to intercept the communication or other data.

**50.** There is currently no legislative mechanism in Canada to compel CSPs to develop, deploy or maintain their systems in such a way as to remain intercept capable. This means that even where prior judicial authorization is obtained by law enforcement or national security officials to intercept the communications of a specific target, they may not be able to obtain these communications because a technological solution may not exist to intercept, collect, and transfer the communications or their associated data to the requesting agency.[86]

**51.** There is one notable, if dated, exception. Under the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications (SOLGEN standards), certain CSPs are required to ensure that their systems are intercept capable to obtain a licence under the *Radiocommunication Act*. Last updated in 1995, this standard only applies to radio frequencies for wireless voice telephony services, i.e., cellular voice services.[87] It does not apply to landline telephones or digital communications technology such as email, social media and messaging platforms, satellite communications, or Wi-Fi. The SOLGEN standards are not law, and not all cellular providers fully comply with them.[88]

**52.** Unlike Canada, all other Five Eyes and Group of Seven countries have legislation compelling CSPs to maintain intercept capable networks. In 2023, the RCMP conducted a comparative analysis of other Western democracies, surveying Australia, Belgium, Denmark, Finland, France, Germany, Ireland, the Netherlands, New Zealand, Norway, Spain, Sweden, Switzerland, the United Kingdom (U.K.), and the United States (U.S.). While each country has its own distinct framework, all have intercept capability legislation.[89] Some countries have legislation that applies only to traditional communications services such as wireline and mobile telephony and Internet service providers, whereas others have legislation that applies to both traditional and modern services (e.g., internet service providers and over-the-top applications). Countries varied on the funding model for costs associated with the

84 Craig Forcese and Leah West, *National Security Law*, 2020.
85 Lawful Access Advisory Committee, "Governance Framework," May 2024.
86 DoJ, Industry Canada, and Solicitor General of Canada, "Lawful Access – Consultation Document," 2022.
87 Lawful Access Advisory Committee, "Governance Framework," May 2024.
88 Public Safety (PS), NSICOP appearance, April 11, 2024.
89 RCMP, "International Comparison of Lawful Access Coordination and Funding Models," draft, 2023.

development and maintenance of intercept capability and operational fees, either using a model in which CSPs paid, the government paid, or a hybrid approach.[90] Table 2.1 summarizes the positions of Five Eyes partners on key aspects of intercept capability.[91]

**Table 2.1: Intercept capability legislation in Canada, the U.K., Australia, the U.S, and New Zealand**

| | CANADA | UNITED KINGDOM | AUSTRALIA | | UNITED STATES | NEW ZEALAND |
|---|---|---|---|---|---|---|
| Legislation | None. | *Investigatory Powers Act 2016* (last amended 2024) | *Telecommunications and Other Legislation (Assistance and Access Act) 2018* | *Telecommunications (Interception and Access) Act 1979* (last amended 2021) | *Communications Assistance for Law Enforcement Act (CALEA)* | *Telecommunication (Interception Capability and Security) Act 2013* |
| Scope | | All CSPs | All CSPs | Carriers | Carriers | Carriers |
| Requirement | | Minister compels individual CSPs to build and maintain intercept capability through orders. | Agencies may require assistance and Ministers may require capabilities be built. | General requirements for intercept capability. | General requirements for intercept capability. | General requirements for intercept capability. |
| Coverage | | Full coverage.<br>Unlike the U.S. or New Zealand, the U.K. and Australia's intercept laws apply to out-of-country social media platforms and messaging apps. | | | Partial coverage:<br>CALEA applies to landline phones, cellular voice & data, texts, broadband internet, and VoIP. | Full coverage of carriers only. |
| Compensation Framework | | Government must make an "appropriate contribution" towards costs of complying with the Act. | Providers are generally compensated for reasonable costs of complying. | CSPs cover costs of intercept capability. | Compensation may be provided if the capability is not "reasonably achievable." | CSPs cover costs of intercept capability. |

90 RCMP, "International Comparison of Lawful Access Coordination and Funding Models," draft, 2023.

91 Adapted from a presentation by Public Safety. NSICOP added the "Coverage" row and the "Canada" column. Public Safety, NSICOP appearance, April 11, 2024. In this context, the Committee understands a "carrier" to mean an entity that operates a transmission facility used to provide telecommunications services to the public for compensation.

## Transparency and Review

**53.** In the context of lawful access, Canada's law enforcement and security organizations are subject to a variety of obligations for disclosure, transparency, and review. With respect to the RCMP, the government is required to report annually to Parliament on the use of audio and video electronic surveillance.[92] The government tabled its most recent report to Parliament, the 2022 Annual Report on the Use of Electronic Surveillance, in 2024.[93]

**54.** CSIS is not required to publicly report on the number of investigations it conducts, nor on its use of electronic surveillance. Similarly, CSE is not required to publicly report on the number of requests for assistance it receives or responds to from CSIS and the RCMP.

**55.** All three organizations are subject to review by the National Security and Intelligence Review Agency and by this Committee.

92 *Criminal Code*, RSC 1985, c C-46, s 195; and RCMP, "RCMP factual accuracy submission – NSICOP Lawful Access Draft Report," December 20, 2024.

93 Public Safety, *2022 Annual Report on the Use of Electronic Surveillance*, May 2024. The report covers a five-year period between 2018 and 2022.

# Chapter 3: Lawful Access Challenges

**56.** Canada's security and intelligence organizations state that they face significant challenges in successfully obtaining lawful access to communications due to the growing gap between the lawful authority to collect information and the technical capability to do so.[94] In 2018, the Director of CSIS described lawful access problems as one of "the most significant challenges" he had identified to the government.[95] Three factors contribute to this state of affairs: the effects of advances in technology; the absence of legislation for intercept capability; and, jurisdictional issues arising due to the cross-border nature of digital data. This chapter describes these challenges, including their impact on the ability of the RCMP and CSIS to conduct national security investigations, and how these organizations have adapted to mitigate the challenges. Throughout this chapter, the views of cybersecurity and legal experts, privacy advocates, and industry representatives have been reflected.

## The Effects of Advances in Technology

**57.** Cybersecurity expert Susan Landau describes humanity as being in the midst of a Digital Revolution, a period transforming human society as significantly as the preceding Agricultural and Industrial Revolutions, but moving more rapidly and with more profound consequences.[96] The introduction of the microprocessor, the opening of the Internet for commercial use, the rapid adoption of cellphones and their subsequent evolution into smartphones, and the advent of social media and webmail, among numerous other advances, have fundamentally transformed how human beings live their everyday lives. Artificial intelligence will likely increase this already exponential rate of change.

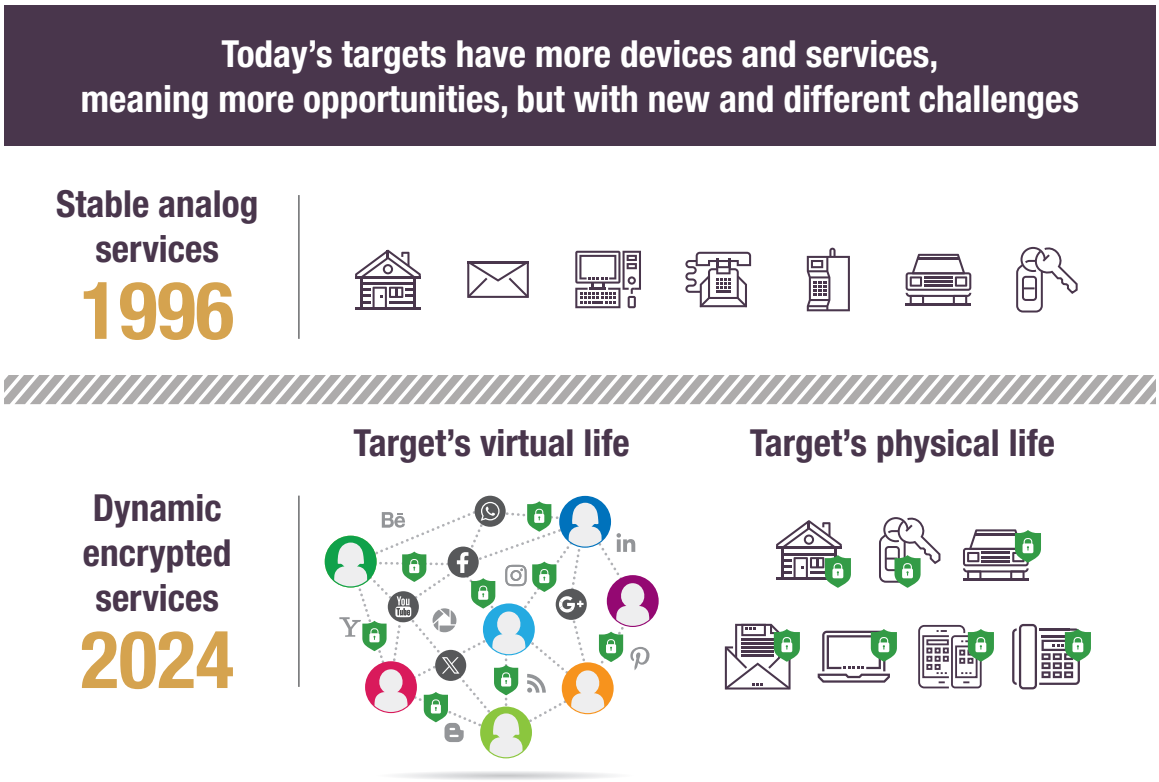
**58.** The widespread adoption of digital technologies has also transformed how intelligence and law enforcement organizations investigate threats to national security. According to Public Safety, while these technological advancements mean there are more opportunities for interception, they come with new and different challenges for national security practitioners, as depicted in Figure 3.1.[97] For their part, CSIS and the RCMP describe this new environment as increasingly complex for several key reasons.[98]

**59.** First, Canadians have more ways of communicating than ever before, including more devices, more services, and more providers.[99] Consequently, the volume, variety, and velocity of data being generated is greater than ever before. Types of data include voice communications, internet browsing histories, chat transcripts, and geolocation, creating an

94 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
95 Stephanie Carvin and Craig Forcese, "Episode 36: An INTREPID Podsight: CSIS Director David Vigneault," May 11, 2018.
96 Susan Landau, *Listening In: Cybersecurity in an Insecure Age*, 2017.
97 Public Safety, "Technological Changes and their Policy Impacts on Lawful Access: Scoping Briefing to the National Security and Intelligence Committee of Parliamentarians," April 11, 2024.
98 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
99 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.

abundance of metadata or "data about data."[100] A variety of everyday web-enabled "smart" objects, such as personal fitness trackers, televisions and cars, now have embedded sensors, electrical components and software collecting data and information from their surroundings, adding to this abundance of metadata. Described as the Internet of Things, the Canadian Centre for Cyber Security projects that there will be more than 30 billion Internet of Things connections by 2025.[101]

**Figure 3.1: Lawful access, then and now[102]**




**60.** Second, the content of communications has become easier to protect with the ubiquitous use of encryption, which is the process of converting digital information into an unreadable format so that only someone with the decryption key can read it. Encryption is used to authenticate users and keep information confidential, safeguarding both "data at rest" and "data in transit."[103] Widely regarded as a best practice to enhance security and protect

100 Vivek Krishnamurthy, "Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws Fit for Purpose?" NSICOP Commissioned Paper, December 2023.

101 Canadian Centre for Cyber Security (CCCS), "Internet of Things (IoT) Security – ITSAP.00.012," July 2022.

102 Adapted from Public Safety, "Technological Changes and their Policy Impacts on Lawful Access: Scoping Briefing to the National Security and Intelligence Committee of Parliamentarians," April 11, 2024.

103 Lex Gill, Tamir Israel, and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, joint research publication by the University of Toronto's Citizen Lab and the University of Ottawa's Canadian Internet Policy & Public Interest Clinic, 2018.

privacy online, encryption is vital to cybersecurity, e-commerce, data and intellectual property protection, and commercial interests.[104] According to CSIS, 90% of internet traffic is encrypted.[105]

**61.** The last decade has also seen an increase in the adoption of "over the top" communication applications and services with end-to-end encryption (e.g., WhatsApp or Telegram). Even where a solution has been put in place with a CSP, use of applications with end-to-end encryption limits the ability of law enforcement and security agencies to read messages for their intended recipient because neither the message service provider nor the carrier can decrypt the messages. In addition to encryption technologies, the prevalence of anonymizing technologies such as virtual private networks, The Onion Router, and the dark web also makes it hard ***.[106] Looking to the *future*, the evolution of artificial intelligence and the anticipated adoption of quantum computing will add further complexity (see text box).

> According to the Canadian Centre for Cyber Security, the **dark web** or DarkNet is an unindexed segment of the Internet that is only accessible by using specialized software or network proxies such as the Onion Router. This access is mainly designed to hide the identity of the user: "[d]ue to the inherently anonymous and privacy-centric nature of the dark web, it facilitates a complex ecosystem of cybercrime, and illicit goods and services trade."[107]

**62.** Third, the transnational nature of the Internet means that cross-border data flows are the rule rather than the exception. Cyberspace is not constrained by geopolitical boundaries. Many, if not most, Canadians use digital services whose messaging solutions are from third-party companies that are based outside of Canada.

> According to CSE, **quantum computers** are a future threat to cyber security, engineered to leverage quantum physics in a way that can solve some computational problems much faster than current computers, making current cryptography methods obsolete.[108] While powerful enough quantum computers capable of decrypting all of today's encryption have yet to be developed and are not projected until the next decade, threat actors could store current encrypted information to decrypt in the future.

104 Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, 2016.
105 CSIS, NSICOP appearance, June 13, 2024.
106 ***
107 Canadian Centre for Cyber Security, "Baseline cyber threat assessment: Cybercrime," August 2023; and FBI, "A Primer on DarkNet Marketplaces," November 2016.
108 CSE, "CSE Comments on NSICOP's Draft Lawful Access Report," December 20, 2024.

## The Impact of New Technologies on National Security Investigations

**63.** According to CSIS, the biggest impediment to fulfilling its mandate "in terms of its ability to detect and mitigate threats is the rapid technological change that is outpacing our authorities and our tools."[109] Both CSIS and the RCMP state that traditional interception techniques used to collect communications have become less useful as encryption has become more widespread, helping threat actors avoid discovery, investigation and prosecution ***.[110] CSIS and the RCMP state that these technologies have challenged investigations linked to terrorism, espionage, foreign interference, and organized crime.[111]

**64.** Neither CSIS nor the RCMP systematically collect data on how many national security investigations encountered encryption. One exception is an older RCMP study about the technological challenges to obtaining judicially authorized digital evidence in 57 major Federal Policing investigations active in 2014, of which 25 were national security investigations. All investigations encountered technological challenges to acquiring judicially authorized evidence. However, none were shut down as a result. ***[112] The RCMP has not completed further studies of this kind since then. In an appearance before the Committee, CSIS noted the difficulty of quantifying successes and failures in overcoming encryption challenges, while Public Safety advised that security organizations are "really good at finding workarounds."[113]

**65.** CSIS also states that while new technologies and new types of data present opportunities for collecting intelligence, the challenges outweigh the benefits as there are too many apps and types of devices to keep up.[114] ***.[115]

109 CSIS, NSICOP appearance, June 13, 2024.
110 CSIS, "Summary of Workshop on Intercept Capability and Encryption," undated; CSIS, NSICOP appearance, May 28, 2024; and RCMP, NSICOP appearance, May 30, 2024.
111 CSIS, NSICOP appearance, June 13, 2024.
112 ***
113 PS and CSIS, NSICOP appearance, November 5, 2024.
114 CSIS, NSICOP appearance, June 13, 2024.
115 CSIS, NSICOP appearance, April 18, 2024.

