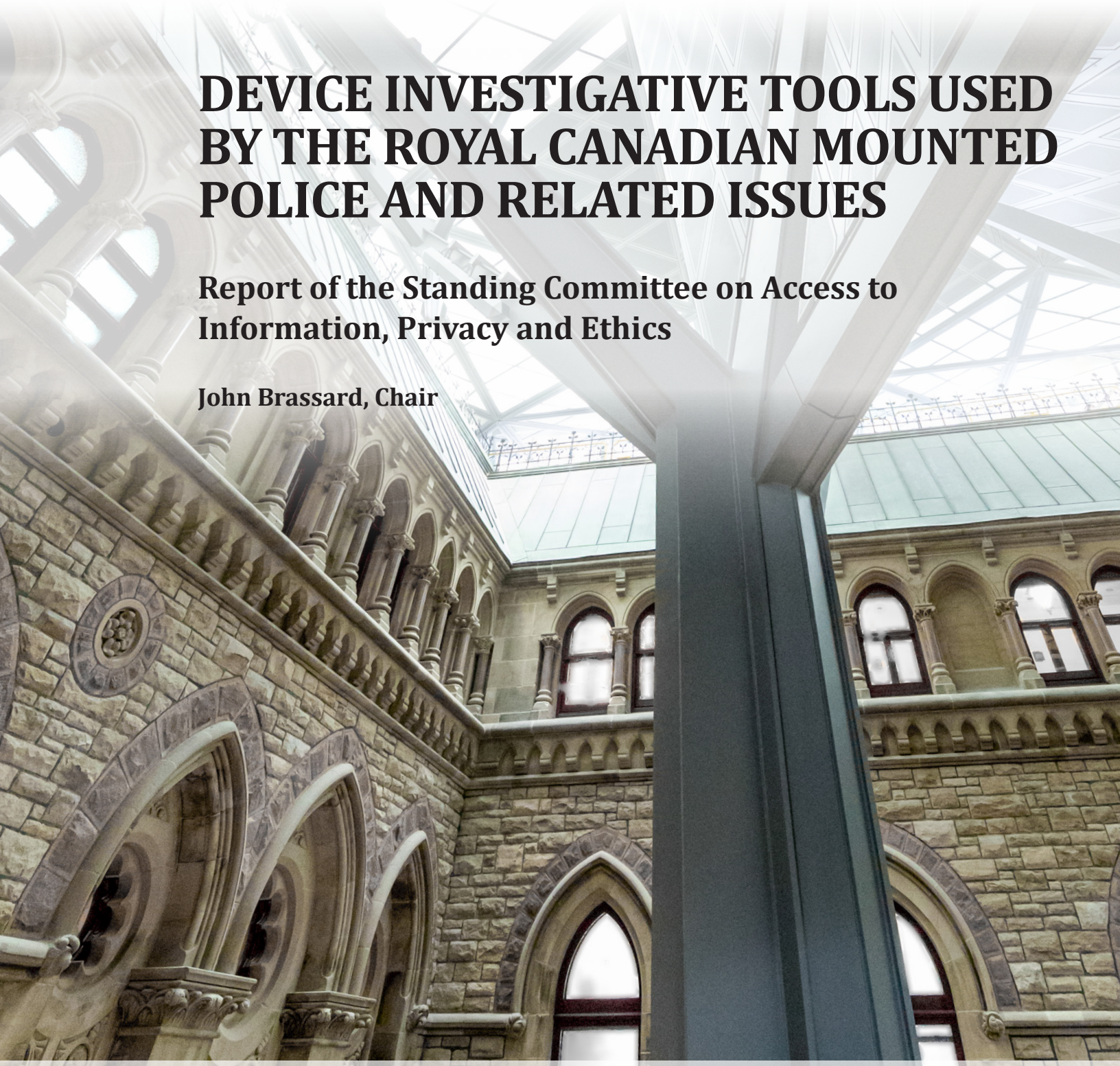
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA



DEVICE INVESTIGATIVE TOOLS USED BY THE ROYAL CANADIAN MOUNTED POLICE AND RELATED ISSUES

Report of the Standing Committee on Access to Information, Privacy and Ethics

John Brassard, Chair

NOVEMBER 2022
44th PARLIAMENT, 1st SESSION

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Standing Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website
at the following address: www.ourcommons.ca

DEVICE INVESTIGATIVE TOOLS USED BY THE ROYAL CANADIAN MOUNTED POLICE AND RELATED ISSUES

Report of the Standing Committee on Access to Information, Privacy and Ethics

John Brassard
Chair

NOVEMBER 2022

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

John Brassard

VICE-CHAIRS

Iqra Khalid

René Villemure

MEMBERS

Parm Bains

Michael Barrett

Hon. Greg Fergus

Jacques Gourde

Matthew Green

Lisa Hepfner

Damien C. Kurek

Ya'ara Saks

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

James Bezan

Kelly Block

Sukh Dhaliwal

Nathaniel Erkine-Smith

Ken Hardie

Arielle Kayabaga

Pat Kelly

Francis Scarpaleggia

Brenda Shanahan

Doug Shipley

Jasraj Singh Hallan

Francesco Sorbara

Rechie Valdez
Anita Vandenbeld
Ryan Williams

CLERK OF THE COMMITTEE

Nancy Vohl

LIBRARY OF PARLIAMENT

Parliamentary Information, Education and Research Services

Sabrina Charland, Analyst
Alexandra Savoie, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

SEVENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(h), the committee has studied the device investigation tools used by the Royal Canadian Mounted Police (RCMP) and has agreed to report the following:

TABLE OF CONTENTS

LIST OF ACRONYMS IX

SUMMARY 1

LIST OF RECOMMENDATIONS 3

ON-DEVICE INVESTIGATIVE TOOLS USED BY THE ROYAL CANADIAN MOUNTED POLICE AND RELATED ISSUES 5

- Introduction 5
  - Background 5
  - Organization of the Report 6
- Chapter 1: On-Device Investigative Tools Such as Spyware 7
  - Benefits of Technological Investigative Tools 8
  - Concerns About the Use of Technological Investigative Tools 9
    - Privacy and Freedom 9
    - Confidence in Institutions and Transparency 12
    - National Security and the Use of Spyware by Foreign Entities 16
- Chapter 2: Use of On-Device Investigative Tools by the Royal Canadian Mounted Police 19
  - Description of On-Device Investigative Tools Used by the Royal Canadian Mounted Police 19
  - High Legal Threshold 21
  - Judicial Authorization and Internal Process 22
  - Privacy Impact Assessment 24
- Chapter 3: Modernization of the Legislative Framework and Other Measures 26
  - Modernization and Enhancement of Part VI of the *Criminal Code* 27
  - Modernizing the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* 28
  - Moratorium or Ban 31

Other Measures 32
Committee Observations and Recommendations 34
Conclusion 36

APPENDIX A LIST OF WITNESSES 37

APPENDIX B LIST OF BRIEFS 39

REQUEST FOR GOVERNMENT RESPONSE 41

LIST OF ACRONYMS

CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
NTOP	RCMP National Technology Onboarding Program
ODIT	On-Device Investigative Tool
OPC	Office of the Privacy Commissioner
PIA	Privacy Impact Assessment
PIPEDA	*Personal Information Protection and Electronic Documents Act*
RCMP	Royal Canadian Mounted Police
TIS	Technical Investigation Services
TIS CAIT	RCMP Technical Investigation Services Covert Access and Intercept Team

SUMMARY

As new technology is developed, law enforcement agencies, such as the Royal Canadian Mounted Police (RCMP), are faced with increasing challenges in gathering digital evidence. As such, these agencies must turn to more sophisticated technological investigative tools to access the information they seek to obtain in certain criminal investigations. On-device investigation tools are an example of such tools.

This report examines the benefits and risks of the use of on-device investigative tools and the use of such tools by the RCMP. It also examines legislative and non-legislative measures that could be considered to better regulate these types of tools in Canada.

Based on the evidence heard and the briefs received, the committee makes several recommendations to reassure Canadians that, when new technology is used by law enforcement agencies, Canadian laws take into account not only the challenges these agencies face in performing their duties, but also the right to privacy and the importance of maintaining, in a democratic society, the public's confidence in the institutions charged with protecting them.

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1

That the Government of Canada amend the *Privacy Act* to include an explicit obligation for government institutions to conduct privacy impact assessments before using high-risk technological tools to collect personal information and to submit them to the Office of the Privacy Commissioner of Canada for assessment. 34

Recommendation 2

That the Government of Canada create a list of banned spyware vendors and establish clear rules on export controls over surveillance technologies. 34

Recommendation 3

That the Government of Canada review Part VI of the *Criminal Code* to ensure that it is fit for the digital age. 35

Recommendation 4

That the Government of Canada amend the preamble to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to indicate that privacy is a fundamental right. 35

Recommendation 5

That the Government of Canada regularly remind former elected or appointed members or any individuals who have previously worked for a national security agency of their lifetime obligations under the *Security of Information Act* and obtain acknowledgment of their understanding of these obligations. 35

Recommendation 6

That the Government of Canada grant the Office of the Privacy Commissioner of Canada the power to make recommendations and issue orders in both the public and private sectors when it finds violations of the laws for which it is responsible. 35

Recommendation 7

That the Government of Canada amend the *Privacy Act* to include the concept of privacy by design and an obligation for federal institutions subject to the Act to meet this standard when developing and using new technologies. 35

Recommendation 8

That the Government of Canada establish an independent advisory body composed of relevant stakeholders from the legal community, government, police and national security, civil society, and relevant regulatory bodies, like the Office of the Privacy Commissioner of Canada, to review new technologies used by law enforcement and to establish national standards for their use..... 35

Recommendation 9

That the Government of Canada amend the *Privacy Act* to include explicit transparency requirements for government institutions, except where confidentiality is necessary to protect the methods used by law enforcement authorities and ensure the integrity of their investigations. 35

ON-DEVICE INVESTIGATIVE TOOLS USED BY THE ROYAL CANADIAN MOUNTED POLICE AND RELATED ISSUES

INTRODUCTION

As individuals who commit crime make use of new technologies, for example, encryption tools, law enforcement agencies, such as the Royal Canadian Mounted Police (RCMP), have to adapt their investigative tools. One such adaptation is the use of on-device investigative tools.

However, as will be outlined in this report, the intrusiveness of these tools and the risks they may pose to privacy are raising concerns not only about their use by law enforcement, but also their use in the private sector.