### Case study: ***

***116 ***117 ***

To investigate this threat to the security of Canada under section 12 of the CSIS Act, CSIS obtained several successive warrants under section 21 of the Act. ***[118]

***119 ***120

***121 ***122 ***

***123 ***124

**66.** As national security targets opt for end-to-end encryption applications and virtual private networks to conceal their activities, the RCMP and CSIS told the Committee that ***, and that this difficulty is compounded by recent judicial decisions.[125] CSIS and the RCMP rely on BSI to determine who is behind a digital identifier (i.e., an IP address) in order to investigate possible threats. As noted in Chapter 2, after the Supreme Court's 2014 decision in *Spencer* that security agencies required judicial authorization to seek BSI, CSIS and the RCMP need to take additional steps to access what they considered to be building block information required for the early stage of an investigation. According to CSIS, the requirement for judicial authorization for this kind of information results in delays and significant effort for CSIS to investigate a potential threat, particularly as it is seeking to rule individuals out to enable investigators to focus on the right threat actors. Canada's Five Eyes partners do not require judicial authorization to obtain BSI.[126]

**67.** The RCMP claims that it is also challenged to make the most of the metadata it has seized, noting that the huge volume of data associated with metadata, most of which is not relevant, can overwhelm investigators.[127] Additionally, there is no legal requirement for CSPs to retain certain metadata for a set period of time.[128] Consequently, while the RCMP or CSIS could seek a preservation order to compel a provider to preserve specified data, investigators may find that the provider has already deleted the data before receiving the order due to the

116 ***
117 CSIS, *2023-2024 Annual s. 6(4) Report to the Minister on CSIS Operational Activities*, 2024.
118 CSIS, Response to RFI #4, November 13, 2024.
119 CSIS, Briefing to NSICOP Secretariat, December 10, 2024; and CSIS, Factual accuracy check of the case study, provided to NSICOP at its request on January 8, 2024.
120 CSIS, Briefing to NSICOP Secretariat, December 10, 2024.
121 CSIS, Briefing to NSICOP Secretariat, December 10, 2024.
122 Michael Geist, "Lawful Interception of Communication by Security and Intelligence Organization: The Policy and Legal Challenges Posed by Real-Time Messaging on Internet Platforms," NSICOP Commissioned Paper, May 2024.
123 CSIS, *2023-2024 Annual s. 6(4) Report to the Minister on CSIS Operational Activities*, 2024.
124 ***
125 CSIS, NSICOP appearance, May 28, 2024.
126 CSIS, NSICOP appearance, May 28, 2024.
127 RCMP, NSICOP appearance, June 13, 2024. See also NSICOP, *Special Report on the Federal Policing Mandate of the Royal Canadian Mounted Police*, Chapter 6, 2023; and CSIS, "Summary of Workshop on Intercept Capability and Encryption," undated.
128 DoJ, NSICOP appearance, November 7, 2024; and Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016: Background Document*, 2016.

provider's own data management policies. According to the RCMP, the absence of a data retention regime has significant implications given some complex investigations run for years, while other investigations may start years after the data was initially created.[129]

> ***Data retention*** refers to a general legal requirement on CSPs to retain certain metadata for a specified period of time. Canada does not have any such laws.[130]
>
> ***Data preservation*** refers to the existing provisions in the CSIS Act and *Criminal Code* that allow investigators to compel a person or entity to preserve data they would have otherwise deleted (i.e., per usual business practice or policy). Preservation demands and orders are issued so data is preserved with a view to the investigator obtaining a warrant or production order to obtain the data itself. In the *Criminal Code*, a preservation demand allows a RCMP officer to compel preservation without judicial authorization.[131] There is no preservation demand in the CSIS Act. Preservation orders, which are found in the CSIS Act[132] and the *Criminal Code*[133], require judicial authorization.

**68.** Privacy advocates maintain that metadata represents a source of valuable, often unencrypted information for investigators that may have been underutilized.[134] According to the Citizen Lab, CSIS and RCMP are not "going dark," rather they are experiencing "investigative friction," a situation in which increased "expertise, cost, or ingenuity" is required in the investigation of threats to national security.[135] Privacy advocates also point out that large pools of potentially revealing personal data are now harvested by private sector organizations as part of general "commercial surveillance,"[136] offering an opportunity for security and intelligence agencies to collect information. They argue that "[f]ar from 'going dark,' more information is available about individuals' private lives today than in any other moment in human history."[137]

**69.** CSIS counters that it is unable to access or collect this data given Canada's current technological and legislative limits. The commercial entities collecting this data are primarily located outside of Canada (jurisdictional barriers are discussed later in this chapter).[138] CSIS also notes that information available to anyone else on the Internet, such as IP addresses, cannot be collected by the state without judicial authorization due to Supreme Court decisions in *Spencer* and *Bykovets*.[139]

129 RCMP, "Lawful Access in Canada: Examining the challenges of lawfully accessing communications data in a digital world," draft, 2023.
130 Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, 2016.
131 *Criminal Code*, RSC 1985, c C-46, s 487.012.
132 CSIS Act, RSC 1985, c C-23, s 20.3.
133 *Criminal Code*, RSC 1985, c C-46, s 487.013.
134 Lex Gill, Tamir Israel, and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.
135 Lex Gill, Tamir Israel, and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.
136 BCCLA, NSICOP appearance, October 1, 2024.
137 Lex Gill, Tamir Israel, and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.
138 CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.
139 CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.

**70.** Privacy experts also state that security agencies overstate their constraints:

> [D]igital storage is so cheap today that any data collected for any investigative purpose can be retained indefinitely from a cost perspective. Moreover, digital tools such as voice recognition, machine translation, and analytics powered by artificial intelligence provide government agencies with automated tools to sift through reams of intercepted digital data, and identify items of interest that require further analysis by their personnel.[140]

**71.** CSIS counters that the reality is more complicated, noting that it has strict restrictions in its warrants detailing retention periods for data collected (i.e., CSIS is unable to indefinitely retain data) and requirements for data to be reviewed by designated CSIS employees (i.e., not via an automated program).[141]

**72.** In reflecting on the origin of the 2011 argument that governments were enjoying a "golden age of surveillance," CSIS notes that at the time, Internet-based communications were more vulnerable than traditional phone calls, unless encryption was used and, that even then, law enforcement reported the ability to retrieve readable communications in the relatively few times it faced this challenge.[142] CSIS states that this situation has shifted significantly with the majority of Internet traffic now being encrypted by default ***.[143]

140 Vivek Krishnamurthy, "Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws Fit for Purpose?" NSICOP Commissioned Paper, December 2023.
141 CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.
142 CSIS, citing Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *Columbia Science and Technology Law Review*, *Vol. 23, 2012*, November 17, 2011.
143 CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.

## Mitigating the Challenges of New Technologies in the National Security Environment

**73.** According to CSIS and the RCMP, mitigating technological challenges requires activities that are resource intensive and present higher operational risk.[144] ***[145]

**74.** Efforts to mitigate technological challenges include growing investments in *** intelligence collection capabilities and human source operations to collect information on warranted subjects of investigation.[146] Mitigation also includes more "high risk, high effort, and costly *** operations ***."[147] ***[148]

*Computer Network Exploitation and the Use of On-Device Investigative Tools*

**75.** One of the primary methods used by CSIS and the RCMP to bypass the challenge posed by encryption technologies in the period under review was computer network exploitation (CNE).[149] CNE refers to tools and techniques that exploit vulnerabilities in systems or software to surreptitiously obtain data that is stored on or transiting communications networks.*** The RCMP uses the term "On-Device Investigative Tool (ODIT)" to describe its CNE tools.[151] An ODIT is "a computer program as defined in s. 342.1(2) of the *Criminal Code* that is installed on a targeted computing device that enables the collection of electronic evidence from the device."[152] ***

> *** It is however one of the most complex and expensive technical collection programs we maintain.[153]

**76.** Where sufficient vulnerabilities can be identified, CNE enables *** the RCMP to collect information directly from a subject's smartphone or computer and can allow investigators access to not only the subject's cellular phone calls or texts, but *** the subject's emails, encrypted messages, ***.[154] CNE can also allow investigators to turn on the microphone or camera of a subject's phone.[155] The case study below describes an example of an investigation in which the RCMP successfully deployed ODITs in response to a national security threat.

144 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
145 ***
146 CSIS, NSICOP appearance, May 28, 2024.
147 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024; and CSIS, NSICOP appearance, May 28, 2024.
148 CSIS, NSICOP appearance, May 28, 2024.
149 RCMP Commissioner quoted in ETHI, *Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues*, November 2022; and CSIS, NSICOP appearance, May 28, 2024.
150 ***
151 RCMP, "Government Response to Inquiry of Ministry Q-566," May 6, 2022.
152 RCMP, "On-Device Investigative Tool (ODIT) Technical Description: Draft for Project," August 2022.
153 ***
154 ***
155 ***

### Case study: RCMP Project SALENTO

***, the U.S. Federal Bureau of Investigation (FBI) provided the RCMP with intelligence about a Canadian (the subject) ***[156] ***[157]. The RCMP investigated the subject throughout 2018 in a criminal investigation called Project SALENTO.[158] ***[159]

*** the subject: ***[160] who was reportedly building a bomb with the intent of committing a terrorist act in Canada, targeting a New Year's celebration on December 31st. ***[161]

In response, the RCMP took numerous investigative steps, including the deployment of ODITs on the devices of the subject and ***. The ODITs revealed text messages and schematics for a pressure cooker bomb.[162]

On January 24, 2019, the RCMP arrested *** in Kingston, Ontario.[163] *** was ultimately charged with four terrorism offences to which he pleaded guilty on July 28, 2020.[164]

Evidence collected by the ODITs supported the charges laid. According to the RCMP, the successful use of ODITs in Project SALENTO can be attributed to several key factors. First, the RCMP had an existing capability to deploy an ODIT on the make and model of phone used by the subject and ***, which is not always the case.[165] ***

**77.** While both CSIS and RCMP use CNE tools in national security investigations, CSE plays a leading role in the management of CNE policy and implementation for the government. Specifically, CSE manages the exploitation of system and software vulnerabilities, also known as "equities," through an Equities Management Framework. The Equities Management Framework provides "a standardized decision-making process in which CSE experts consider all available information to responsibly manage equities associated with an identified vulnerability in an information system or technology in a way that puts the security interests of Canada and Canadians first."[166] CSIS and the RCMP are members of the Equities Review Board as part of the Equities Management Framework. ***[167]

156 ***
157 ***
158 The RCMP refers to major criminal investigations as projects.
159 ***
160 ***
161 ***
162 See, for example, the RCMP's two Intercept Room Supplementary Reports dated January 2, 2019 (reports # 00006710 and 00006711), and the RCMP file named "Images captured by ODIT – 00014169".
163 Canadian Broadcasting Corporation, "RCMP charge Kingston, Ont. youth with terror-related offence after security probe," January 25, 2019; and PPSC, "Young Person Pleads Guilty to Four Terrorism Offences," July 28, 2020.
164 PPSC, "Young Person Pleads Guilty to Four Terrorism Offences," July 28, 2020.
165 RCMP, Briefing to NSICOP Secretariat, November 27, 2024.
166 ***
167 ***

**78.** For both CSIS and the RCMP, seeking judicial authorization for the use of CNE can be complex depending on what the activity seeks to do. The RCMP requires several authorizations, including a wiretap if using an ODIT to intercept private communications, as well as a general warrant and a transmission data recorder warrant.[168] ***[169] ***[170] ***[171]

**79.** CSIS states that there are several privacy safeguards contained within the warrants authorizing the installation and use of ODITs, as well as within its internal policies, ***[172] ***[173] ***[174]

**80.** According to CSIS, in 2018 it began providing the Federal Court an explanation of how CSIS' ODITs function and the various methods by which they are deployed with every warrant application so that all designated judges were "provided with consistent information about the ODIT-related powers that they would be authorizing."[175]

**81.** Warrants granted to the RCMP for the deployment of ODITs to intercept private communications also include privacy safeguards. The issuing judge may attach terms and conditions to a wiretap authorization,[176] such as limits on topics and categories that may be searched in the data extracted from the device, or requirements to destroy collected data that falls outside the authorized time period or cease examination of data that does not relate to a target.[177]

**82.** *** the RCMP deploy CNE in three different ways, ***:[178]

1. *Remote access CNE*: ***
2. *Near access CNE*: ***[179]
3. *Close access CNE* ***: ***[180]

**83.** CNE is not a panacea. CNE relies on exploiting vulnerabilities ***. In recent years the number of devices and apps has increased the cost and complexity of CNE as operators need to search more devices and apps for vulnerabilities.[181] ***[182] ***[183]

168 RCMP, "On-Device Investigative Tool (ODIT) Technical Description: Draft for Project," August 2022.
169 ***
170 ***
171 ***
172 CSIS, Response to "Inconsistencies between CSIS RFI #4 Response (Nov. 14/24) and CSIS Factual Accuracy Response (Dec. 20, 2024)," January 6, 2024.
173 *** CSIS, Response to "Inconsistencies between CSIS RFI #4 Response (Nov. 14/24) and CSIS Factual Accuracy Response (Dec. 20, 2024)," January 6, 2024.
174 CSIS, "CSIS Response to NSICOP RFI #4 on Lawful Access," November 13, 2024.
175 CSIS, "CSIS Response to NSICOP RFI #4 on Lawful Access," November 13, 2024; CSIS, "CSIS' factual accuracy response to the NSICOP Lawful Access (Going Dark) DRAFT review," December 20, 2024.
176 *Criminal Code*, RSC 1985, c C-46, s 186(3) or s 186(4)(d).
177 Court of Ontario Superior Court of Justice, "Authorization to intercept communications, make observations, and related orders and warrants," January 3, 2019.
178 ***
179 ***
180 ***
181 RCMP, NSICOP appearance, May 30, 2024.
182 ***
183 ***

**84.** ***[184]

**85.** ***[185] ***[186] ***

***[187]

**86.** In 2022, the RCMP advised the Standing Committee on Access to Information, Privacy and Ethics (ETHI) that since 2017 it had used ODITs in 32 investigations, targeting 49 devices.[188] Since then, the RCMP made 8 attempts at deploying an ODIT in 2023, of which only two were successful. The RCMP did not deploy any ODITs in 2024.[189] The RCMP similarly advised that increased cybersecurity awareness in recent years has led to a significant decline in their overall ODIT success rate.[190] Table 3.2 summarizes the number of ODITs deployed by the RCMP since 2017.

**Table 3.2: RCMP ODIT Use, 2017-2024[191]**

| YEAR | NUMBER OF TARGETED DEVICES | SUCCESSFUL DEPLOYMENTS |
|---|---|---|
| 2017 | 2 | 2 |
| 2018 | 3 | 3 |
| 2019 | 2 | 2 |
| 2020 | 15 | 8 |
| 2021 | 16 | 9 |
| 2022 | 11 | 7 |
| 2023 | 8 | 2 |
| 2024 | 0 | 0 |

For both CSIS and the RCMP, the Committee understands a successful ODIT deployment to be that an ODIT collected information from the targeted device and generated a report, ***[192]

184 CSIS, ***
185 *** CSIS, "CSIS Response to NSICOP RFI #4 on Lawful Access," November 13, 2024.
186 CSIS, "CSIS Response to NSICOP RFI #4 on Lawful Access," November 13, 2024.
187 ***
188 RCMP, *Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP*, August 2022.
189 RCMP, "RCMP Response to NSICOP's Review of the Lawful Access to Communications by Security and Intelligence Organizations (RFI #05)," November 14, 2024.
190 CSIS, NSICOP appearance, June 13, 2024; and RCMP, NSICOP appearance, May 30, 2024.
191 RCMP, "RFI #7 Chart," December 18, 2024. The RCMP noted that generally it does not attempt to deploy an ODIT unless it believes the deployment will be technically successful, which suggests a lower rate of success. RCMP, "RE: [NEW RFI] NSICOP lawful access report – verification request," February 4, 2025.
192 CSIS, "RE: [NEW RFI] NSICOP lawful access report – request for further details & clarification," February 3, 2025; RCMP, "RE: [NEW RFI] NSICOP lawful access report – verification request," February 4, 2025; and, RCMP, "RE: Heads up on incoming time-sensitive consultation request / fact-check," February 6, 2025.

*Challenges Associated with the Protection of Investigative Techniques*

**87.** The RCMP states that it is faces other acute challenges which make it increasingly difficult for investigators to use ODITs. As described in Chapter 2, during a prosecution, the Crown is obligated to disclose all relevant and material information, except that which is privileged, to the defence so that accused persons may make full answer and defence to any charges brought against them.[193] Under the *Canada Evidence Act*, the government can seek to prevent the disclosure of information relating to a sensitive law enforcement investigative tool or technique under section 37 and withhold access to information that is sensitive or injurious to Canada's international relations, national defence or national security, including tools and techniques used by security and intelligence organizations, under section 38. According to the RCMP, although these provisions can be easily applied to certain traditional investigative tools and techniques, the complexity of going through this process with ODITs within acceptable timelines is challenging.[194]

**88.** The RCMP states that it would like to rely on CSE through requests for assistance for ODIT deployment, due to the significant cost and resources required to use ODITs.[195] ***[196] If a particular tool or technical capability were made public in a court disclosure, it could affect other investigations underway.[197] The RCMP states that, consequently, CSE *** "increasingly unable, or unwilling to aid the RCMP out of concern that these tools are subject to disclosure in court."[198] According to CSE, there is insufficient confidence that the Crown will be able to protect classified CNE capabilities in legal proceedings: "Using any of these capabilities as part of assistance to RCMP, with a not insignificant likelihood of them being exposed as part of legal proceedings, presents an unacceptable risk to CSE, to its operations and reputation, ***[199]

**89.** The RCMP contends that this puts the RCMP position where they "must choose between 'burning a tool' ***, and staying the charges due to a lack of disclosure." [200]

**90.** ***[201] ***[202]

**91.** According to the RCMP, concerns about disclosure have also forced Public Prosecution Service of Canada (PPSC) to stay charges, as the preparation to apply for protection under section 37 or 38 is so complex that the resulting delays are long enough to infringe on the accused's right to be tried within a reasonable time.[203] ***[204]

**92.** National security law expert and defence counsel, Anil Kapoor, advised the Committee that the prosecution of criminal cases did not always represent "the most effective way to manage national security threats," due to their cost, the length of time involved, and the risk of the

193 *R v Stinchcombe*, [1991] 3 S.C.R. 326.
194 In *R v Jordan*, the Supreme Court established clear time limits for the completion of criminal trials. If a trial exceeds these time limits without reasonable cause, the charges may be stayed. *R v Jordan*, 2016 SCC 27, [2016] 1 S.C.R. 631.
195 RCMP, "RCMP factual accuracy submission -- NSICOP Lawful Access Draft Report," December 20, 2024.
196 ***
197 CSE, NSICOP appearance, May 30, 2024.
198 ***
199 ***
200 RCMP, "RCMP factual accuracy submission -- NSICOP Lawful Access Draft Report," December 20, 2024.
201 ***
202 ***
203 RCMP, "RCMP factual accuracy submission -- NSICOP Lawful Access Draft Report," December 20, 2024.
204 ***

"disclosure of information which the agencies would wish to protect."[205] However, he stated that, "when intelligence assets are at risk and the interest of the accused or constitutional imperatives may require disclosure, … that is the nature of criminal law proceedings and we shouldn't be afraid of that or think that is somehow improper. It is entirely proper."[206] According to Mr. Kapoor,

> …current existing law provides a proper and well-balanced approach to the protection of information while protecting against the risk that innocent persons will be convicted. The problem, respectfully, is a cultural problem, and it is a concern that agencies may be too risk-averse, in taking decisions on how to manage a particular threat, and in particular, the use of criminal proceedings.[207]

**93.** Mr. Kapoor suggests that agencies like CSIS and CSE may have an insufficient understanding of the extent to which the law can protect their sensitive information at trial.[208] Of note, in 2019 Mr. Kapoor authored a classified Operational Improvement Review, at the request of CSIS and the RCMP, which examined the Federal Court's section 38 decisions from 2008 to 2018 relating to national security-related prosecutions.[209] The review found that the government had used section 38 to successfully protect sensitive information from disclosure in more than 85% of national security criminal cases, particularly information derived from international partners.[210] The review concluded that there was nothing about the section 38 process or test that necessarily led to the improper release of sensitive information.[211] The review, however, did not conduct a similar analysis on section 37.

*Other Challenges Working with ODITs*

**94.** *** Unlike the U.S., Canada does not have a clear policy that sets out guidance on what kinds of commercial ODITs may be approved for purchase and use by government investigative agencies.[212]

**95.** Privacy advocates, as well as legal and cybersecurity experts, are highly critical of the use of CNE given the significant amount of private and personal information people have about themselves and others on their digital devices. In the context of Canada's legal framework, they argue that CNE blurs the distinction between the prospective interception of communications and the retrospective retrieval of stored communications because the same tool may be used to accomplish both. They argue that current *Criminal Code* and CSIS Act provisions do not adequately address the degree of invasion of privacy that certain CNE capabilities pose such as the ability to "access all of an individual's stored data

205 Anil K. Kapoor, NSICOP appearance, October 3, 2024.
206 Anil K. Kapoor, NSICOP appearance, October 3, 2024.
207 Anil K. Kapoor, NSICOP appearance, October 3, 2024.
208 Anil K. Kapoor, NSICOP appearance, October 3, 2024.
209 The prosecutions involved seven accused persons and resulted from the following five RCMP national security criminal investigations (the RCMP refers to any major criminal investigation as a project): Project Souvenir (*R v Nuttall*), Project Smooth (*R v Esseghaier and Jaser*), Project Slype (*R v Ader*), Project Servant (*R v Peshdary*), and Project Samossa (*R v Alizedeh and Ahmed*). Anil K. Kapoor and Dana C. Achtemichuk, *Operational Improvement Review*, 2019. Four of the accused were found guilty of terrorism offences at trial; two pled guilty; and one was found not-guilty. Craig Forcese and Kent Roach, *False Security: The radicalization of Canadian anti-terrorism*, 2015; Michael Nesbitt and Harman Nijjar, "Counting Terrorism Charges and Prosecutions in Canada Part 1: What does the data say?" A blog called Intrepid, June 17, 2021; and PPSC, "2021 Transition Book for the Attorney General of Canada," "Annex 1: National Security Prosecutions Case Summaries—Ongoing Terrorism-related Prosecutions," February 17, 2022.
210 Anil K. Kapoor, NSICOP Appearance, October 3, 2024.
211 Anil K. Kapoor and Dana C. Achtemichuk, *Operational Improvement Review*, 2019.
212 *** White House, "Executive Order on Prohibition of use by the United States Government of Commercial Spyware that Poses Risks to National Security," March 27, 2023.

– whether it is stored on the device itself, or accessible via a cloud computing service to which the device is connected."[213] They also state that the complex and convoluted warrant application processes undermines transparency and accountability.[214] The BCCLA called for "a more robust set of statutory factors" to guide ODIT use by security and law enforcement organizations and provide transparency to Canadians about when courts might grant such a warrant. It also suggested a requirement to notify those investigated with an ODIT after an investigation, similar to the requirement for Part VI intercepts, so they could seek a remedy from the courts for any impropriety on the part of the investigating agency.[215]

**96.** The Citizen Lab warns against the risks posed by the absence of state regulation of commercially available ODITs, which allows the industry to operate without effective public or government oversight: "The existence of this unregulated market has provided a growing number of countries – including countries hostile to Canada or with a history of human rights abuses – access to highly intrusive surveillance technology." [216] Advocates may also assume that Canadian security organizations are using commercially available ODITs, arguing that the "characteristic secrecy of the spyware industry and its use by the government represents a significant barrier to any meaningful accountability in Canada."[217]

**97.** Some likeminded democracies have taken steps to update laws and regulations to better reflect modern technology and transparently share surveillance capabilities with the public. In 2017, Germany amended its *Code of Criminal Procedure* to better reflect modern law enforcement, amending provisions authorizing the retrieval of encrypted communications stored on an online device; law enforcement's access to information technology systems to gather stored data; and the use of CNE to remotely activate an electronic device's microphone and camera as a mode of surveillance.[218] In 2016, the U.K. publicly released its *Equipment Interference Code of Practice* for U.K. law enforcement and security agencies on how to lawfully conduct CNE. The *Code of Practice* includes guidance on the need to demonstrate the necessity and proportionality of activities, establishes rules for the handling of information, and outlines safeguards for oversight, such as obtaining authorization from the Secretary of State and review by the Intelligence Service Commissioner.[219]

**98.** CSIS states that it does not believe a dedicated ODIT warrant is required due to the Federal Court's awareness that "ODITs carry a high level of intrusiveness and [the Federal Court] balances privacy interests by imposing conditions within the warrants authorizing ODIT installation and use."[220] According to the RCMP, the current provisions of the *Criminal Code*

213 Vivek Krishnamurthy, "Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws Fit for Purpose?" NSICOP Commissioned Paper, December 2023.
214 Vivek Krishnamurthy, "Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws fit for Purpose?" NSICOP Commissioned Paper, December 2023.
215 BCCLA, NSICOP appearance, October 1, 2024.
216 Siena Anstis, Ronald J. Deibert, Camila Franco, and Zoe Panday, "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," June 30, 2023.
217 Siena Anstis, Ronald J. Deibert, Camila Franco, and Zoe Panday, "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," June 30, 2023.
218 Vivek Krishnamurthy, "Communications Interception and Digital Searches in an Age of Encryption and Spyware: Are Canada's Laws Fit for Purpose?," NSICOP Commissioned Paper, December 2023.
219 U.K. Home Office, "Equipment Interference Code of Practice Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000," January 2016.
220 CSIS, "CSIS Response to NSICOP RFI #4 on Lawful Access," November 13, 2024.

are adequate and in keeping with RCMP needs, although it welcomed any added simplicity in obtaining judicial authorization for the deployment of an ODIT.[221] According to Public Safety, ODITs are an area it intends to analyze in greater detail.[222]

## Requests for Assistance from CSE

**99.** Another option for CSIS and the RCMP to respond to technological challenges is to seek help through a formal RFA from CSE, ***[223] ***

**Table 3.3: Types of Requests for Assistance to CSE[224]**

| TYPE OF REQUEST FOR ASSISTANCE (RFA) | DESCRIPTION |
|---|---|

***

**100.** Between 2012 and 2023, CSE completed *** RFAs for the two investigative agencies: *** for CSIS and *** for the RCMP (see Figures 3.2 and 3.3 below). Both CSE and RCMP attribute the *** fewer RFAs to the RCMP because of the risk of investigative techniques being subject to disclosure in court, as noted above, or because the RCMP opted not to move forward with CSE assistance after finding another solution.[225] That said, both CSE and RCMP have increasingly sought ways for CSE to support the RCMP in the "unclassified realm,"[226] such as RCMP leveraging CSE's ***:

***[227]

***[228]

**Figure 3.2: CSIS Requests for Assistance to CSE: Trends & Statistics[229]**

***

**Figure 3.3: RCMP Requests for Assistance to CSE: Trends & Statistics[230]**

***

221 RCMP, "RCMP Response to NSICOP's Review of the Lawful Access to Communications by Security and Intelligence Organizations (RFI #05)," November 14, 2024.
222 Public Safety, "NSICOP Lawful Access RFI #3 to Public Safety," November 15, 2024.
223 CSE, NSICOP appearance, May 28, 2024.
224 ***
225 CSE, NSICOP appearance, May 28, 2024; CSE, NSICOP appearance, May 30, 2024; and ***.
226 CSE, NSICOP appearance, May 30, 2024.
227 ***
228 CSE, NSICOP appearance, May 28, 2024.
229 ***
230 ***

## Absence of Legislation for Intercept Capability

**101.** As described in Chapter 2, intercept capability refers to the tools built into a telecommunications network or service that allow a CSP to intercept communications and other data and provide them to law enforcement or intelligence agencies in response to a warrant. Canadian law does not require CSPs to develop, deploy, or maintain their telecommunications systems to enable interception of communications and related data. In other words, while judicial authorization can compel a CSP to provide information, it cannot compel a CSP to provide technical connectivity to law enforcement and security agencies.[231] According to the RCMP, without a legislative framework, "lawful access processes and capabilities are not standardized and vary greatly."[232]

## How Security Organizations Intercept Communications

**102.** ***[233] According to the RCMP, lawful access tools and equipment do not introduce any changes to the network itself; rather these tools are designed to capture data that is either already collected and stored by the CSP as part of their day-to-day business activities or accessible to the CSP by virtue of the type of service provided, such as Internet services.[234]

**103.** Data is segregated to ensure that a requesting agency only receives the data it is lawfully authorized to see.[235] ***[236] ***

***[237] ***

**104.** Intercept capability does not provide exceptional access, or a "backdoor," to encrypted content. In a system that is intercept capable, the RCMP or CSIS can obtain or intercept the communications from a CSP's network, but that does not necessarily mean that they are able to read it, as encryption often makes content undecipherable. Some cybersecurity experts and privacy advocates, however, view lawful intercept capability in and of itself as a "backdoor."

### Intercept capability and "backdoors"

Policy debates about how to respond to the challenge of encryption have included proposals that the government could require companies to create exceptional access to encryption programs, or **backdoors**, for security and intelligence organizations. CCCS defines a backdoor as an "undocumented, private, or less detectable-way of gaining remote access to a computer, bypassing authentication measures, and obtaining access to plaintext."[238]

The Citizen Lab states, "[o]nce a backdoor is created, there is no practical guarantee that only state agencies will walk through it. This fundamental flaw makes exceptional access

231 RCMP, NSICOP Site Visit, September 26, 2024.
232 RCMP, International Comparison of Lawful Access Coordination and Funding Models, draft, 2023.
233 RCMP, "RCMP factual accuracy submission -- NSICOP Lawful Access Draft Report," December 20, 2024.
234 RCMP, "RCMP's Response to NSICOP's Review of the lawful access to communications by security and intelligence organizations (RFI) #4," October 18, 2024.
235 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
236 ***
237 ***
238 CCCS, "Glossary," undated.

systems an inherent threat to persons who rely on encrypted communications products."[239] This view is echoed by many cybersecurity experts.[240]

CSE told the Committee that it also has a concern with backdoors. While it noted that "there are means of creating technical solutions which are currently considered secure," [241] it stated that it would have a concern with legislation compelling CSPs or software providers to implement backdoors, which could compromise the cybersecurity more generally.[242]

According to the RCMP, backdoors "create vulnerabilities and can weaken the overall security of a network; they create valid security concerns given the potential for these vulnerabilities to be exploited by criminals or other hostile actors. Recognizing the need to protect sensitive information and maintain individuals' right to privacy, the RCMP does not advocate for the creation of 'backdoors' into CSPs' networks. Instead, it would be safer and more beneficial for law enforcement and national security agencies to be able to leverage the information already accessible by CSPs."[243]

Some cybersecurity experts and privacy advocates, however, consider lawful intercept capability a backdoor, citing that there is "no such thing as a security backdoor that is only for the 'good guys.'"[244] Others similarly contend that while it might be argued that "surveillance technology can be built securely and without risk of penetration by hostile forces," the "track record is not encouraging."[245]

Neither CSIS or RCMP view intercept capability as a backdoor, because it does not compromise encryption platforms or software. They instead regard the judicially authorized practice of using tools built into a CSP's system, which are encryption neutral, as using the "front door."

**105.** In the absence of legislation for intercept capability, CSIS and the RCMP rely on *** cooperation of CSPs to build and maintain intercept capability. Funding is required to develop and implement intercept solutions, ***[246] CSIS and the RCMP pay the majority of these costs – which also benefit provincial and municipal police agencies – without a formal mandate to do so.[247] In 2022, CSIS and the RCMP spent a combined $*** in development and maintenance, and a combined total of $*** in operational costs billed by the CSPs to national security and law enforcement agencies across Canada.[248]

239 Lex Gill, Tamir Israel, and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.
240 Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, "Keys under doormats: Mandating insecurity by requiring government access to all data and communications," Massachusetts Institute of Technology Press, July 6, 2015; and Susan Landau, "CALEA Was a National Security Disaster Waiting to Happen," Lawfare, November 13, 2024.
241 CSE, "CSE Comments on NSICOP's Draft Lawful Access Report," December 20, 2024.
242 CSE, NSICOP appearance, May 30, 2024.
243 RCMP, "RCMP factual accuracy submission -- NSICOP Lawful Access Draft Report," December 20, 2024.
244 Lawfare, citing the Electronic Frontier Foundation and TechCrunch, "How Telegram Turbocharges Organized Crime," October 11, 2024.
245 Susan Landau, "CALEA Was a National Security Disaster Waiting to Happen," Lawfare, November 13, 2024.
246 ***
247 RCMP, NSICOP appearance, May 30, 2024.
248 CSIS and the RCMP, "Lawful Access Requests and Funding," undated.

**106.** According to CSIS and the RCMP, only ***% of CSP networks in Canada have a technical solution in place to allow for the lawfully authorized interception of communications and related data, and thus would be considered intercept capable, as shown in Table 3.4. The table does not, however, account for differences in the size of networks (i.e., not all networks are equal in terms of market share and users). According to the Canadian Radio-television and Telecommunications Commission, Canada's five largest CSPs make up more than 87 percent of revenue share.[249] ***

**Table 3.4: Summary of Lawful Interception Capabilities[250]**

| | | | NUMBER OF INDIVIDUALLY OPERATED NETWORKS (SERVICES) | | |
|---|---|---|---|---|---|
| Service Category | Number of CSPs | Total Number of networks | Lawful Intercept Capable | Partially Capable or Under Developed | Lawful Intercept Gap |
| | | *** | | | |

## Impact of the Absence of a Legal Framework for Intercept Capability

**107.** According to CSIS and the RCMP, the absence of intercept capability legislation and an outdated legal framework have operational, financial, and policy consequences. First, there is no formal, central authority to set standards or establish priorities. This leaves CSPs to triage multiple requests from CSIS, the RCMP, and provincial or municipal police departments and determine their level of priority.[251] In the absence of standards for lawful access technology, CSPs choose the technology they deem appropriate, which requires CSIS and the RCMP to tailor individual lawful intercept solutions to each CSP's infrastructure, which are not easily transferable to other CSPs.[252]

**108.** The absence of a formal framework to regulate technical upgrades leaves the government with little ability to control costs. ***[253] ***[254]

**109.** Second, there is no established compensation framework determining who is responsible for paying the costs associated with the development and maintenance of intercept capability. The RCMP, CSIS, and CSP representatives all point to inconsistent approaches across the police and intelligence community on compensating CSPs for intercept capability activities and investments. Some compensate CSPs for their cooperation, while others do not, either

249 Canadian Radio-television and Telecommunications Commission, *Annual highlights of the telecommunications sector*, February 2024.
250 ***
251 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
252 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
253 CSIS and RCMP, NSICOP appearance, June 13, 2024.
254 CSIS, "CSIS Examples" (email), May 10, 2017.

because they do not have the resources or in the belief that CSPs have an obligation to support public safety and national security or that these costs, like compliance costs more generally, should be seen as a cost of doing business.[255]

**110.** A primary CSP concern is the absence of a formal compensation framework to regulate the cost of intercept solutions and the cost of processing requests from investigators. One CSP noted that current agreements are contracts "subject to great variation depending on the working conditions between the parties involved. For example, the unilateral decision made by several law enforcement agencies over the years to stop compensating the CSPs for technical assistance, including lawful intercepts … has placed financial pressure on CSPs and broke the tacit agreement that [CSPs] would be able to recover [their] costs to operate the new capacity [they] had agreed to develop."[256] ***[257]

**111.** The RCMP states, "To keep pace with international partners, Canada requires a robust and enduring lawful access framework that introduces legislation, clarifies funding responsibilities, streamlines engagement, and standardizes operations."[258] According to CSIS, the lack of intercept capability legislation "is the single greatest differentiator with our [Five Eyes] partners who all have more success than we do because they have lawful access legislation."[259] The RCMP states the absence of legislation for intercept capability in Canada is regarded as a hindrance ***.