Background

On 22 June 2022, the Government House Leader tabled a response to a question on the *Order Paper* in the House of Commons with regard to government programs conducting surveillance or gathering information from Canadians through their phones and other mobile devices. The question asked for details of such programs since January 2020.[1]

The response tabled in the House of Commons indicates that the RCMP has been using on-device investigative tools as part of targeted investigations in recent years. It describes two specific RCMP programs that led to the use of these tools: the Technical

1 House of Commons, *Order/Address of the House of Commons*, Q-566, 22 June 2022, p. 2. The written question was the following: "May 6, 2022 — Mr. Van Popta (Langley—Aldergrove) — With regard to government programs conducting surveillance or gathering information from Canadians through their phones or other mobile devices, including programs involving anonymized data: what are the details of these programs since January 1, 2020, including, for each, (i) the name of program, (ii) the date the program began, if it began after January 1, 2020, (iii) the description of the data being collected, (iv) the purpose of the program, (v) the description of how the data is collected, (vi) the department or agency responsible for overseeing the program, (vii) whether or not the privacy commissioner was consulted before the program was implemented, (viii) the concerns raised by the privacy commissioner, (ix) how each concern was addressed, (x) the end date of the program, (xi) the number of Canadians who had their data tracked?"

Investigation Services Covert Access and Intercept Team (TIS CAIT) and the Technical Investigations Special "I" Program.[2]

In July 2022, after the response was tabled and both RCMP programs were revealed, the Committee passed a motion to study the RCMP's use of on-device investigative tools, referred to as "ODITs" by the organization.

The Committee held four public meetings and one *in camera* meeting and heard from 12 witnesses. It also received two briefs. The Committee would like to thank all those who contributed to the study.

Organization of the Report

The report is divided into three chapters. Chapter 1 provides a broad description of spyware and different on-device investigative tools, in addition to an overview of the benefits and concerns surrounding their use. Chapter 2 looks specifically at the RCMP's use of on-device investigative tools. Chapter 3 discusses the modernization of the legislative framework applicable to the use of surveillance technologies by law enforcement and others. It also provides an overview of other measures that would allow for a better oversight of the use of these technological tools in Canada. The recommendations of the Committee are found at the end of the last chapter.

2 House of Commons, *Order/Address of the House of Commons*, Q-566, 22 June 2022, pp. 92-99. According to the information provided in the response, "CAIT techniques and tools are used primarily to collect data from mobile devices and other electronic devices used by suspects associated to serious criminal and national security matters" and "Special 'I' techniques are used primarily to perform lawful electronic surveillance with regards to covert audio, video, tracking and alarms." The response indicates that the CAIT program was established in 2016, but similar activities were conducted by the RCMP's Network Information Operations Team prior to that. The Special "I" program exists since approximately 1975; Royal Canadian Mounted Police, *Letter to Committee*, 16 September 2022. Brenda Lucki, Commissioner of the RCMP, indicates that the RCMP has been using "digital intercepts tools of different variety for approximately two decades" and that "[b]y 2017, as technological advancements to combat criminality continued to increase, the RCMP recognized a necessity to further enhance its records management practices to maintain specific ongoing central records of ODIT deployments."

CHAPTER 1: ON-DEVICE INVESTIGATIVE TOOLS SUCH AS SPYWARE

> **"[Spyware] is extraordinarily powerful surveillance technology. Keep in mind that we live in a different time than even 20 years ago, when a wiretap was something you put on a landline, or you'd place a bug or a GPS tracker in a suspect's car. This gives you all of that and more, because these devices are designed by their manufacturers to be as invasive as possible."**
>
> Ronald J. Deibert,
> Professor of Political Science, and Director,
> Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto,
> who appeared before the Committee on 9 August 2022.

Ronald J. Deibert, a Professor of Political Science and the Director of the Citizen Lab based at the Munk School of Global Affairs and Public Policy at the University of Toronto, explained that there are several types of spyware, but the most sophisticated can provide persistent, silent, and unfettered access to a target's device, without the owner of the device knowing. He said that the latest versions of this spyware use "zero-click" versions, meaning that there is no need to trick a target into clicking on the link of a fake message. A "user, a government client of spyware, can simply issue a command to take over any device in the world that's vulnerable to this type of exploit."

Dr. Deibert added that once the spyware is inside a device, anything is possible for the software user. The user can intercept and listen to phone calls, access emails and text messages (even those that are encrypted), silently turn on the camera and microphone, see the individual's contacts, alter files, access a person's cloud, and track their location. In his view, this spyware is "designed, as well as the apps contained in them, to track every aspect of our lives, so this is a gold mine of information that is available to clients of spyware." In short, manufacturers design them to be as intrusive as possible. As will be explained in further details in Chapter 2, ODITs used by the RCMP can accomplish the many functions listed by Dr. Deibert, when they are deployed after obtaining a judicial authorization.[3]

3 Royal Canadian Mounted Police, *On-Device Investigative Tool (ODIT) Technical Description Draft for Project*, 8 August 2022, paras. 13 and 14; ETHI, *Evidence*, Dave Cobey.

Benefits of Technological Investigative Tools

Public Safety Minister, the Honorable Marco Mendicino mentioned the close link between technology and policing. In his view, the exponential growth of technology makes it imperative for law enforcement agencies to implement technological tools so they can continue to effectively "pursue those who would exploit new technologies for malicious intent." He said that the state uses these tools "to protect the security, safety and health of Canadians."

Sergeant Dave Cobey (Sgt.), from the Technical Case Management Program of the RCMP's Technical Investigation Services, explained that on-device investigative tools can help with evidence collection because like most people, criminals also have devices, which they use in a more complex way. This new reality is not conducive to old-fashioned wiretap activities that allowed law enforcement to send an order to a telecommunications company to obtain communications. According to Sgt. Cobey, this makes the RCMP's use of ODITs essential.