**112.** ***[260]

**113.** For example, *** the FBI provided intelligence to the RCMP about a Canadian subject of interest who was reportedly a long-time supporter of the Islamic State,[261] stockpiling weapons and bomb-making materials, and planning to kidnap a former Canadian soldier to engage the government in hostage negotiations on behalf of the Islamic State.[262] ***[263] *** As discussions about the legality and feasibility of the assistance order took longer than expected, RCMP investigators opted not to pursue an ODIT and instead engaged the subject directly, given public safety concerns.[264] Unlike in the U.K.[265] or Australia[266], Canadian CSPs are not legally required to assist CSIS and the RCMP with CNE.[267]

255 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
256 The Supreme Court of Canada's 2008 decision in *R v Telus* found that CSPs cannot charge police agencies for the production of data pursuant to a court order. A Canadian CSP, NSICOP appearance, June 11, 2024.
257 ***
258 RCMP, International Comparison of Lawful Access Coordination and Funding Models, draft, 2023.
259 CSIS and RCMP, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.
260 CSIS, "CSIS Response to RFI #3: NSICOP Lawful Access Review," October 17, 2024.
261 The Islamic State is a listed terrorist entity under the *Criminal Code*. Public Safety, "Currently listed entities," webpage, June 2021.
262 RCMP, "SPROS ***-570 Operational Plan Approval Request" for Project ***, ***.
263 ***
264 RCMP, Briefing to NSICOP Secretariat, November 27, 2024.
265 *Investigatory Powers Act*, section 253, "Technical capability notices," 2016; U.K. Home Office, "Explanatory Memorandum to The Investigatory Powers (Technical Capability) Regulations 2018," 2017; U.K. Home Office, *Equipment interference code of practice*, 2018; and U.K. Secretary of State, *The Investigatory Powers (Technical Capability) Regulations 2018*, 2018.
266 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, "Part 15—Industry assistance"; Australian Department of Home Affairs, "The Assistance and Access Act: what does the industry assistance framework mean for domestic and international companies?" undated; Australian Department of Home Affairs, "Scenarios – industry assistance to law enforcement and national security agencies," undated; Parliament of the Commonwealth of Australia, Revised explanatory memorandum for TOLA, 2018; and Stilgherrian, *The Encryption Debate in Australia: 2021 Update*, Carnegie Endowment for International Peace, 2021.
267 CSIS, "Not Going Dark: Protecting our collection authorities in a digital world," April 18, 2024.

**114.** CSPs also note that their companies must balance public perception and reputational risk with corporate responsibility in using a voluntary approach to responding to lawful access requests. In their view, legislation that would compel cooperation would mitigate these risks.[268] Public Safety summarizes the operational, financial, and policy consequences of the voluntary approach to lawful access in the Table 3.5 below.

**Table 3.5: Operational, financial, and policy consequences of the voluntary approach to lawful access[269]**

| CURRENT SITUATION | CONSEQUENCE |
|---|---|
| No intercept capable requirement applies to new technologies, and where SOLGEN standards applies, there is still the risk that CSPs will not cooperate. | • Intercept coverage gaps, particularly with new technologies.<br>• Canada lags behind peers. |
| CSIS and the RCMP pay majority of development and maintenance costs, and must individually negotiate costs with CSPs. | • Limited government control over costs.<br>• No standardization of costs between CSPs or agencies, both with respect to when to pay and how much to pay. |
| CSIS and the RCMP are funding intercept solutions for all police agencies, without a mandate for this model. | • The federal government is bearing much of the costs, including for provincial and local law enforcement intercepts. |

***

## Managing the Lack of Legislation for Intercept Capability

**115.** CSIS and the RCMP claim to have mitigated the challenges presented by the voluntary approach to intercept capability by closely coordinating their activities. CSIS and the RCMP sign annual memoranda of understanding in support of intercept capability development, support, and maintenance, and share the costs of CSP service agreements.[270] ***[271] ***[272] ***[273]

**116.** In 2023, CSIS and RCMP informally created the National Lawful Access Centre (NLAC), to serve as the central coordination point for lawful access in Canada for all domestic law enforcement and intelligence agencies.[274] As of November 2024, the government has not yet formally established the NLAC, but it is intended to be responsible for "establishing national lawful access processes and standards; managing common lawful access data

268 Canadian CSP, NSICOP appearance, June 11, 2024.
269 Adapted from Public Safety, NSICOP appearance (presentation deck), April 11, 2024.
270 CSIS and the RCMP, Lawful Access Requests and Funding, undated.
271 ***
272 CSIS, NSICOP appearance, April 18, 2024; and Public Safety, NSICOP appearance, April 11, 2024.
273 CSIS and RCMP, NSICOP appearance, April 18, 2024.
274 RCMP, "National Lawful Access Centre – Unclassified," undated.

collection and network infrastructure technology; and, coordinating with CSPs, all levels of law enforcement, and federal partners on behalf of law enforcement and national security agencies in Canada."[275]

**117.** In 2023, CSIS and the RCMP also created the Lawful Access Advisory Committee (LAAC), which first met in November 2023. The committee is co-chaired by the RCMP and the director of security at a leading CSP, and includes seven leading CSPs. According to CSIS and the RCMP:

> The creation of the LAAC formalizes the intention and dedication of government and private industry alike to work collaboratively to develop long-term solutions to address long-standing lawful access challenges….The LAAC will discuss challenges and explore solutions related to lawful access such as the development of a Canadian lawful access governance framework; the creation of a compensation model for CSP services; the development and integration of new lawful access technical solutions and capabilities; and, the implementation of a national strategy to ensure a common understanding of lawful access across all members of the Canadian lawful access community.[276]

**118.** In its governance framework, the LAAC sets out a number of guiding principles, the first of which identifies privacy as a foundational pillar of lawful access, and the commitment to ensuring lawful access practices "will balance Canadians' safety and security, with privacy and the protection of personal information."[277] The principles also include standardization by default, which means that security agencies and CSPs will seek to standardize their technical solutions and processes. Another key principle includes a commitment to a cost neutral and fair compensation model:

> The lawful access community acknowledges that CSPs are private or semi-private companies and deserve fair compensation for the effort required to develop, maintain, and operate capabilities that is not part of their normal business processes. CSPs will aim to perform lawful access operations based on a cost neutral principle (i.e. they do not financially benefit nor lose money while providing legally authorized support to the requesting agencies). These costs account for the development of technical solutions, the maintenance and operation of these solutions, and other related services.[278]
> According to the CSP co-chair, there has been more cooperation between security agencies and CSPs in the year since the creation of the LAAC than during the entire previous decade.[279]

**119.** Between 2012 and 2024, privacy advocates repeatedly criticized legislative proposals and consultations to create intercept capability legislation on the grounds that the government had not presented sufficient evidence of the problem or failed to accurately estimate the potentially significant projected cost (described further in Chapter 4). More recently, Professor Geist cautions about focusing too narrowly on traditional telecommunications infrastructure when considering modernizing lawful access legislation. He points to the diminished role of CSPs in being able to provide the content of the communications due to the increasing prevalence of end-to-end encrypted over-the-top Internet-based messaging services: "Lawful access policy has long focused on the role of communications

275 RCMP, "National Lawful Access Centre – Unclassified," undated.
276 CSIS and RCMP, "Creation of and Invitation to Participate in the Lawful Access Advisory Committee," August 30, 2023.
277 CSIS and RCMP, "Creation of and Invitation to Participate in the Lawful Access Advisory Committee," August 30, 2023.
278 CSIS and RCMP, "Creation of and Invitation to Participate in the Lawful Access Advisory Committee," August 30, 2023.
279 Canadian CSP, NSICOP appearance, June 11, 2024.

intermediaries such as internet service providers and wireless providers. However, today's reality is such that communication is no longer exclusively mediated primarily through their infrastructure."[280]

**120.** According to the RCMP, new legislation is needed that includes requirements for Canadian CSPs, including "over-the-top applications, satellite service providers, communications service resellers, and certain vehicle manufacturers whose products have integrated communications capabilities."[281]

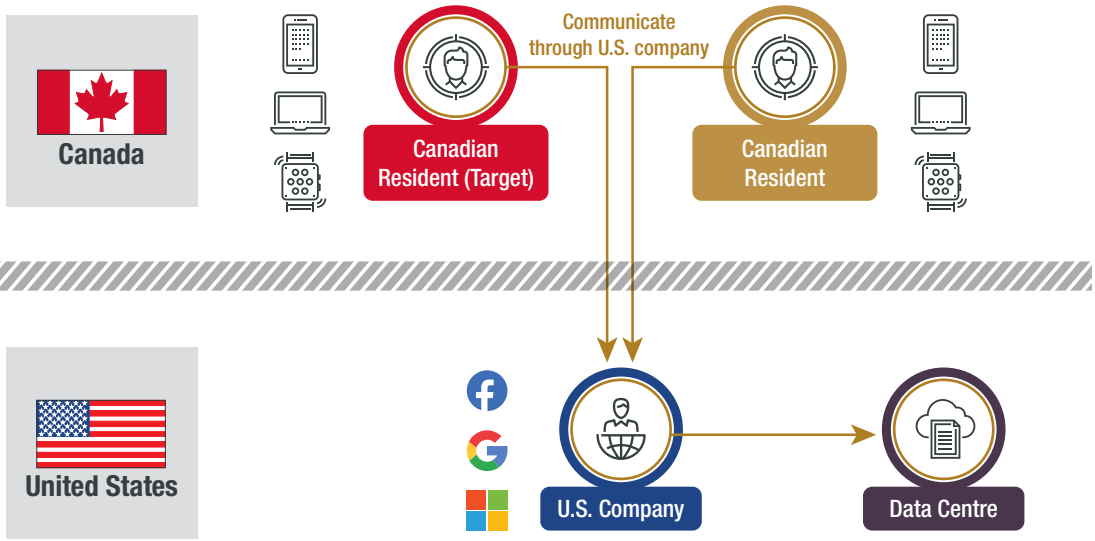
## Cross-border Nature of Digital Data: Impact and Mitigation Activities

**121.** CSIS and the RCMP contend that the global nature of the internet presents significant jurisdictional challenges and delays. Although Internet platforms and real-time communications services have "assumed a critical role in facilitating network-enabled communications services," they are "rarely Canadian-based, deploy varying degrees of encryption, may establish differing standards for law enforcement disclosure, and frequently issue expansive transparency reports." [282]

**122.** Many of the most popular communications services used by Canadians are based in the U.S. (e.g., Google, Facebook, and Apple), as illustrated in Figure 3.5.[283] Under the U.S. *Stored Communications Act*, it is illegal for U.S. companies to disclose the content of communications to foreign authorities unless an order is served on them through the U.S. court system.[284]

280 Michael Geist, "Lawful Interception of Communication by Security and Intelligence Organizations: The Policy and Legal Challenges Posed by Real-Time Messaging on Internet Platforms," NSICOP Commissioned Paper, May 2024.
281 RCMP, "RCMP's Response to NSICOP's Review of the lawful access to communications by security and intelligence organizations (RFI) #4," October 18, 2024.
282 Michael Geist, "Lawful Interception of Communication by Security and Intelligence Organizations: The Policy and Legal Challenges Posed by Real-Time Messaging on Internet Platforms," NSICOP Commissioned Paper, May 2024.
283 Public Safety, "U.S. CLOUD Act: DMNS Presentation," February 22, 2019.
284 CSIS, "The U.S. *CLOUD Act* and Opportunities for CSIS: Executive Brief," undated.

**Figure 3.5: Many popular messaging services used by Canadians are based in the U.S.[285]**




**123.** If digital information is required from a company based outside Canada, the RCMP may request it through a mutual legal assistance treaty (MLAT), where one is in place.[286] For example, if the RCMP requires information from Facebook or Apple, it sends a request to Canada's Department of Justice (DoJ), which sends it to the U.S. Department of Justice. After a request is accepted by the U.S. Department of Justice, an Assistant U.S. Attorney makes an application before a U.S. judge to obtain a warrant for the information. The FBI may execute the warrant after it is issued by the U.S. judge.[287] Once the company provides the FBI with the information, it makes its way back to the RCMP via the two Justice departments. Even if the legal process is successful, if a company does not have a data retention policy, the content sought by an investigator may be deleted before the legal request arrives.[288]

**124.** According to the RCMP, the MLAT process can take three to six months, and that delay can have an impact on investigations.[289] In 2016, the U.S. Department of Justice described the MLAT process as "an important but often labor intensive mechanism for facilitating law enforcement cooperation, [and it] must contend with the challenges posed by significant increases in the volume and complexity of requests for assistance made to the U.S. in the Internet age" when many leading global CSPs are based there.[290] *** the MLAT process was not designed to process "a very large number of electronic evidence requests at speed."[291]

285 Public Safety, "U.S. CLOUD Act: DMNS Presentation," February 22, 2019.
286 Canada has over thirty bilateral MLATs. Robert J Currie and Dr. Joseph Rikhof, *International & Transnational Criminal Law*, 2020.
287 DoJ, "Justice Response for Factual Accuracy," December 20, 2024.
288 Michael Geist, "Lawful Interception of Communication by Security and Intelligence Organizations: The Policy and Legal Challenges Posed by Real-Time Messaging on Internet Platforms," NSICOP Commissioned Paper, May 2024.
289 RCMP, NSICOP appearance, April 18, 2024.
290 U.S. Assistant Attorney General, Letter to the Honourable Joseph R. Biden, President of the United States Senate, July 15, 2016.
291 ***

**125.** MLATs are not an option for CSIS. ***[292] ***[293] ***[294]

**126.** Both RCMP and CSIS see a potential solution to jurisdictional issues with a U.S. nexus by leveraging the U.S. *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act). Enacted in 2018, the CLOUD Act seeks to expedite access to electronic information held by U.S.-based global CSPs.[295] Canada and the U.S. are currently negotiating a Data Access Agreement to allow their respective law enforcement and security agencies to request data, including communications content, from each other's service providers (discussed further in Chapter 4).

**127.** Apple, Facebook, Google, and Microsoft publicly support the CLOUD Act's approach to cross-border data sharing, noting it would "allow law enforcement to investigate cross-border crime and terrorism in a way that avoids international legal conflicts."[296] ***[297] ***[298]

**128.** Some Canadian CSPs have expressed concern about how they will be able to respond to incoming requests from the U.S. when and if a bilateral Data Access Agreement is approved, particularly in light of the absence of a legal framework for intercept capability.[299]

292 CSIS, "2022 11 25 NSICOP Meeting Write Up," November 2022.
293 ***
294 ***
295 U.S. Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around World: The Purpose and Impact of the CLOUD Act White Paper," April 2019.
296 Apple, Facebook, Google, Microsoft, and Oath, Letter to U.S. Senators Orrin Hatch, Christopher Coons, Lindsey Graham, and Sheldon Whitehouse, February 6, 2018.
297 ***
298 ***
299 Canadian CSP, NSICOP appearance, October 3, 2024.

# Chapter 4: Government Response

**129.** The previous chapter describes the operational response by security and intelligence agencies to lawful access challenges, which the Committee views as "bottom-up" initiatives to mitigate these challenges within Canada's existing lawful access framework. This chapter examines the "top-down" attempts by the government to modernize this framework from 2012 to late 2024. In this time period, the government tried to address lawful access challenges across several cross-cutting policy initiatives, including through legislative attempts, public consultations, funding initiatives, and international cooperation. The Committee has opted to present the government's response chronologically, by parliamentary session.

## Policy Leads and Governance

**130.** The Minister of Public Safety and the Minister of Justice are accountable to Parliament for lawful access. They are advised by the departments of Public Safety and Justice. The primary operational departments are CSIS and the RCMP. In the time period under review, several successive Cabinet Committees could have served as forums to discuss lawful access policy.[300] According to the Minister of Public Safety, the Cabinet Committee on Global Affairs and Public Security is the more likely venue for a discussion on lawful access policy than the newly created National Security Council, which first met in October 2023.

**131.** Cabinet deliberations on lawful access policy are supported by the Deputy Ministers' Committee on National Security (DMNS). The mandate of DMNS is to consider security, defence and foreign policy issues in order to provide coherent, integrated advice to the Prime Minister and Cabinet committees.[301] Normally co-chaired by the National Security and Intelligence Advisor and the Deputy Minister of Public Safety, its members include the deputy heads of CSE, CSIS, the RCMP, Innovation, Science, and Economic Development Canada, and DoJ.[302]

300 These included the Cabinet Committee on Foreign Affairs and Security (from February 2006 to November 2015); the Cabinet Committee on National Security (from May 2011 to July 2013); the Cabinet Committee on Canada and the World (from November 2015 to September 2023), renamed the Cabinet Committee on Global Affairs and Public Security in September 2023; and the National Security Council (from October 2023).

301 DMNS Terms of Reference, undated.

302 Members: Canada Border Services Agency, Canadian Armed Forces, Canadian Food Inspection Agency, CSE, CSIS, Department of National Defence, Innovation, Science, and Economic Development Canada, DoJ, Department of Finance, Financial Transactions and Reports Analysis Centre, Global Affairs Canada, Immigration, Refugees and Citizenship Canada, PCO (National Security and Intelligence Advisor to the Prime Minister) (co-chair), Public Health Agency of Canada, Public Safety (co-chair), RCMP, and Transport Canada. PCO, "Governance Structure – National Security," undated.

**132.** Several distinct yet overlapping lawful access issues were contemplated by the government in the period under review. They included:

- A legal framework for intercept capability for Canadian CSPs;
- The development of legislation to access BSI, following the Supreme Court decision in *R v Spencer*;
- The development of a policy on encryption, including whether to require CSPs and other communications platforms to decrypt communications for investigators;
- Determining whether the law should require CSPs to retain metadata for a specified period of time; and
- The negotiation of treaties to enable access to information held by CSPs outside Canada through enhanced multilateral and Canada-U.S. cooperation.

# The Government's Response to Lawful Access Challenges

## Early Efforts

**133.** The government's response to lawful access policy issues predates the period under review. In 1998, the government published its cryptography policy for electronic commerce, which acknowledged potential challenges for law enforcement, but supported strong encryption as essential to economic prosperity and the digital economy.[303]

**134.** In 1999, the government established the Lawful Access Initiative, whose goal was to "implement a strategic framework" to assist law enforcement (RCMP and non-federal police services) and national security agencies (CSIS and CSE) "in maintaining lawful access to information and communications."[304] Led by Public Safety, the initiative also involves CSE, CSIS, DoJ, Innovation, Science and Economic Development Canada, PPSC, and the RCMP. The government initially funded the initiative for five years at $*** annually, and provided ongoing funding of $*** from 2005 to the present day. The initiative provides CSIS and the RCMP with funding for intercept solutions at CSPs, processing and analysis, and *** techniques.[305]

**135.** Efforts by the government to modernize lawful access legislation for the digital age began in earnest following Canada's signature in November 2001 of the Council of Europe's *Budapest Convention on Cybercrime* (Budapest Convention), a multilateral agreement which committed the government to create new *Criminal Code* powers specific to electronic evidence, including specialized production orders.[306] Between 2001 and 2004, the

303 Industry Canada, *A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society*, February 1998.

304 Solicitor General of Canada, Minister of National Defence, and Minister of Justice, "Maintaining Lawful Access to Information and Communications Needed to Ensure Public Safety and Security," Memorandum to Cabinet, February 17, 1999.

305 Since 2005, the Lawful Access Initiative has provided CSIS with $*** annually including *** FTEs and the RCMP with $*** annually including *** FTEs, for a total (for those two organizations) of $*** annually including *** FTEs. CSIS, "CSIS Funding Letter," from CSIS's Assistant Director of Technology to Public Safety's Associate Deputy Minister, April 17, 2013; CSIS, CSIS costing spreadsheet created for NSICOP in response to RFI #2, September 13, 2024; and Public Safety, *Lawful Access Initiative: Final Performance Measurement Report, Fiscal Years 2015-2018*, undated.

306 The Budapest Convention harmonizes cybercrime offences and production orders for electronic evidence, and acts as a mutual legal assistance treaty for the 76 countries which have ratified it as of September 2024. Council of Europe, *Convention on Cybercrime*, November 23, 2001; and Council of Europe, "Chart of signatures and ratifications of Treaty 185," September 2024.

government held several public consultations on lawful access issues to inform legislative proposals. Between 2005 and 2012, the government tabled seven bills in an effort to update Canada's lawful access legislation. All died on the Order Paper following the dissolution or prorogation of Parliament. None became law. See Annex E.

**136.** The bills attracted criticism from privacy advocates, cybersecurity experts, and CSPs,[307] which stated the government had not provided sufficient evidence of the problem, had not explained why existing authorities were insufficient, and could not say how much the initiative would cost.[308] In particular, cybersecurity experts and privacy advocates were concerned about any attempt to legally require the introduction of weaknesses in encryption by requiring "backdoors" for law enforcement and security agencies, in part because such weaknesses could also be used by nefarious actors.[309]

## 41st Parliament (2011 to 2015)

**137.** Each of the government's successive attempts to pass lawful access legislation drew from the previous failed efforts and included the same or similar provisions.[310] In February 2012, the government tabled Bill C-30, the *Protecting Children from Internet Predators Act*.[311] The bill would have created the *Investigating and Preventing Criminal Electronic Communications Act*, requiring CSPs to be intercept capable and able to decrypt encrypted communications. The bill also would have created specialized *Criminal Code* production orders for investigators to obtain certain electronic data that attracts a lower expectation of privacy, such as geolocation data.[312] The bill quickly attracted the same criticisms as the earlier proposed legislative attempts. In February 2013, the Minister of Justice publicly set the bill aside and noted that any future bill "'to modernize the *Criminal Code* will not contain the measures contained in Bill C30.'"[313]

**138.** In November 2013, the government tabled Bill C-13, the *Protecting Canadians from Online Crime Act*, which came into force in March 2015. It retained the least controversial parts of Bill C-30, specifically new preservation demands and orders, and specialized production orders.[314] The coming into force of the Act enabled Canada to ratify the Budapest

307 Christopher Parsons, "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada," Chapter IX in Michael Geist (editor), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, 2015.

308 Michael Geist, "Why The Government's Lawful Access Claims Stand on a Shaky Foundation," December 12, 2011; Michael Geist, "Everything You Always Wanted to Know About Lawful Access, But Were (Understandably) Afraid to Ask," February 13, 2012; Michael Geist, "How to Fix Canada's Online Surveillance Bill: A 12 Step To-Do List," February 24, 2012; Kevin McArthur and Christopher Parsons, "Understanding the Lawful Access Decryption Requirement," September 18, 2012; Christopher Parsons, "Lawful Access, Its Potentials, and its Lack of Necessity," November 9, 2011 (reposted August 18, 2022); and Privacy Commissioner of Canada, "Letter to Minister of Public Safety Vic Toews," News release, October 26, 2011.

309 CSE, "Policy Considerations on End-to-End Encryption," undated; Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, "Keys under doormats: Mandating insecurity by requiring government access to all data and communications," Massachusetts Institute of Technology Press, July 6, 2015; Lex Gill, Tamir Israel, and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018 ; and Kevin McArthur and Christopher Parsons, "Understanding the Lawful Access Decryption Requirement," September 18, 2012.

310 Bill C-74, the *Modernization of Investigative Techniques Act* in 2005; Bill C-46, the *Technical Assistance for Law Enforcement in the 21st Century Act* in 2009; and Bill C-52, *the Investigating and Preventing Criminal Electronic Communications Act* in 2010.

311 Full title: *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*.

312 These production orders became law when the *Protecting Canadians from Online Crime Act* came into force in March 2015.

313 Minister of Justice quoted by the CBC, "Government killing online surveillance bill," February 11, 2013.

314 This included specialized production orders and new *Criminal Code* powers for police to compel Canadian entities to preserve computer data until such time as the investigator has the grounds to compel the entity to provide it.

Convention, which came into force for Canada on November 1, 2015.[315] With the passage of the Act, the government launched the Investigative Powers for the 21st Century initiative to support the implementation of the Act and Canada's obligations under the Budapest Convention. Led by DoJ in collaboration with PPSC, the RCMP, and GAC, the purpose of the initiative was to inform Canadian prosecutors and foreign police agencies about the new powers under the Act, facilitate international cooperation under the Budapest Convention, and for the RCMP to expand its digital forensic capacity. Under this initiative, the government provided the four departments with $60.74 million over five years (2015-16 to 2019-20), and $12.25 million ongoing (from 2020-21).[316]

**139.** In June 2014, the Supreme Court rendered its unanimous decision in *R v Spencer*, ruling there is a reasonable expectation of privacy in BSI when it is linked to an IP address. The Supreme Court's decision gave the government two options: police could use existing Criminal Code powers or the government could table a new "reasonable law" for police to access BSI.[317] DoJ and its provincial and territorial counterparts undertook concerted efforts to understand the operational impact of Spencer and analyze legal and privacy issues, including post-2014 jurisprudence as the courts applied *R v Spencer* to various cases.[318] ***

## 42nd Parliament (2015 to 2019)

**140.** In October 2015, Canadians elected a new government. The following month, the Prime Minister instructed the Minister of Justice and the Minister of Public Safety and Emergency Preparedness to introduce new national security legislation. Between September and December 2016, the government held public consultations on this proposed legislation through a national security green paper.[319] Intended to "prompt discussion and debate about Canada's national security framework," the green paper included a chapter on "Investigative Capabilities in the Digital World" that raised four challenges: BSI, intercept capability, data retention, and encryption. There was also a chapter about "Intelligence and Evidence."[320]

**141.** ***[321] ***[322] ***[323] ***[324] ***[325] ***

**142.** In May 2017, Public Safety published the "What We Learned" report about the green paper consultation. Public Safety had held five in-person town halls, fourteen in-person sessions with academics and experts, and one roundtable with civil society experts. The Ministers of Public Safety and Justice co-hosted several of the events, including the roundtable with 36 civil society experts.[326] The two ministers' parliamentary secretaries also hosted events; for example, the Parliamentary Secretary to the Minister of Justice hosted a town hall in

315 Council of Europe, "Chart of signatures and ratifications of Treaty 185," September 2024.
316 DoJ, *Evaluation of the Investigative Powers for the 21st Century Initiative*, Final Report, March 2020.
317 *R v Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212.
318 ***
319 Government of Canada, *National Security Consultations: What We Learned*, May 19, 2017.
320 Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, 2016; and Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016: Background Document*, 2016.
321 ***
322 ***
323 ***
324 ***
325 ***
326 Public Safety, "Roundtable on the National Security Framework Civil Society Evening – October 19, 2016," event summary, November 29, 2016.

Yellowknife, Northwest Territories.[327] There were also seventeen engagement events led by members of Parliament at the constituency level that involved members of the public. Public Safety received 58,933 responses to the online questionnaire, 17,862 email submissions, and 79 submissions from organizations and experts. The lawful access part of the consultation generated about 70% of total online responses and significant input from experts and organizations, demonstrating a high level of public and stakeholder engagement. The vast majority of responses indicated that the expectation of privacy in the digital world is the same as or higher than in the physical world. A clear majority of respondents opposed any move to weaken encryption, and 7 out of 10 respondents considered their BSI to be as private as the actual contents of their emails or personal diary. Almost half (44%) of online responses saw no demonstrable need to give investigators new tools, although a further 41% of online responses said investigators should have access to updated tools in a digital world if they could demonstrate the need for them.[328]

**143.** Public Safety's internal analysis of the 2016 consultation highlighted the views of 35 notable entities including law enforcement, civil society, academics, CSPs, and FPT privacy commissioners: "Across all themes, [these] stakeholders believed it was unclear why existing statutory powers were inadequate for the needs of investigators. Many stakeholders called on the Government to provide clear evidence to justify that changes are necessary." These stakeholders responded to the four lawful access issues in the green paper:

- ***Lawful access to BSI:*** "Most stakeholders – spanning the civil society, academic, and CSP sectors – believed that investigators should require judicial authorization in order to access BSI."
- ***Intercept-capable CSP networks:*** "While they did not express support for this proposal, most CSP stakeholders did not outright oppose the introduction of intercept capability requirements" as long as the requirements "do not interfere with business operations or competitiveness" and the government compensates them.
- ***Data retention:*** "Many civil society, academic, and CSP stakeholders, as well as FPT Privacy Commissioners questioned the necessity of creating data retention requirements given that data preservation powers were enacted [in the *Criminal Code*] in 2015." "CSP and civil society stakeholders which did not express outright opposition to data retention still noted serious concerns regarding the potential impact of such [a] measure on the privacy of Canadians and on the security of their data."
- ***Encryption:*** "Stakeholders across the civil society, academic, and CSP sectors supported strong encryption … [and] opposed 'exceptional access' measures (such as [decryption] key escrow or technical 'backdoors') … ."[329]

**144.** Also in May 2017, and expressly in response to the green paper, the Standing Committee on Public Safety and National Security (SECU) tabled a report entitled *Protecting Canadians and their Rights: A New Roadmap for Canada's National Security*. SECU recommended against legislation regarding encryption or access to BSI.[330] In its public response to the report, the government agreed, stating that it was "in Canada's interest to ensure that encryption technologies remain robust and widely used," and that: "…While the spread of

327 Public Safety, "Yellowknife Town Hall National Security Framework – December 5, 2016," event summary, webpage, December 23, 2016 .
328 Government of Canada, *National Security Consultations: What We Learned*, May 19, 2017.
329 Public Safety, "Summary of Notable Submissions on Lawful Access," draft, undated.
330 SECU, *Protecting Canadians and their Rights: A New Roadmap for Canada's National Security*, May 2, 2017.

powerful encryption has created significant gaps for law enforcement and national security agencies, the Government does not consider legislative responses to these challenges to be viable. The Government continues to examine options to ensure departments and agencies have the resources necessary to gain access to decrypted data required to prevent terrorist incidents and address criminal activity."[331] The response was silent on SECU's recommendation against legislation for BSI.

**145.** On June 20, 2017, the government tabled Bill C-59, the *National Security Act, 2017*, without any lawful access provisions.[332] Earlier that month, Public Safety had informed DoJ that it had "some concern" about proceeding with planned consultations on intercept capability, and similarly asked Justice to "'stand down'" any further consultations on BSI.[333]

**146.** Later that month, Canada hosted the 2017 Five Country Ministerial meeting of Ministers of Public Safety and Attorneys General in Ottawa. In their public communiqué, Ministers acknowledged how encryption could "severely undermine public safety efforts by impeding lawful access to the content of communications," but committed Five Eyes' governments to engaging CSPs to "explore shared solutions while upholding cybersecurity and individual rights and freedoms."[334]

**147.** The following year in Australia, the Ministers of Public Safety and Attorneys General of the Five Eyes met and published a Statement of Principles on Access to Evidence and Encryption. The statement encouraged CSPs to "voluntarily establish lawful access solutions to their products," but also noted that governments might "pursue technological, enforcement, legislative or other measures to achieve lawful access solutions."[335]

**148.** ***[336]

**149.** In June 2019, SECU tabled a report entitled *Cybersecurity in the Financial Sector as a National Security Issue*. The report endorsed an expert's definition of strong encryption – i.e., "'encryption algorithms for which no weaknesses or vulnerabilities are known or have been injected …'"[337] – and recommended "that the Government of Canada reject approaches to lawful access that would weaken cybersecurity."[338]

**150.** The Five Eyes' focus on encryption continued at the following meeting in July 2019 in the U.K. Its Five Country Ministerial communiqué noted that CSPs "should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and useable format" to support investigations and to take action against illegal content.[339]

---

331 Minister of Public Safety and Emergency Preparedness, Government response to SECU's report of May 2, 2017, undated.
332 Bill C-59 would receive royal assent in 2019.
333 DoJ, "Consultation on Access to Basic Subscriber Information," June 9, 2017.
334 Governments of Australia, Canada, New Zealand, the U.K., and the U.S., "Joint Communiqué," Five Country Ministerial Joint Communiqué, June 27, 2017.
335 Governments of Australia, Canada, New Zealand, the U.K., and the U.S., "Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019," July 30, 2019.
336 ***
337 Christopher Parsons (Research Associate, Citizen Lab, University of Toronto), SECU Evidence, February 27, 2019, quoted in SECU, *Cybersecurity in the Financial Sector as a National Security Issue*, June 2019.
338 SECU, *Cybersecurity in the Financial Sector as a National Security Issue*, June 2019.
339 Governments of Australia, Canada, New Zealand, the U.K., and the U.S., "Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019," July 30, 2019.

## 43rd Parliament (2019 to 2021)

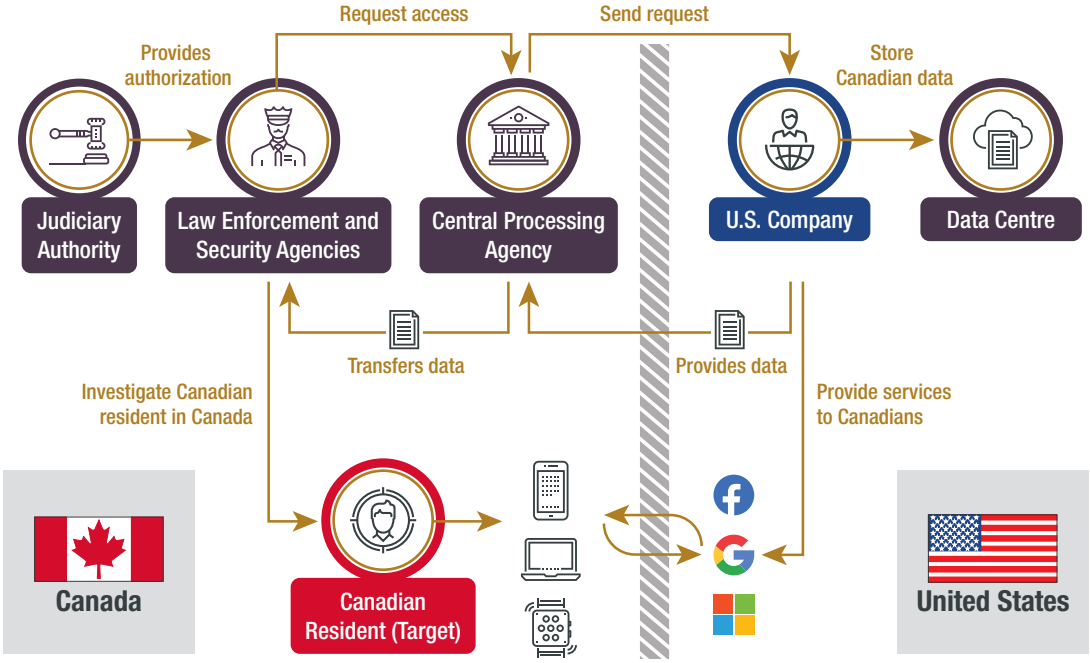
**151.** In October 2020, the Minister of Public Safety and Emergency Preparedness joined his counterparts in the other Five Eyes countries, India, and Japan to publish the "International Statement: End-to-end Encryption and Public Safety," led by the U.K.[340] The International Statement was largely a response to Facebook's March 2019 announcement of its plan to implement end-to-end encryption across its platforms, including Facebook Messenger.[341] The statement noted that end-to-end encryption impedes police investigations and undermines a company's "own ability to identify and respond to … illegal content and activity on its platform, including … terrorist propaganda and attack planning." The statement urged companies to focus "on reasonable, technically feasible solutions" to enable them to read and identify illegal content on their platforms and take action, thereby "facilitating the investigation and prosecution of offences" including by being able to produce "content in a readable and useable format" when presented with a warrant.[342]