Deputy Commissioner Bryan Larkin (D/Commr.), from the RCMP's Specialized Policing Services, emphasized that encryption is essential in the modern world, because it "protects financial and other sensitive information and helps ensure that Canadians' online activities remain safe and private." However, it also helps criminals conduct illegal activities without police detection. ODITs helps to put a stop to these illegal activities by providing law enforcement agencies, such as the RCMP, with the capability to secretly collect private communications and other data that can no longer be obtained through old-fashioned wiretap activities or other less intrusive investigation techniques.

Daniel Therrien, the former privacy commissioner of Canada, also acknowledged that although encryption has many benefits for society and helps protect the privacy of Canadians' communications and commercial transactions, it can pose a serious challenge for law enforcement authorities. In his view, "to have technology to address the challenges of encryption with judicial authorization on a case-by-case basis" is acceptable.

According to Sharon Polsky, president of the Privacy and Access Council of Canada, technology itself is "morally neutral." It is "how its use is justified" that determines if it is more beneficial than concerning. She acknowledged that spyware could help police do their work but pointed out that it is more commonly used by others for malicious purposes, such as human trafficking.

Nevertheless, she noted that if the question is whether there are any social benefits of spyware, the answer is a "resounding yes," even though this may seem contradictory. In her view, spyware is:

> … [T]he Ford Pinto of technology, a danger hidden to the public in general and to certain people in particular with lots of socially beneficial spinoff jobs, commerce and taxes.

Ms. Polsky mentioned, for example, that the global cybercrime industry generates more than US$1.5 trillion per year. The global cybersecurity industry generates US$1.7 trillion per year, while the Canadian cybersecurity industry generates US$3.5 billion per year.

Concerns About the Use of Technological Investigative Tools

Privacy and Freedom

Multiple witnesses raised concerns about the use of on-device investigative tools by the RCMP or other government entities, and spyware generally, especially about how these tools could violate Canadians' freedom and right to privacy.

The Committee was particularly concerned about the potential use of the Pegasus software, created by the NSO Group.[4] The response to the question on the *Order Paper* tabled in the House of Commons on 22 June 2022 reveals that the RCMP uses on-device investigative tools in targeted investigations, without, however, mentioning the name of the software used.

Minister Mendicino, reassured the Committee that the Pegasus spyware is not used by the RCMP.

D/Commr. Larkin also confirmed that "the RCMP has never procured or used the Pegasus software, or any other NSO product." Other witnesses said that they were not aware of any use, by Canadian government entities or the RCMP, of the Pegasus spyware from the NSO Group.[5]

---

4 See for example: Amnesty International, *Briefing on Recommendations to the European Union to End Unlawful Targeted Surveillance*. The Pegasus Project is a collaboration between journalists and human rights organizations, such as Amnesty International, which was coordinated by Forbidden Stories. This investigation revealed how different countries targeted journalists, lawyers and politicians by using spyware sold by cybersurveillance company NSO Group: Pegasus.

5 ETHI, *Evidence*, Philippe Dufresne; ETHI, *Evidence*, Marco Mendicino; ETHI, *Evidence*, Bryan Larkin; Royal Canadian Mounted Police, *Letter to Committee*, 4 August 2022.

However, Michel Juneau-Katsuya, an expert and researcher on national security and intelligence, said that it was likely that agencies other than the RCMP, such as the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), use technology similar to Pegasus.

Assistant Commissioner Mark Flynn (A/Commr.), for the national security, and protective policing at the RCMP, confirmed that the RCMP works in partnership with various national security agencies, including CSIS, CSE and the Canada Border Services Agency. However, he assured the Committee that these relationships do not expand the RCMP's powers.

Ms. Polsky pointed out that there are several other platforms and that Pegasus is simply the latest spyware to make headlines.[6] She expressed concern that this "lucrative new sector," of which spyware is a part, is creating uncertainty about Canadians' privacy, freedom, and democracy. She added that Pegasus reminds us that spyware is a non-partisan endeavour, and that counterterrorism tools "have made us all fair game to be targeted and our words used against us."

Mr. Juneau-Katsuya also noted that, in addition to the spyware used on mobile devices, there are other forms of surveillance technology, such as aerial and drone surveillance. For example, he said that drones are being used by other departments, "particularly National Defence."

Other witnesses noted that while this study deals with the RCMP's use of spyware, they suspect other government agencies such as CSIS and CSE are using on-device investigative tools to intercept communications, without disclosing the details of that use.[7]

When asked whether entities under his purview other than the RCMP have used on-device investigative tools, Minister Mendicino stated that "these techniques, if and when they are used, are always done in a manner that is consistent with the law and the Charter."

Other examples of the risks to privacy and freedom on-device investigative tools and spyware may present were provided by witnesses. For example, Dr. Deibert said that Citizen Lab investigators have "documented extensive harms and abuses in just about every jurisdiction in which spyware is deployed." They discovered that

6 ETHI, *Evidence*, Sharon Polsky.

7 ETHI, *Evidence*, Daniel Therrien; ETHI, *Evidence*, Michel Juneau-Katsuya.

> [g]overnments routinely use spyware to hack civil society, political opposition, journalists, lawyers, activists, family members and other innocent victims–both domestically and abroad—including victims living here in Canada.

As indicated above, the global cybercrime industry and the global cybersecurity industry, which may require the use or sale of on-device investigative tools such as spyware, are very lucrative. Dr. Deibert indicated, for example, that "the spyware industry has a very strong appetite to sell to local law enforcement, where the abuses tend to be more problematic."