**152.** In November 2020, the government approved a plan for the Minister of Public Safety and Emergency Preparedness to lead public and stakeholder consultations to support the development of a government policy position on end-to-end encryption and lawful access.[343] The consultations were intended to inform the government about how to respond to the challenge of encryption as part of its broader strategy to promote Canadian prosperity in a digital world, while protecting privacy and public safety.[344] According to Public Safety, these consultations ultimately did not proceed because of "stakeholder fatigue" and a concern that proceeding would have had a potentially "adverse effect on responses."[345]

**153.** As noted in Chapter 3, in spring 2021, Canada and the U.S. began formal negotiations towards a Data Access Agreement under the framework of the U.S. CLOUD Act.[346] Such an agreement would allow law enforcement and security agencies with the requisite authorization to request data, including communications content, from the other country's CSPs directly,[347] as shown in Figure 4.1 below. To date, the U.S. has concluded agreements with the U.K. in 2019 and Australia in 2021.[348] A Canada-U.S. agreement would allow Canada to serve Canadian court orders for stored data or interception directly to U.S. companies as long as the Canadian court order did not "intentionally target" a U.S. person or a person in the U.S., and it would "not be unlawful" for the U.S. companies to comply.[349] The reverse would also hold, so a U.S. request could not intentionally target a Canadian person or a person in Canada. ***[350]

340 Governments of Australia, Canada, India, Japan, New Zealand, U.K. and the U.S., "International Statement: End-To-End Encryption and Public Safety," October 11, 2020.
341 Mark Zuckerberg, "Privacy-Focused Vision for Social Networking," March 6, 2019.
342 Governments of Australia, Canada, India, Japan, New Zealand, the U.K., and the U.S., "International Statement: End-To-End Encryption and Public Safety," October 11, 2020.
343 CSE, "Material for bilat between [CSE] Chief and ISED [Innovation, Science, and Economic Development Canada] Assoc. DM [Associate Deputy Minister] Paul Thompson," September 21, 2020.
344 CSE, "Seeking an Approach on Encryption Consultations with Public Safety," Briefing note for the Chief, undated.
345 Minister of Public Safety, NSICOP appearance, November 5, 2024.
346 Canada and the U.S. announced the negotiations in March 2022. The U.S. is also negotiating similar agreements with the European Union and New Zealand. Governments of Canada and the U.S., "United States and Canada Welcome Negotiations of a CLOUD Act Agreement," Press release, March 22, 2022; and Public Safety, "Negotiations Status Update – Canada-US Data Access Agreement," deck for Minister, November 2023.
347 Public Safety, "US CLOUD Act: DMNS," February 22, 2019.
348 U.S. Department of Justice, CLOUD Act Resources, webpage, accessed October 2024.
349 U.S. CLOUD Act, sections 104 and 105 respectively.
350 DoJ, "Department of Justice Response to Request for Information #3," November 15, 2024.

**Figure 4.1: Bilateral agreements under the framework of the U.S. CLOUD Act[351]**




## 44th Parliament (2021 to November 2024)

**154.** In June 2022, the government's response to a written question on the Order Paper about electronic surveillance informed the House of Commons about the RCMP's previously unknown use of ODITs, prompting a study by ETHI. In November 2022, the Committee tabled its report entitled *Device Investigative Tools used by the Royal Canadian Mounted Police and related issues*. ETHI made several recommendations, including that the government amend the *Privacy Act* to require government institutions to conduct a privacy impact assessment before using high-risk technological tools and submit them to the Office of the Privacy Commissioner for assessment. The government responded that it was currently leading a review of the *Privacy Act*.[352]

**155.** ETHI also recommended the government establish an independent advisory body composed of relevant stakeholders from the legal community, government, police and national security, civil society and relevant regulatory bodies to review new technologies used by law enforcement and to establish national standards for their use. The government responded that the RCMP has established the National Technology Onboarding Program to implement an internal, centralized process to assess new technological investigative tools that includes evaluating privacy and legal considerations. ETHI also recommended the government

351 Public Safety, "U.S. CLOUD Act: DMNS Presentation," February 22, 2019.
352 President of the Treasury Board, "Letter to the Chair of the Standing Committee on Access to Information, Privacy and Ethics," November 2022.

create a list of banned spyware vendors. The government's response recognized the need to have clear rules over surveillance technology, but did not respond specifically to the recommendation for a list outside of the regular export regime.

**156.** In March 2023, Public Safety "renewed" the lawful access policy discussions with a presentation to DMNS. According to Public Safety, there was no particular impetus that prompted the renewal of discussions at this table. Officials noted that "policy work on lawful access at the working level never stopped," and acknowledged that "growing concerns of gaps in the investigative tool kit *** played a part."[353] Public Safety's presentation took stock of the challenges and sought views on a strategic plan to address them. The challenges were access to BSI, access to metadata, interception, computer network exploitation, and international cooperation. Public Safety proposed three elements as the potential way ahead: build conditions for success by addressing transparency, credibility, and coordination gaps; introduce legislative proposals which could include capability requirements for CSPs; and *** ratifying the Council of Europe's *2nd Additional Protocol to the Budapest Convention on Cybercrime*.[354]

**157.** Unlike the 2016 green paper, the renewed lawful access policy discussion did not include data retention. According to Public Safety, it has been "monitoring the development of data retention policy in other international jurisdictions since 2016" and it states that "data retention is still part of the lawful access policy conversation today," with policy work focused on "potential legislative reforms ***."[355]

**158.** In May 2023, the National Security Transparency Advisory Group (NS-TAG)[356] held a meeting with civil society, academia, and national security departments and agencies on "Emerging Technologies and Digital Tools in the Protection of National Security." According to the summary report, Public Safety experts briefed the members of NS-TAG on the development of a transparency framework for digital investigative capabilities (i.e., the ability by security organizations to access information of targets being held by CSPs).[357] The summary of the meeting does not include any recommendations on a way forward.

**159.** In June 2023, Canada signed the Council of Europe's *2nd Additional Protocol to the Budapest Convention on Cybercrime*, which provides "a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for BSI, effective means to obtain BSI and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal protection safeguards."[358] After Canada signed the *2nd Additional Protocol*, DoJ conducted stakeholder consultations, including with provinces,

353 Public Safety, "NSICOP Lawful Access RFI #3 to Public Safety," November 15, 2024.
354 Public Safety, "Digital Investigative Capabilities: Renewal of the Lawful Access Policy Development Agenda," Deck for DMNS, March 22, 2023.
355 Public Safety, "NSICOP Lawful Access RFI #3 to Public Safety," November 15, 2024.
356 In July 2019, the Minister of Public Safety and Emergency Preparedness announced the creation of NS-TAG as a means of implementing the government's 2017 National Security Transparency Commitment. An independent and external body, NS-TAG is composed of former civil servants, academics, and members of civil society. Its role is to advise the Deputy Minister of Public Safety on "steps to infuse transparency into Canada's national security policies, programs, and activities in a manner that will increase democratic accountability and public awareness." NS-TAG, "The Digitization of National Security: Technology, Transparency & Trust," July 2024.
357 Government of Canada, "Summary of the Meeting of the National Security Transparency Advisory Group (NS-TAG) May 26-27, 2023," April 18, 2024.
358 Council of Europe, "Details of Treaty No. 224," accessed October 2, 2024. As of September 2024, 45 states – including Canada – have signed but not ratified the *2nd Additional Protocol*, and two states have ratified it. Council of Europe, "Chart of signatures and ratifications of Treaty 224," accessed October 2, 2024.

territories, and privacy commissioners.[359] The consultation asked "what type of authorization (e.g., judicial or other) Canada should require" for foreign investigators to obtain various types of data from Canadian CSPs, and "whether Canada should opt out of permitting direct access" by foreign investigators "to subscriber information held by Canadian [CSPs]." The Office of the Privacy Commissioner believes Canada should opt out, and that Canada's implementation of the *2nd Additional Protocol* should require a Canadian court order for all foreign requests.[360]

**160.** As noted in Chapter 2, in March 2024 a majority of the Supreme Court found in *R v Bykovets* that there is also a reasonable expectation of privacy associated with a person's IP address.[361] In response to this decision, Department of Justice officials revisited "the issue of lawful access to subscriber information and [examined] possible solutions to address some lawful access challenges in the short-to-medium term."[362] The Minister of Justice indicated that he was open to examining the possibility of a reasonable grounds to suspect threshold for BSI.[363]

**161.** In July 2024, NS-TAG released a report entitled "The Digitization of National Security: Technology, Transparency & Trust."[364] The report noted its concerns about the national security and intelligence community's lack of transparency on data management and its use of metadata. It also flagged concerns about the government's position on encryption, noting that "if national security require[s] that encryption must indeed be weakened, either by making it 'breakable' or through back doors, a number of safeguards will have to be prepared, including the rapid, if not automatic diffusion of information to the public about breaches and the close oversight and reporting of law enforcement use…."[365] The report calls on the government to engage with Canadians on "the needs and the risk of police or security intelligence decryption capabilities," and provide "fully intelligible justifications for policy decisions regarding cryptography…[including] complete information on the actual impact of encryption on national security, well beyond buzzwords such as 'going dark.'"[366]

**162.** As of November 2024, Canada and the U.S. continue negotiations for a Canada-U.S. Data Access Agreement, ***[367] ***[368] ***[369] In July 2024, the Minister of Public Safety and the Minister of Justice met their U.S. counterparts in Washington, D.C. The U.S. Attorney

359 This was not the government's first engagement of stakeholders on this issue. OPC, "Submission of the Office of the Privacy Commissioner (OPC) to Justice Canada Re (Response): Consultation Paper for the Second Additional Protocol to the Budapest Convention," March 22, 2024; DoJ, "Second Additional Protocol on Cybercrime," webpage, last modified February 21, 2024; and DOJ, "Council of Europe Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence: Consultations, 2023," deck from webpage.

360 OPC, "Submission of the Office of the Privacy Commissioner (OPC) to Justice Canada Re (Response): Consultation Paper for the Second Additional Protocol to the Budapest Convention," March 22, 2024.

361 *R v Bykovets*, 2024 SCC 6.

362 DoJ, "Department of Justice Response to Request for Information #3," November 15, 2024.

363 Minister of Justice, NSICOP appearance, November 7, 2024; and DoJ, "Department of Justice Response to Request for Information #3," November 15, 2024.

364 NS-TAG, "The Digitization of National Security: Technology, Transparency & Trust," July 2024.

365 NS-TAG, "The Digitization of National Security: Technology, Transparency & Trust," July 2024.

366 NS-TAG, "The Digitization of National Security: Technology, Transparency & Trust," July 2024.

367 ***

368 Minister of Public Safety, NSICOP appearance, November 5, 2024.

369 Minister of Justice, NSICOP appearance, November 7, 2024; and DoJ, "Justice Response for Factual Accuracy," December 20, 2024.

General acknowledged consensus on most of the agreement with a few important issues to be resolved, and the Minister of Justice reiterated Canada's interest in concluding the agreement, noting that he believed the remaining issues were surmountable.[370] ***[371]

**163.** In October 2024, ETHI tabled a report about the *Federal Government's Use of Technological Tools Capable of Extracting Personal Data From Mobile Devices and Computers*, which focused on government-issued devices. While not expressly focused on lawful access per se, the report reiterated five recommendations ETHI had made in its 2022 study of the RCMP's use of ODITs, including the recommendation that the government amend the *Privacy Act* to require government institutions to conduct privacy impact assessments before using high-risk technological tools and submit them to the Office of the Privacy Commissioner for review.[372]

370 Public Safety, Email update for senior Public Safety and Justice officials from Public Safety's Counsellor at the Embassy of Canada in Washington, D.C., about the 2024 Cross-Border Crime Forum, July 24, 2024.

371 ***

372 ETHI, *Federal Government's Use of Technological Tools Capable of Extracting Personal Data From Mobile Devices and Computers*, October 10, 2024. As of November 4, 2024, the government had not tabled a response.

# Chapter 5: Assessment

**164.** At the outset of this review of the lawful access to communications by security and intelligence organizations, the Committee set out to consider three key questions:

- Are Canada's lawful access challenges for national security investigations as serious as the security and intelligence organizations claim?
- Has the government been effective at mitigating or developing solutions to these challenges?
- How does the government facilitate and enable national security investigations while at the same time protect Canadians' right to privacy?

**165.** Over the course of its review, the Committee heard from two Ministers and 33 officials from five departments and agencies, ranging from deputy heads to national security investigators. Mindful that these appearances would only yield the government's perspective, the Committee also sought the views of defence counsel, legal and cybersecurity experts, and privacy and civil society advocates. Additionally, the Committee heard from several Canadian CSPs. Finally, the Committee relied upon classified briefings, government records spanning over twelve years, academic literature, media articles, podcasts, blogs, and similarly-themed reports completed by like minded democracies.

**166.** The Committee's assessment explores the significance of Canada's lawful access challenges and the government's response to these challenges at the operational and strategic levels, and considers the interplay between national security and Canadians' right to privacy.

## Assessing Canada's Lawful Access Challenges

**167.** The Committee heard that Canada's security and intelligence organizations regularly face challenges in investigating threats to national security because of the combined effects of rapidly evolving technology, the global nature of digital communications, and a legal framework that has not kept pace with the advances in technology. While these advances in technology have created new opportunities for CSIS and the RCMP to collect information in support of their respective mandates, both organizations state that the challenges currently outweigh the opportunities. The Committee observed that the impact and significance of each of these challenges present themselves differently for each organization, depending on the degree to which CSIS or the RCMP have been able to mitigate them. These dynamics are explored below.

## Technology

**168.** The Committee did not see any clear, empirical data to substantiate claims by Canada's security and intelligence organizations that they face serious lawful access challenges because of rapidly evolving technology. CSIS and the RCMP do not systematically track how often they encounter various technological challenges in their national security investigations, for example, instances in which communications content could not be accessed because of encryption. As a result, they do not know in quantifiable terms the degree of impact and overall significance of these challenges. Consequently, the Committee had no data to analyze to identify trends over time. This is an important omission because as these organizations advise the government and attempt to convince Canadians – particularly those concerned about the potential erosion of their privacy – that new legislation and resources are required to keep pace with evolving technology, they are only able to offer anecdotes and not concrete figures.

**169.** Senior officials from Public Safety, CSIS, and the RCMP repeatedly stated that in situations where CSIS or the RCMP ran into situations in which communications content was unavailable, they found other ways to get the information required. All organizations confirmed that, where known, available and precise enough, metadata was also useful in their investigations. This would appear to confirm that CSIS and RCMP are not "going dark," rather that they experiencing what the Citizen Lab describes as "investigative friction."[373]

**170.** However, the Committee heard compelling and detailed testimony about how the rapid pace of technological change has increased the complexity, operational risk and cost of national security investigations. More digital devices, more communications applications or apps, and more operating systems mean that investigators need to develop more methods of access, with an impact on both time and resources. CNE is costly and not always effective (this is discussed further below). Other mitigation efforts to *** get access to encrypted communications content*** are now complicated ***. (The Committee notes that none of security and intelligence organizations cited concerns about artificial intelligence from a lawful access perspective, beyond surmising that increased use of artificial intelligence could assist with forensic debriefing efforts.)

**171.** In summary, notwithstanding CSIS and the RCMP's failure to systematically track data about technological challenges encountered over the time period of the review, the Committee nonetheless believes there is sufficient information to confirm their claims that they face significant challenges in their ability to access relevant and timely digital evidence and intelligence.

| | |
|---|---|
| F1 | Canada's security and intelligence organizations do not systematically track how often they encounter technological challenges in their national security investigations and whether they are successful in mitigating these challenges. |
| F2 | The RCMP and CSIS face significant challenges in accessing communications content, for which metadata is not necessarily a substitute. |

373 Lex Gill, Tamir Israel, and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, 2018.

| | |
|---|---|
| R1 | Under the leadership of the Minister of Public Safety, the government develop and implement a comprehensive strategy to address Canada's lawful access challenges, drawing from the Committee's review and findings. Such a strategy should:<br>• Affirm key principles, such as legitimacy, necessity, and proportionality;<br>• Identify, track, and report on key lawful access challenges and associated risks;<br>• Include communications, stakeholder engagement and transparency commitments; and<br>• Consider challenges that may arise due to emerging technology, e.g., artificial intelligence. |

**172.** The ubiquitous use of encryption presents an important dilemma. In reviewing the government's policy response to encryption, despite the mounting challenges for national security investigations, the Committee believes that the government's decision in 2020 not to proceed with new consultations on encryption was reasonable, as the views of key stakeholders were indeed unlikely to have changed since Public Safety-led consultations on national security in 2016. The Committee notes that almost no concerted policy work on encryption has occurred since then. Government departments and agencies do appear to have arrived at a common, internal working position: encryption is essential in a society that is digital by default and any effort to degrade its integrity is incompatible with cybersecurity. Importantly, the Committee did not hear any government official call for legislation to compel the creation of exceptional access or "backdoors" to get around encryption.