Brenda McPhail, the Director of the Privacy, Technology and Surveillance Program at the Canadian Civil Liberties Association, also argued that the use of these tools encourages law enforcement to exploit vulnerabilities in technologies on which we all depend, instead of working to fix our devices' and software's vulnerabilities.

In fact, several witnesses mentioned that spyware is able to perform because of technological shortfalls. For example, Ms. Polsky expressed concern that "[n]obody is talking about how the spyware is able to take advantage of the shortcomings, the deficiencies in so many software programs." She noted that our daily technologies are ill-equipped to protect us from spyware programs that are all "available commercially to anybody who has an Internet connection and wants to download them."

Dr. Deibert said that Citizens Lab routinely performs forensic analysis on victims of spyware and that in several instances, they have made responsible disclosures to the vendors, which have resulted in security patches affecting billions of people worldwide. He believes government agencies should follow suit, because if "the government is going to withhold that information from the vendors and put all of our safety at risk, there needs to be a proper process around that." This process is typically called the "vulnerabilities equities process."

Mr. Therrien agreed that when "government officials see a vulnerability in a system, they should notify the creator or the vendor of the system of the vulnerability as a principle generally applicable and implemented."

Some witnesses noted that there are gaps in the legislative framework applicable to on-device investigative tools and spyware with respect to the protection of privacy, namely the *Criminal Code*, which prohibits certain conducts and the interception of communications without warrant, and federal privacy laws. For example, Ms. Polsky said that the *Criminal Code,* as far as she is aware, does not address the installation by somebody of spyware on a phone, only the crime committed with such software (e.g.,

the sharing of intimate pictures). Ms. McPhail and Mr. Therrien both underscored that Canada's privacy regime has fallen behind, in both the public and private sectors.

Finally, Mr. Juneau-Katsuya underscored the importance of protecting privacy as defined in the *Canadian Charter of Rights and Freedoms* and Canadian laws by explaining that "[p]rivacy protection is one of the cornerstones of a healthy democracy and, without it, there can be no democracy." He added that "relevance, lawfulness, legitimacy and accountability" with respect to "the use of one or more technologies that make it possible to intercept conversations or obtain [private] information" may be protected under the *Privacy Act*. He also said that "the idea that the end justifies the means is not an acceptable argument when conducting criminal or national security investigations." The RCMP must follow the law. The modernization of the legislative framework will be discussed in further details in Chapter 3.

Confidence in Institutions and Transparency

Some witnesses noted the importance of maintaining public confidence in government institutions and identified proactive transparency as a means to foster that trust.

Philippe Dufresne, the Privacy commissioner of Canada, said that the Office of the Privacy Commissioner (OPC) was not informed or consulted on the RCMP's ODITs program prior to or since its implementation. He added that the OPC became aware of the RCMP's use of on-device investigative tools in the media in late June 2022 and that the OPC had to reach out to the RCMP to obtain additional information. The RCMP subsequently scheduled a demonstration for the OPC's officials in late August 2022.[8]

Regarding the benefit of releasing information about the RCMP's use of on-device investigative tools, Mr. Dufresne said:

> [T]he impact of this type of information coming out in the public through media reports or questions can raise questions and can raise concerns. I think from a trust standpoint and generating confidence, it would be far preferable that privacy impact assessments be done at the front end, that my office be consulted, and that this can be conveyed somehow to Canadians so that they are reassured that there are institutions there, such as my office, to provide advice and to make sure that privacy is top of mind.

8 In 2011, the Office of the Privacy Commissioner established a Technology Analysis Directorate staffed by highly skilled information technology research analysts with capabilities and expertise in different areas of technology, including reverse engineering and malware analysis. Office of the Privacy Commissioner, *Letter to Committee*, 22 August 2022.

Minister Mendicino said that he found it "unfortunate" that the Privacy Commissioner learned about the use of this investigative technique in the media. M. Dufresne stated that "[i]n its response to the question on the Order Paper, the RCMP indicated that it began drafting a [Privacy Impact Assessment] in relation to these tools in 2021, but [OPC officials] have not yet seen it."

Mr. Therrien added the following with respect to the tool used by the RCMP:

> I was surprised by the tool itself, by how intrusive it is, and that it was used for so long. Certainly, there have been many discussions over the years—as the RCMP said yesterday, probably since the early 2000s—on the lawful access issue. Both in my term as commissioner and when I was at the Department of Justice, I was following and part of these discussions. But the use of this particular tool to go around encryption, yes, was a surprise.

Mr. Dufresne said that ensuring privacy is a way of enhancing Canadians' trust in their institutions. In his view, when

> organizations such as the RCMP consider privacy impacts at the front end and are seen to be doing so, this generates trust and reassures Canadians about the necessity of the tools and the measures put in place to mitigate privacy impacts and ensure proportionality between the measures and the objectives.

According to Mr. Therrien, the Committee's study concerns "the fundamental condition that must exist so that Canadians can be confident that their rights are protected when law enforcement agencies employ intrusive methods."