**173.** The government's public statements to date, however, leave room for confusion. Canada's signing of the 2019 Five Country Ministerial communique on encryption and the U.K.-led 2020 "International Statement: End-to-end Encryption and Public Safety" allows for an interpretation that the government is still considering such legislation. Indeed, the fact that NSTAG published a report as recently as the summer of 2024 expressing concern that this was the government's position when it is clear to the Committee that it is not, suggests this remains important to clarify publicly in light of public concerns about cybersecurity and privacy.

**174.** In the Committee's view, in articulating Canada's position on encryption, the government will need to clearly explain that *** access encrypted communications content is more than just investigative friction. The Committee heard that CNE is not a panacea, and access to associated metadata is not the same as being able to access communications content in real time. As such, the Committee believes new laws, tools and resources for the security and intelligence community are required to mitigate this risk, but ones that leave encryption intact.

**175.** The Committee also observed that privacy and cybersecurity advocates and national security practitioners appear to be talking past one another in debates about encryption and exceptional access for law enforcement and intelligence organizations. As stakeholders debate policy initiatives or legislation, it will be critical for both sides to ensure a common understanding of key concepts. For the government, the Committee suggests that a robust, transparent communications strategy, which explains technical concepts in detail, is fundamental.

| | |
|---|---|
| F3 | There was consensus across appearances that legislation to compel the creation of exceptional access or "backdoors" to encryption platforms was neither required nor desired. |
| F4 | Canada's public position on lawful access to encrypted communication is unclear. National security practitioners, cybersecurity experts and privacy advocates do not have a common understanding of the problem. |

| | |
|---|---|
| R2 | The government publicly clarify its position on exceptional access to communications information protected by encryption. |

**176.** The Committee learned that the use of encryption and anonymizing technologies is also affecting how the RCMP and CSIS can obtain building block information required at the early stage of an investigation, ***. In this regard, the Committee heard that the Supreme Court's 2014 decision in *Spencer* requiring judicial authorization to seek BSI has created delays and significant increased effort on the part of security agencies to investigate a potential national security threat. DoJ efforts to address this issue have failed for years to progress. In addition, the Committee understands that the absence of a data retention regime has had significant implications given the length of some complex investigations.

| | |
|---|---|
| F5 | The government's failure to develop and implement a solution to the Supreme Court's decision in *Spencer* is impeding CSIS and the RCMP's ability to respond to national security threats. |
| F6 | Without a general legal requirement on CSPs to retain metadata for a specified period of time, there is a risk that data sought pursuant to a warrant will be unavailable. |

| | |
|---|---|
| R3 | The government table legislation creating new authorities in the *Canadian Security Intelligence Service Act* and the *Criminal Code* to enable the production of basic subscriber information, and the government consider legislation with respect to data retention. |

**177.** Security and intelligence practitioners, privacy advocates, and cybersecurity experts alike point to CNE, including the deployment of ODITs, as one of the *** solutions to obtaining communications content in the face of ubiquitous encryption. The Committee learned that these tools are expensive and often unreliable, as targets have become increasingly cybersecurity savvy and as companies work to identify and address the vulnerabilities in operating systems and encryption platforms ***.

**178.** The use of CNE also raises important questions about the protection of investigative techniques. The Committee learned that because of the complexity of CNE, ***. The Committee heard that the RCMP faces particular challenges in using ODITs in support of investigations because Canadian intelligence *** do not have confidence in Canada's legal system to adequately protect them from disclosure during court proceedings.

**179.** ***. ***, as well as legal experts, argue instead that provisions under the *Canada Evidence Act* have been shown to protect such information in legal proceedings and suggest that the problem may not be one with Canada's legal framework, but with institutional risk aversion. The Committee also heard that in responding to threats to national security, criminal proceedings may not be the most effective means, and that disruption without prosecution may be more viable when sensitive techniques are at issue.

**180.** As advances in both the change and complexity of technology continue, the Committee surmises that Canada's security and intelligence organizations ***. While CSIS and CSE appear to be secure because there is little risk of disclosure, the Committee is concerned that the RCMP will be limited in its ability *** technical solutions. While the Committee agrees that there may be some instances in which disruption is the most prudent response to a national security threat, the Committee has no information to suggest that Canadians want a legal system in which law enforcement regularly relies on disruption and not prosecution to address a national security threat.

**181.** The Committee notes that this particular challenge is a perennial feature in the larger, long-running debate in Canada about the intelligence and evidence dilemma. The Committee is concerned that, like the encryption debate, this issue too has reached a stalemate. The Committee recognizes that there is no simple solution to the challenge of using intelligence, or sensitive tools and techniques, in a criminal proceeding; it also notes the efforts by CSIS and the RCMP to improve cooperation and collaboration through the 2019 Operational Improvement Review. However, regardless of whether the problem is legislative or driven by institutional risk aversion, the Committee believes that the lack of urgency the government has afforded to addressing the intelligence and evidence problem at a strategic policy level is having unintended consequences for the rule of law in Canada as it relates to responding to national security threats.

| | |
|---|---|
| F7 | The government's inability to make progress on the intelligence and evidence dilemma, particularly with respect to the protection of investigative techniques, has contributed to a situation in which the RCMP is forced to choose either to not use sensitive tools and techniques during an investigation because of the potential disclosure issues, or risk not being able to rely on evidence obtained through their use at trial or having a prosecution stayed because of a court order to disclose. |

| | |
|---|---|
| R4 | Further to the Committee's 2024 recommendation in its *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* that the government address intelligence and evidence challenges, the government develop and implement a solution to address concerns about the protection of investigative tools, which may include revisions to the relevant provisions of the *Canada Evidence Act*. |

**182.** In addition to addressing the pressing need to improve the protection of investigative techniques, the Committee believes there is more policy work to do on the use of ODITs. The Committee was satisfied to hear that both CSIS and the RCMP ensure privacy safeguards are included in warrants authorizing the installation and use of these highly invasive tools. However, the Committee notes the lack of policy guidance on the procurement of commercial ODITs for use by law enforcement and intelligence agencies,

beyond the general requirement to complete a Privacy Impact Assessment. The Committee believes that a policy is also required to address concerns about transparency in ODIT use, including with respect to the complex warrant application process.

| | |
|---|---|
| F8 | The government lacks formal policies to address the procurement, regulation and use of commercial On-Device Investigative Tools, and ensure transparency in reporting with respect to their use by law enforcement and CSIS. |

| | |
|---|---|
| R5 | The government develop policies and guidelines on the procurement, use and reporting requirements for commercial On-Device Investigative Tools. |

## Absence of Intercept Capability Legislation

**183.** The Committee learned that unlike a number of likeminded democracies, Canada does not have legislation to compel CSPs to develop, deploy or maintain their systems in such a way as to remain intercept capable. Instead, in the period under review, CSIS and the RCMP primarily relied on a voluntary approach, ***. The Committee heard that the absence of intercept capability legislation creates unnecessary risks for all stakeholders, including CSIS, federal, provincial, territorial and municipal law enforcement, and CSPs. These risks include delays, legal ambiguity, financial inefficiencies, and ***. The situation also challenges Canada's ability to work with likeminded partners, who have intercept capability frameworks in place.

**184.** The Committee also heard that the absence of a centralized authority to coordinate lawful intercept initiatives, triage requests, and standardize approaches across national security and law enforcement agencies has caused confusion and frustration for all parties. The Committee notes CSIS and the RCMP's progress towards the creation of a National Lawful Access Centre, but questions why it took so long and why so much of the effort to derive a solution to this particular lawful access challenge appears to be driven from the bottom up.

**185.** All CSP representatives expressed their concerns to the Committee about the absence of legislation, notably with respect to the lack of a clear compensation framework for judicially authorized services provided by CSPs. The Committee also notes that, in the absence of any formal policy development led by Public Safety or discussion by ministers at Cabinet, the RCMP and CSIS have developed informal principles, which have informed their policies, procedures and practices. To date, these have all been geared towards ensuring continued buy-in from CSPs, including the question of whether or how CSPs are compensated by the government for their services. The question of whether compliance costs should be borne by CSPs or by government is a question that should be discussed at Cabinet, and ultimately debated in Parliament.

| | |
|---|---|
| F9 | The absence of legislation requiring communications service providers (CSPs) to maintain lawful intercept capability creates unnecessary risks for all stakeholders, including CSIS, federal, provincial, territorial and municipal law enforcement, CSPs and ultimately the Canadian public. It also impedes Canada's ability to work with international partners. The failure to address this issue at a strategic policy level has resulted in operational agencies themselves developing foundational policies and procedures, notably compensation models, geared toward ensuring continued cooperation from CSPs, rather than a principled approach based on input from Ministers and Parliament. |
| F10 | The risks associated with the absence of legislation requiring communications service providers to be intercept capable is compounded by the absence of a centralized national authority to coordinate, develop, and maintain lawful intercept capabilities in Canada. |

| | |
|---|---|
| R6 | The government table legislation to compel intercept capability for communications service providers (CSPs). The legislation should be encryption neutral and not include a decryption requirement. The government must also decide on a compensation model for compliance costs, i.e., whether CSPs should be compensated for the development, maintenance, and operating costs associated with lawful access.<br><br>The legislation should:<br><br>• establish and identify the national authority (i.e., the National Lawful Access Centre) for the coordination of lawful interception initiatives;<br>• define communications service provider so as to include any service provider operating in Canada offering electronic communications services or capabilities;<br>• define intercept capability to include support for computer network exploitation; and<br>• set mandatory technical standards, including those related to cybersecurity. |

## Jurisdictional Barriers

**186.** The Committee learned about how the cross-border flows of digital information inhibits national security investigations, which has become especially problematic as more Canadians use communications applications and services that are based in other countries. This dynamic is not new, and Canada has taken important steps to join international efforts to address such jurisdictional barriers, such as the signing and ratification of the Budapest Convention and the more recent signing of its *2nd Additional Protocol*. Canada and the U.S have also been negotiating a Data Access Agreement under the U.S. CLOUD Act. Once concluded, this encryption-neutral agreement will remove long-standing jurisdictional barriers to judicially-authorized access to U.S. CSPs, including major social media platforms. This is particularly important for CSIS, which cannot avail itself of the mutual legal assistance process that the RCMP uses. Canada stands to gain a lot from this agreement.

**187.** The Committee is concerned about the length of time it is taking Canada and the U.S. to negotiate this agreement. The Committee notes that since the passage of the CLOUD Act in 2018, the U.S. has concluded agreements with the U.K. and Australia in 2019 and 2021, respectively. *** the Committee is concerned that the government may find that it missed an opportunity to finalize an agreement if the U.S. decides to prioritize other countries for Data Access Agreements.

| | |
|---|---|
| F11 | The Canada-U.S. Data Access Agreement would remove long-standing jurisdictional barriers to judicially-authorized access to U.S. communications service providers, including major social media platforms, without compromising privacy or encryption. |

| | |
|---|---|
| R7 | The government prioritize the signing and implementation of the Canada-U.S. Data Access Agreement. |

## Assessing the Government's Response

**188.** The Committee notes that while successive governments have recognized these challenges, they have been largely ineffective at developing responses through policy solutions or legislative change. The government has not made any meaningful attempt to address lawful access since the 2016 green paper consultations in which Canadians clearly expressed concern about proposals to address lawful access challenges. The Committee would have found the government's response to this result reasonable, if concerted policy work to develop solutions that respected both concerns about privacy and the need to equip security agencies with modern tools and resources had continued.

**189.** However, the Committee found that, instead of reassessing the way forward, the government has let significant policy initiatives continue to languish. First, the Supreme Court rendered its *Spencer* decision on BSI over ten years ago. The government has not brought any proposals forward to deal with the BSI issue. Second, no government has attempted to address the absence of lawful intercept capability legislation since 2012. Third, the government's attempts to articulate a coherent policy on encryption have also demonstrated little progress. Finally, negotiations on a much needed Canada-U.S. Data Access Agreement have proceeded with little sense of urgency.

**190.** The cumulative effect of this approach to lawful access is that Canada now lags behind likeminded democracies who took strides over a decade ago to adapt their legal frameworks to fight national security threats in the digital age. In a global environment in which Canada will need to increasingly work with its international partners to address ideologically motivated violent extremism, serious organized crime, cybercrime, foreign interference, and other threats, this puts Canada at a disadvantage.

**191.** In the Committee's view, this legislative and policy inertia fundamentally comes down to a lack of political will. Lawful access has not featured in a single mandate letter since the government adopted the practice of making them public, which leads the Committee to infer that the government is unconvinced by the significance and impact of Canada's lawful access challenges. The Committee notes the complexity of the lawful access challenges, which cover the intersection of rapidly evolving technology, changing views on privacy,

legal frameworks and jurisprudence, and distinct but interrelated policy initiatives. One aspect of lawful access necessarily touches upon another, such that several implications must be considered before deciding on a course of action. The Committee suspects that this complexity in and of itself has also contributed towards the years of inertia.

**192.** The Committee also believes that the current situation may reflect the government's challenges in engaging effectively with Canadians who are concerned about their privacy.

## The Committee's Observations on the Debate about National Security and Canadians' Right to Privacy

**193.** The Committee agrees with the Privacy Commissioner's statement that there are ways to ensure that privacy and national security are respected concurrently, rather than one traded-off at the expense of another. The Committee is encouraged to note that none of the witnesses who appeared for this review depicted the balance of privacy and national security as a zero-sum game. Privacy advocates acknowledged that, in certain circumstances, security agencies required access to private communications in support of their national security investigations. National security practitioners regularly stressed the need for their electronic surveillance activities to be compliant with the Charter, serve a legitimate purpose, and be necessary and proportionate. All agreed that reducing the debate to a competing narrative of Canadians being either for "Big Brother" or for the protection of privacy was unhelpful. In the Committee's view, this suggests there is scope for key stakeholders to have a principled discussion about the way forward.

**194.** In order to do so, the Committee believes that it will be important for the government to close the gap between what Canadians *assume* security and intelligence organizations are able to do and the current reality. The Committee is aware that the RCMP and CSIS are unwilling and in some cases unable to share information publicly about investigative techniques and operational vulnerabilities. The Committee believes the rationale for limiting such information in the public sphere is largely reasonable. However, the information vacuum that this creates may perpetuate inaccurate assumptions that the capacity and resources of security and intelligence agencies are greater than they are. In the Committee's view, assertions about a "golden age of surveillance" may have been accurate a decade ago, but they do not fully reflect the current challenges faced by national security practitioners today.

**195.** The Committee believes the modernization of lawful access legislation is an issue in which transparency about technical details and capabilities will matter in order to dispel incorrect assumptions and address cybersecurity and privacy concerns. If the government is to make meaningful progress on lawful access reform, this will not be an effort in which it can rely on high level talking points when it engages with key stakeholders. The Committee notes that other like minded democracies have made progress in this regard, particularly the U.K. in the drafting, passage, and recent review of its *Investigatory Powers Act*. There are principled approaches to transparency that Canada can follow.

**196.** The Committee also believes there remains room for improvement in *how* the RCMP and CSIS interpret and respond to Canadians' concerns about privacy. For example, the Committee observed that CSIS and the RCMP regularly cited judicial authorization and the

complexity of the warrant process as evidence that privacy concerns had been addressed in the context of the use of lawful access techniques. The Committee suggests that this response, while reasonable, may not be effective, as it does not explicitly detail how either organization has assessed privacy concerns. In another example, when the BCCLA cited the Federal Court's 2016 ruling on CSIS' duty of candour, CSIS responded that it had since restored trust with the Court. In the Committee's view, this is not the point; the point is that amongst Canadians who are concerned about privacy, CSIS still has work to do to restore *their* trust.

**197.** Finally, the Committee notes Professor Goold's observation that privacy advocates often feel the need to "be on the defensive" when the government contemplates modernizing lawful access legislation. The Committee believes that if the government is to make any progress in advancing lawful access reform, a key pillar of its strategy should be to determine how to engage and communicate effectively with Canadians, particularly those who are concerned about privacy and the Charter, with a view to identifying and proactively addressing instances where both sides are talking past one another.

# Conclusion

**198.** Lawful access represents one of the most intrusive powers of the state in the protection of national security. Accordingly, Canadians expect strong safeguards for its use, including that it be prescribed by law, serve a legitimate purpose, and be necessary and proportionate. Canadians rightfully want to understand any proposals for new tools and authorities to security and intelligence organizations that have implications for their privacy. However, Canadians also expect security and intelligence organizations to have the tools, policies, and lawful authorities in place to conduct lawful access techniques. The Committee thinks Canadians would be surprised to learn how difficult it actually is for security and intelligence agencies to do so.

**199.** In reflecting upon the information that came to light over the course of its review, the Committee is concerned by the lawful access challenges described by the security and intelligence community and by the long-standing inability of successive governments to address them. The RCMP and CSIS may not be going completely dark, but it is not because new technologies and an abundance of metadata counterbalance the loss of access to communications content. Rather, they appear to be mitigating the challenges associated with encryption technologies, an outdated legal framework, and jurisdictional limits by managing – for now – increasing operational complexity and risk. The Committee is concerned, however, with how much of this successful mitigation presently relies upon the ingenuity of CSIS and the RCMP rather than the right configuration of tools, lawful authorities, and resources.

**200.** The Committee is equally concerned that, if left unaddressed, these challenges will undermine Canada's national security in the long term by increasingly hampering the ability of CSIS and the RCMP to fulfil their respective mandates. The failure to respond to these challenges may also impede Canada's continued ability to benefit from Five Eyes efforts to detect and respond to security threats if it cannot meaningfully contribute to this partnership.

**201.** In the Committee's view, the primary way the government could facilitate and enable national security investigations while at the same time protecting Canadians' right to privacy would be to modernize lawful access legislation, based on clearly articulated principles that reaffirm the requirement for a legitimate need for exceptional, targeted and judicially authorized access, emphasize privacy and cybersecurity protections, and define transparency and oversight mechanisms. In light of the complexity of the lawful access challenge, the Committee suggests that the government implement an incremental approach to allow for meaningful engagement with stakeholders and a diversity of input.

**202.** It is critical, however, that the government approach these issues proactively. There are examples internationally of like minded democracies having hurriedly passed controversial lawful access legislation in response to serious national security events. Parliamentarians should have the opportunity to debate new legislation about lawful access with clear eyes and careful consideration, not in a rushed, emotional debate in reaction to a national tragedy. The longer these issues are kept on the backburner, the more the government opens itself up to the risk of following a similar path.

**203.** These challenges are not new. Successive governments have been aware of them for some time. It is time for the government to act and provide the security and intelligence community with the tools, policies, and lawful authorities they require to do the work asked of them in the manner expected by Canadians which is responsive to and protective of their privacy.

# Findings

**204.** The Committee makes the following findings.

| | |
|---|---|
| F1 | Canada's security and intelligence organizations do not systematically track how often they encounter technological challenges in their national security investigations and whether they are successful in mitigating these challenges. |
| F2 | The RCMP and CSIS face significant challenges in accessing communications content, for which metadata is not necessarily a substitute. |
| F3 | There was consensus across appearances that legislation to compel the creation of exceptional access or "backdoors" to encryption platforms was neither required nor desired. |
| F4 | Canada's public position on lawful access to encrypted communication is unclear. National security practitioners, cybersecurity experts and privacy advocates do not have a common understanding of the problem. |
| F5 | The government's failure to develop and implement a solution to the Supreme Court's decision in *Spencer* is impeding CSIS and the RCMP's ability to respond to national security threats. |
| F6 | Without a general legal requirement on CSPs to retain metadata for a specified period of time, there is a risk that data sought pursuant to a warrant will be unavailable. |
| F7 | The government's inability to make progress on the intelligence and evidence dilemma, particularly with respect to the protection of investigative techniques, has contributed to a situation in which the RCMP is forced to choose either to not use sensitive tools and techniques during an investigation because of the potential disclosure issues, or risk not being able to rely on evidence obtained through their use at trial or having a prosecution stayed because of a court order to disclose. |
| F8 | The government lacks formal policies to address the procurement, regulation and use of commercial On-Device Investigative Tools, and ensure transparency in reporting with respect to their use by law enforcement and CSIS. |
| F9 | The absence of legislation requiring communications service providers (CSPs) to maintain lawful intercept capability creates unnecessary risks for all stakeholders, including CSIS, federal, provincial, territorial and municipal law enforcement, CSPs and ultimately the Canadian public. It also impedes Canada's ability to work with international partners. The failure to address this issue at a strategic policy level has resulted in operational agencies themselves developing foundational policies and procedures, notably compensation models, geared toward ensuring continued cooperation from CSPs, rather than a principled approach based on input from Ministers and Parliament. |
| F10 | The risks associated with the absence of legislation requiring communications service providers to be intercept capable is compounded by the absence of a centralized national authority to coordinate, develop, and maintain lawful intercept capabilities in Canada. |

| | |
|---|---|
| F11 | The Canada-U.S. Data Access Agreement would remove long-standing jurisdictional barriers to judicially-authorized access to U.S. communications service providers, including major social media platforms, without compromising privacy or encryption. |

# Recommendations

**205.** The Committee makes the following recommendations:

| | |
|---|---|
| R1 | Under the leadership of the Minister of Public Safety, the government develop and implement a comprehensive strategy to address Canada's lawful access challenges, drawing from the Committee's review and findings. Such a strategy should:<br>• Affirm key principles, such as legitimacy, necessity, and proportionality;<br>• Identify, track, and report on key lawful access challenges and associated risks;<br>• Include communications, stakeholder engagement and transparency commitments; and<br>• Consider challenges that may arise due to emerging technology, e.g., artificial intelligence. |
| R2 | The government publicly clarify its position on exceptional access to communications information protected by encryption. |
| R3 | The government table legislation creating new authorities in the *Canadian Security Intelligence Service Act* and the *Criminal Code* to enable the production of basic subscriber information, and the government consider legislation with respect to data retention. |
| R4 | Further to the Committee's 2024 recommendation in its *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* that the government address intelligence and evidence challenges, the government develop and implement a solution to address concerns about the protection of investigative tools, which may include revisions to the relevant provisions of the *Canada Evidence Act*. |
| R5 | The government develop policies and guidelines on the procurement, use and reporting requirements for commercial On-Device Investigative Tools. |

| | |
|---|---|
| R6 | The government table legislation to compel intercept capability for communications service providers (CSPs). The legislation should be encryption neutral and not include a decryption requirement. The government must also decide on a compensation model for compliance costs, i.e., whether CSPs should be compensated for the development, maintenance, and operating costs associated with lawful access.<br><br>The legislation should:<br>• establish and identify the national authority (i.e., the National Lawful Access Centre) for the coordination of lawful interception initiatives;<br>• define communications service provider so as to include any service provider operating in Canada offering electronic communications services or capabilities;<br>• define intercept capability to include support for computer network exploitation; and<br>• set mandatory technical standards, including those related to cybersecurity. |
| R7 | The government prioritize the signing and implementation of the Canada-U.S. Data Access Agreement. |

# Annexes

## Annex A: Terms of Reference

### Review

Framework review of the lawful interception of communications by security and intelligence organizations pursuant to s. 8(1)(a) of the *National Security and Intelligence Committee of Parliamentarians Act*.

### Overview

According to DoJ, lawful access consists of the legally authorized interception of communications and collection of information and data by intelligence and law enforcement organizations in the conduct of investigations. Intelligence and law enforcement agencies already have significant lawful access capabilities and authorities, but maintaining this lawful access in an environment of rapidly changing technology constitutes a significant challenge.

According to numerous open sources, the national security and intelligence community faces mounting challenges to their ability to intercept communications or access the content of those communications, even where the lawful authority to do so exists. This issue is commonly referred to as "going dark" by law enforcement, security and intelligence organizations, and results from the increasing prevalence and sophistication of end-to-end or strong encryption, as well as other technological changes that render existing intercept solutions unworkable.

At the same time, civil rights and security advocacy groups question government efforts to modernize authorities in this area, arguing that such modernization would violate the privacy rights of Canadians, or could compromise the security of online data.

### Objectives

As noted in the letter sent to the Ministers of Justice, National Defence and Public Safety, the review will examine the legislative, regulatory, policy and financial framework for the lawful interception of communications by security and intelligence organizations, the challenges of new and emerging technologies, including the use of end-to-end encryption, and any limitations of the current framework.

The objectives of the review are to examine:

- The current state of lawful access, including the challenges identified by the national security and intelligence community;
- Concerns and criticisms raised by civil society and privacy experts with respect to modernizing authorities in this area;
- The technological challenges relating to the lawful interception of communications, including end-to-end encryption and access to communication networks in real-time;

- The extent to which the security and intelligence community has mitigated the challenges of "going dark" through technology, policy and cooperation with communication service providers; and
- The extent to which gaps remain to address the impact of new and emerging technologies on the lawful interception of communications.

This review will include, but may not be limited to, the Canadian Security Intelligence Service, the Communications Security Establishment, the Department of Public Safety and Emergency Preparedness, the Royal Canadian Mounted Police, and the Department of Justice.

## Appearances

Following the provision of preliminary documentation, the Committee will hold appearances, the content of which will be determined by the results of the Committee's preliminary review of material provided.

## Timeline

The Secretariat and the Committee will identify deadlines for each stage of the review.

# Annex B: List of Witnesses

## Ministers

- The Honourable Dominic LeBlanc, P.C., M.P., Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs
- The Honourable Arif Virani, P.C., M.P., Minister of Justice and Attorney General of Canada

## Canadian Security Intelligence Service

- Director
- Director General, Scientific and Technical Services
- Deputy Director General, Counter Terrorism
- Deputy Director General, Scientific and Technical Services
- Deputy Director General, Scientific and Technical Services
- Chief, Scientific and Technical Services
- Deputy Chief, Scientific and Technical Services
- Director General, Policy and Foreign Relations

## Communications Security Establishment

- Director General, ***
- Director General, ***

## Department of Justice

- Associate Deputy Minister
- Deputy Assistant Deputy Minister, Policy Sector
- Counsel, Legal Services Unit, CSE
- Counsel, National Security Litigation and Advisory Group, CSIS
- Counsel, Legal Services Unit, RCMP

## Office of the Privacy Commissioner of Canada

- Privacy Commissioner of Canada
- Deputy Commissioner and Senior General Counsel
- Chief of Staff, Special Advisor and Counsel
- Executive Director, Policy, Research & Parliamentary Affairs

## Department of Public Safety

- Deputy Minister
- Senior Assistant Deputy Minister, National and Cyber Security
- Director, Intelligence Policy, National and Cyber Security Branch
- Acting Manager, Intelligence Policy Division, National and Cyber Security Branch
- Acting Special Advisor, Intelligence Policy Division, National and Cyber Security Branch

## Royal Canadian Mounted Police

- Deputy Commissioner, Federal Policing
- Deputy Commissioner, Specialized Policing Services
- Chief Superintendent, Technical Investigation Services
- Acting Executive Director, Technical Operations
- Director, CLOUD Act Program
- Sergeant, Lawful Access Liaison
- Sergeant, Technical Case Management Program
- Policy Analyst, Specialized Policing Services

## Non-governmental witnesses

- Representatives from six Canadian communications service providers
- Ronald Deibert, Director, The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
- Michael Geist, Professor, Faculty of Law, University of Ottawa
- Benjamin Goold, Professor, Allard School of Law, University of British Columbia
- Aislin Jackson, Policy Staff Counsel, British Columbia Civil Liberties Association
- Anil K. Kapoor, Kapoor Barristers
- Vivek Krishnamurthy, Associate Professor of Law and Director of the Samuelson-Glushko Technology Law and Policy Clinic, University of Colorado Law School

## Annex C: Acronyms and Abbreviations

| | |
|---|---|
| BCCLA | British Columbia Civil Liberties Association |
| BSI | Basic subscriber information |
| Budapest Convention | *Budapest Convention on Cybercrime* (Council of Europe) |
| *Charter* | Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982*, 1982, c 11 (U.K.) |
| CLOUD Act | *Clarifying Lawful Overseas Use of Data Act* (U.S.) |
| CNE | Computer network exploitation |
| CSE | Communications Security Establishment |
| CSIS | Canadian Security Intelligence Service |
| CSP | Communications service provider |
| DMNS | Deputy Ministers' Committee on National Security |
| DoJ | Department of Justice |
| ETHI | Standing Committee on Access to Information, Privacy and Ethics (House of Commons) |
| Five Eyes | Australia, Canada, New Zealand, the U.K., and the U.S. |
| FPT | Federal, Provincial, and Territorial |
| G7 | Group of Seven: Canada, France, Germany, Italy, Japan, the U.K., and the U.S. |
| IP | Internet Protocol |
| MLAT | Mutual legal assistance treaty |
| NLAC | National Lawful Access Centre |
| NSICOP, or the Committee | National Security and Intelligence Committee of Parliamentarians |
| NS-TAG | National Security Transparency Advisory Group |
| ODIT | On-Device Investigative Tool |
| OPC | Office of the Privacy Commissioner of Canada |
| PPSC | Public Prosecution Service of Canada |
| Public Safety | Department of Public Safety and Emergency Preparedness |
| RFA | Request for assistance |
| SCC | Supreme Court of Canada |
| SECU | Standing Committee on Public Safety and National Security (House of Commons) |
| SOLGEN Standards | Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications |
| U.K. | United Kingdom |
| U.S. | United States |

# Annex D: Glossary

| | |
|---|---|
| Backdoor | An undocumented, private, or less detectable-way of gaining remote access to a computer, bypassing authentication measures, and obtaining access to plaintext.[374] |
| Basic subscriber information | Basic identifying information that corresponds to a customer's telecommunications subscription. This can include name, home address, phone number, email address, and/or IP address. BSI does not include the contents of communications.[375] |
| Carrier | An entity that operates a transmission facility used to provide telecommunications services to the public for compensation.[376] |
| Computer network exploitation | Tools and techniques that exploit vulnerabilities in systems or software to surreptitiously obtain data that is stored on or transiting communications networks.*** |
| Communications service provider | An entity that offer telecommunications services or some combination of information and media services, content, entertainment, and application services over networks.[378] |
| Encryption | The conversion of information from one form to another to hide its content and prevent unauthorized access.[379] |
| Internet of Things | A variety of everyday web-enabled "smart" objects, such as personal fitness trackers, televisions and cars, with embedded sensors, electrical components and software collecting data and information from their surroundings.[380] |
| IP address | A numerical identification and logical address that is assigned to devices participating in a computer network.[381] |
| Lawful access | The judicially authorized interception of electronic communications, and the search and seizure of electronic information, in accordance with Canada's legal framework.[382] |
| Metadata | Data about data, or an informal term for transmission data. In the context of communications, metadata is the who, where, when, how and with whom of a communication, but not the contents of the communication.[383] |
| On-Device Investigative Tool | A term the RCMP uses to refer to its computer network exploitation tools. |

374 CCCS, "Glossary," undated.
375 Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016: Background Document*, 2016.
376 *Telecommunications Act* (S.C. 1993, c. 38), s. 2(1).
377 ***
378 Lawful Access Advisory Committee, "Governance Framework," May 2024.
379 Canadian Centre for Cyber Security, "Glossary," undated.
380 Canadian Centre for Cyber Security, "Internet of Things (IoT) Security – ITSAP.00.012," July 2022.
381 OPC, "What an IP Address Can Reveal About You," May 2013.
382 DoJ, Industry Canada, and Solicitor General of Canada, "Lawful Access – Consultation Document," 2002.
383 Adapted from U.K. Home Office, "Fact sheet: communications data," July 8, 2016.

| | |
|---|---|
| Virtual private network | A private communications network used to communicate over a wider network. VPN communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the VPN. [384] |
| Vulnerability | A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations. [385] |

384 Canadian Centre for Cyber Security (CSE), "Glossary," undated.
385 Canadian Centre for Cyber Security (CSE), "Glossary," undated.

# Annex E: Timeline of Lawful Access Legislative Efforts in Canada since 2001

| 2005 | |
|---|---|
| Bill C-74, *Modernization of Investigative Techniques Act* | |
| **PURPOSE** | **OUTCOME** |
| • Compel communication service providers to have the capability to intercept communications on their networks, including decryption.<br>• Allow law enforcement to obtain subscriber information from communication service providers without prior judicial authorization. | • Died on the Order Paper.<br>• Dissolution of Parliament. |

| 2009 | |
|---|---|
| Bill C-46, *Investigative Powers for the 21st Century Act*<br>Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act* | |
| **PURPOSE** | **OUTCOME** |
| Similar or same provisions as previous bill.<br>Addition:<br>• Establish new judicial authorities: preservation demands and orders, transmission and tracking production orders.<br>• Establish warrants for transmission and tracking data capture in real time.<br>• Update mutual assistance legislation. | • Died on the Order Paper.<br>• Prorogation of Parliament. |

| 2010 | |
|---|---|
| Bill C-50, *Improving Access to Investigative Tools for Serious Crimes Act*<br>Bill C-51, *Investigative Powers for the 21st Century Act*<br>Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act.* | |
| **PURPOSE** | **OUTCOME** |
| Similar or same provisions as previous bills.<br>Addition:<br>• Allow for supplementary judicial orders concurrently to an interception authorization.<br>• Reporting and safeguard requirements for lawful access related judicial authorizations. | • Died on the Order Paper.<br>• Dissolution of Parliament. |

| 2012 | |
|---|---|
| Bill C-30, *Protecting Children from Internet Predators Act* | |
| **PURPOSE** | **OUTCOME** |
| Similar or same provisions as previous bills.<br><br>Addition:<br><br>• Specifications of maximum duration for judicial authorities. | • Not pursued by government.<br>• Died on the Order Paper. |

| 2013 | |
|---|---|
| Bill C-13, *Protecting Canadians from Online Crime Act.* | |
| **PURPOSE** | **OUTCOME** |
| Similar or same provisions as previous bill.<br><br>Includes:<br><br>• Establish new judicial authorities: preservation demands and orders, transmission and tracking production orders.<br>• Establish warrants for transmission and tracking data capture in real time.<br>• Allow for supplementary judicial orders concurrently to an interception authorization.<br>• Reporting and safeguard requirements for lawful access related judicial authorizations.<br>• Specifications of maximum duration for judicial authorities.<br>• Update mutual assistance legislation.<br><br>Excludes:<br><br>• Compel communication service providers to have the capability to intercept communications on their networks, including decryption.<br>• Allow law enforcement to obtain subscriber information from communication service providers without judicial authorization. | • Received royal assent on December 9, 2014.<br>• Came into force on March 9, 2015. |

| 2017 | |
|---|---|
| Bill C-59, *An Act Respecting National Security Matters.* | |
| **PURPOSE** | **OUTCOME** |
| Several measures changing Canada's national security framework.<br><br>Includes:<br><br>• Separate enabling statute for CSE and expansion of mandate.<br>• Authorization for CSIS regarding dataset collection, retention, and creation. | • Received royal assent on June 21, 2019.<br>• Came into force in phases starting in July 2019. |