A/Commr. Flynn said that the RCMP has already made a considerable effort in terms of visibility and transparency. He noted that

> public articles that had been published by people such as Sergeant Dave Cobey … are meant to bring more public visibility into what we are doing. We are pulling back the veil. We are trying to do that in a way that's professional, that respects both the law around the protection of tools and techniques.[9]

As for Minister Mendicino, he believes that "there are already a number of mechanisms to ensure transparency," particularly the requirement to obtain the approval of a superior court judge, but he said, "we should always be open to having a conversation on how we can raise the bar." He added that one must always be prepared to do more in terms of transparency. In his view, the annual report on electronic surveillance is one of

9 Royal Canadian Mounted Police, *Q&A with an expert in electronic surveillance on the challenges and opportunities of collecting evidence*, 27 July 2022.

the tools that can be used to shed light on how these investigative techniques are used to protect Canadians.[10]

As explained in the annual report on electronic surveillance, Part VI of the *Criminal Code* sets out the provisions that allow law enforcement to obtain judicial authorization to conduct electronic surveillance of communications for criminal investigations. Section 195 of the *Criminal Code* requires Public Safety Canada to prepare and present to Parliament an annual report on the use of electronic surveillance under Part VI, for offences that may be prosecuted by, or on behalf of the Attorney General of Canada. The report provides various statistics, including the number of applications made for audio and video authorizations and renewal each year, and the period for which authorizations or renewals were granted in number of days or hours.[11]

However, Ms. McPhail was of the view that the annual report is insufficient because it simply gives statistics for any audio or visual surveillance. She added that only one warrant application, out of the 331 in the last annual report, was refused. In her opinion, a public interest *amicus curiae* (also known as "friend of the court") should be present at hearings relating to those applications for authorization to provide a counterpoint to police positions.[12]

Other witnesses acknowledged the need for more transparency on the part of the RCMP and the Government of Canada regarding the use of new technologies.[13]

Mr. Dufresne reiterated that the "onus is on the organizations to advise the Privacy Commissioner of the use of those tools." According to the Treasury Board's directive and policies, it is the government organizations' responsibility to be proactive, for example with respect to conducting a privacy impact assessment (PIA), not the OPC.[14] He said that the OPC must be informed far enough in advance of a PIA so that it can provide meaningful input. When a PIA is conducted after the tools have been used for some time, it is difficult to address or prevent problems, because the OPC is in a reactive mode.

---

10 Public Safety Canada, *2020 Annual Report on the Use of Electronic Surveillance*.

11 Ibid. The 2020 Annual Report covers 2016 to 2020.

12 See, for example: Department of Justice, *Legal Representation of Children in Canada*.

13 ETHI, *Evidence*, Ronald J. Deibert; ETHI, *Evidence*, Brenda McPhail; ETHI, *Evidence*, Michel Juneau-Katsuya; ETHI, *Evidence*, Daniel Therrien; ETHI, *Evidence*, Sharon Polsky.

14 The Treasury Board's directive states that PIAs are conducted on "new or substantially modified programs and activities involving the creation, collection and handling of personal information." Treasury Board, *Directive on Privacy Impact Assessment*, section 5.1.

According to Mr. Therrien, the RCMP was not proactive in improving their processes around privacy during his term as privacy commissioner. He gave the example of the use of facial recognition, which led to the creation of the National Technology Onboarding Program (NTOP). The creation of the program was not proactive, but rather at the request of the OPC.[15] He added that

> [i]f the law was clearer that transparency is the rule and only when necessary to protect police methods is it acceptable to not be transparent, there might be progress.

Minister Mendicino said that the purpose of the NTOP is to bring greater transparency, in addition to centralizing and standardizing, to the processes that govern how the RCMP identifies, evaluates, tracks, and approves the use of new technology and investigative tools. In his opinion, this centralized process will ensure greater compliance with professional and legal standards on the use of new technology.

Dr. Deibert said "[w]e definitely have a problem of trust with public institutions, and we're not alone in that respect." He called for public consultations on the use of spyware and for information on the type of software being used, for example the name of vendor, to be disclosed. In his view:

> [P]rocurement should be transparent and include rules for vendors so that we do not purchase from—and help enrich—firms that sell to governments abroad that threaten Canada's values and security.

Mr. Therrien noted that disclosing vendors' names would support greater transparency, as long as the information does not make the methods ineffective. In his view, ensuring transparency in the procurement process is a good idea.

Mr. Dufresne acknowledged that there "may well be information that cannot and should not be made public" with respect to criminal investigative techniques but that consulting with his office confidentially with respect to a PIA would not go against this principle.

Some witnesses were skeptical that the RCMP would release this information without a legal obligation to do so. Ms. McPhail said that the RCMP seems prepared to go to great lengths to protect the use of its tools. She gave the example of the Project Clemenza case, which revealed that the RCMP chose to drop a number of prosecutions rather than reveal the fact that a key to access encrypted communications had been obtained by law

15 Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the way forward*, Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology, 10 June 2021.

enforcement. Dr. Deibert also indicated that law enforcement agencies tend to be reluctant to disclose certain investigative techniques.

In fact, with respect to the use of the ODITs described in the document tabled in the House of Commons in June 2022, RCMP Commissioner Brenda Lucki declined to share with the Committee the specific names of the tools used by the RCMP, as "[s]haring details publicly exposes sensitive information that could negatively impact the RCMP and our public safety partners' ability to effectively use ODITs."[16]

Mr. Juneau-Katsuya supported the idea that making public all the information about the on-device investigative tools used by the RCMP could be harmful. He said:

> We shall not forget that the hearings of this committee are public. Some of the bad guys, being criminals or foreign agents, are listening and taking notes. Asking questions while pushing to get, for example, the country of origin of a technology that must remain secret is to serve on a silver platter to the bad guys the means to counter tactical capabilities.

While the RCMP refuses to make public the technology it uses for fear of revealing secrets about its investigation tools and methods to the criminal underworld, Dr. Deibert believes it is important to avoid "taxpayer money going to some of these rogue, mercenary companies that are contributing to human rights violations abroad and national security problems here in Canada." Ms. McPhail agreed. She proposed creating an entity list of banned spyware vendors.

Dr. Deibert and Ms. McPhail also raised the need for appropriate safeguards to match the sophistication and power of the spyware in use.

Lastly, D/Commr. Larkin noted that the RCMP recognizes that there are gaps in the current legislative framework and that it is very open to working to strengthen protections, mitigate risks, and improve transparency in the use of new technology.

National Security and the Use of Spyware by Foreign Entities

According to Dr. Deibert, "the mercenary spyware industry is not only a threat to civil society and human rights; it is also a threat to national security."

Dr. Deibert added that very little is known about the weapons technology or private intelligence industry. Because these companies generally don't like to publicly disclose

16 Royal Canadian Mounted Police, *Letter to Committee*, 4 August 2022.

what they're doing or who their clients are, Dr. Deibert said that this makes public accountability and transparency very difficult. In its research, the Citizen Lab found

> there's almost no international regulation around this industry; they're selling to any government client. Most of the governments, unfortunately, in the world are authoritarian or illiberal, and naturally, they're using this technology not in the ways we're hoping for it to be used here. They're using it to go after political opposition, civil society, journalists, activists and others. They're making millions of dollars doing so, and they obfuscate their corporate infrastructure from investigators like [the Citizen Lab].

According to Dr. Deibert,

> [t]he fact of the matter is that you have devices that are highly invasive and tend to be poorly secured overall, given the nature of the digital ecosystem that we live in, next to an industry that, as I've described, spends millions of dollars to identify software flaws without disclosing them to the vendors in order to provide this hacking as a service. We've also documented numerous cases of government officials and even heads of state having their devices hacked with the most advanced spyware. As I mentioned in my opening remarks, we observed a hack device at 10 Downing Street, the residence of the Prime Minister, and reported that to the U.K. authorities.

Dr. Deibert stated that Canadians are not immune to foreign interference with spyware, which he calls "digital transnational repression." For example, in 2018, the Citizen Lab observed that Saudi Arabia was undertaking espionage in Quebec.[17] According to Mr. Deibert, "Canadians are definitely not immune to this worldwide risk that is growing in leaps and bounds."

Dr. Deibert said that the Citizen Lab has found through its research that governments, both authoritarian and democratic, have used this type of spyware to hack into the phones of hundreds of individuals worldwide who are neither criminals nor terrorists.

Mr. Therrien said that, while he had never had any evidence of foreign interference in Canadians' privacy during his tenure as privacy commissioner, he had his doubts about some foreign powers and businesses.

According to A/Commr. Flynn, Canada is protected from foreign interference by international agreements with certain partners, particularly the Five Eyes.[18] However, it

---

17 Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert, "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," Citizen Lab Research Report No. 115, University of Toronto, October 2018.

18 The Five Eyes is an intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom and the United States. Public Safety Canada, *Five Country Ministerial*.

is a concern that foreign states that are not partners use these types of tools and techniques against Canadians.

Mr. Juneau-Katsuya said that in the past, it has been necessary for law enforcement to surveil elected officials at every level, whether municipal, provincial, or federal, who were in the pockets of foreign governments. They are known as "agents of influence." They may exercise influence consciously or unconsciously, but in all cases the result is the same from a national security standpoint and puts Canada at risk. He added that foreign agencies have always tried to recruit elected officials and that it is not that hard to do because politicians do not always listen to what CSIS tells them or they simply disregard the information because doing so is to their personal benefit. He added

> [v]ery often the politicians or elected officials, as I like to say, were not necessarily the initial target, but they actually came to our attention when we were watching foreign intelligence officers or foreign criminals or Canadian criminals being in contact with them. It became a concern to either CSIS or the RCMP when these people demonstrated certain activities or certain actions that were questionable in light of the responsibility of their office.

Mr. Juneau-Katsuya also expressed concern that some ministers, after leaving public office, go to work for foreign companies that work directly against the national security and the national interests of Canada. He confirmed that he knows that various foreign countries have succeeded in recruiting elected officials, municipal, provincial, or federal, and were capable of influence in that way.[19]

19 Following an in-camera appearance to provide the Committee with further information on foreign interference, Mr. Juneau-Katsuya provided the Committee with information relating to Australia's initiatives to deter and counter foreign interference: Australia Government, Department of Home Affairs, National Security, *Countering foreign interference*; Australia Government, Department of Home Affairs, National Security, Countering foreign interference, *Resources and related links*.

CHAPTER 2: USE OF ON-DEVICE INVESTIGATIVE TOOLS BY THE ROYAL CANADIAN MOUNTED POLICE

> **"Given all of the devices and the fact that users have complete choice over what device they buy, what apps they use and how they use those apps, ODITs are essential because they help us manage all that complexity."**
>
> Dave Cobey,
> Sergeant, Technical Case Management Program, Technical Investigation Services,
> Royal Canadian Mounted Police,
> who appeared before the Committee on 8 August 2022.

Description of On-Device Investigative Tools Used by the Royal Canadian Mounted Police

The RCMP describes an ODIT as software that is deployed on devices or computer networks via remote, near or close access, to allow electronic monitoring.[20] ODITs allow for the interception of information on a device without the knowledge of the device owner. An ODIT can be programmed to perform more than one function.[21]

Traditionally, the RCMP has intercepted data and communications between two computing devices. However, encryption tools that have become widely available through popular applications such as iMessage, WhatsApp, Telegram, Signal, Kik and Skype, are preventing the RCMP from using traditional investigative techniques to gain access to certain data.[22] Encrypted data can still be intercepted by the RCMP, but the encryption renders it unintelligible. "ODITs may be used to obtain this data in a readable format."[23]

---

20 A computing device means a cellular phone, computer, server, tablet, or other electronic device such as wireless cameras and smart locks, which may be used to send or receive data, including private communications, on a network such as the Internet. Royal Canadian Mounted Police, *Draft Policy OM-Ch.*, 8 August 2022, para. 1.1; The RCMP provided the Committee with the "RCMP's Covert Access and Intercept Team (CAIT) draft policy on the management of ODITs and other sensitive assets." Royal Canadian Mounted Police, *Letter to Committee*, 4 August 2022.

21 Royal Canadian Mounted Police, *OM Draft Policy – Ch.*, 8 August 2022, para. 1.4.

22 Royal Canadian Mounted Police, *On-Device Investigative Tool (ODIT) Technical Description Draft for Project*, 8 August 2022, para. 12.

23 Ibid., para. 13.

Specifically, ODITs can be deployed or installed on devices without the knowledge of the owners of the devices and used to:

1) collect/intercept data from within the target device while the data is in an unencrypted form;

2) collect/intercept data after it has been received by the device and decrypted;

3) collect/intercept data before it is encrypted and sent;

4) covertly copy data stored on a device or available to that device through cloud storage[24] or another networked device;

5) capture data that identifies the user of the device; and

6) activate peripheral components of the targeted device, i.e., the camera and microphone, to conduct electronic surveillance.[25]

Under the RCMP's policy, the TIS CAIT, provides covert electronic services to the RCMP and its law enforcement partners. This specialized team deploys ODITs that enable the interception of private communications and transmission data, the collection of tracking information and data at rest from computing devices. Only CAIT operators are authorized to use ODITs in the RCMP.[26] Sgt. Cobey said that service providers such as Rogers, Telus or Bell are not involved in the use of ODITs.

CAIT operators are located in certain divisions and at CAIT headquarters, and may only use ODITs if certified to do so, in consultation with CAIT headquarters, and with all required approvals.[27]

24 Cloud storage includes transmission data that can facilitate the use of ODITs such as passwords, login credentials, encryption keys, and the configuration of systems and programs. Royal Canadian Mounted Police*, On-Device Investigative Tool (ODIT) Technical Description Draft for Project*, 8 August 2022, para. 17.

25 Ibid., paras. 13 and 14.

26 Royal Canadian Mounted Police, *OM Draft Policy – Ch.*, 8 August 2022, para. 1.2.

27 Ibid., paras. 1.3 and 2.

High Legal Threshold

Minister Mendicino and RCMP officials said that the legal threshold for the RCMP to use ODITs is very high.[28]

Minister Mendicino said that the RCMP uses only approved investigative technology for serious offences under the *Criminal Code*, and under judicial authorization. Many protections are built into the *Criminal Code* and the law generally, which he said are there to "achieve the balance between allowing the state to protect individuals while at the same time protecting the individual privacy of all Canadians."

D/Commr. Larkin said that "ODITs are used extremely rarely and in limited cases. Their use is always targeted. It's always time-limited, and it's never to conduct unwarranted and/or mass surveillance." Sgt. Cobey told the Committee that, since 2017, the RCMP has used ODITs in only 32 investigations. D/Commr. Larkin clarified that those 32 investigations targeted 49 devices.

Mr. Juneau-Katsuya indicated that caution is needed when making allegations of mass surveillance for two reasons. First, according to him "there [is] no evidence that there is mass surveillance" in Canada. Second the high cost of such an operation: "Just one operation will easily reach half a million dollars. That's just to make one interception on one target with maybe one device only." He added that the RCMP, CSIS and the Department of National Defence do not have an operational capability comparable to that of the U.S. National Security Agency, as leaked by Edward Snowden.

Mr. Juneau-Katsuya further stated that the number of targeted uses of ODIT spread over five years is not mass surveillance.

Mr. Therrien also said he does not think the RCMP conducts mass surveillance because it only uses ODITs with judicial authorization.

Sgt. Cobey added that, of the investigations in which investigators have requested the use of ODITs, approximately one in ten have resulted in ODITs being deployed. He also specified the instances in which the use of ODITs was authorized in the past.

> The most investigations are related to terrorism or serious drug trafficking investigations. There were also five murder investigations and there were also some breach of trust investigations, one of those being the investigation of a police officer's

28 ETHI, *Evidence*, Marco Mendicino; ETHI, *Evidence*, Dave Cobey; ETHI, *Evidence*, Bryan Larkin.

> activities. But for the total, all combined, there were 32, and all 32 investigations had at least one offence that was under section 183 … Those are all serious offences.[29]

The 32 investigations in which the RCMP used ODITs related to the following offences: drug importation or trafficking, money laundering, trafficking in the proceeds of crime, fraud, organized crime offences, participation or contribution to terrorist activity, murder, breach of trust by a public officer, cybercrime (malware) and extortion (ransomware), kidnapping and criminal harassment.[30]

Judicial Authorization and Internal Process

Several witnesses raised the importance of requiring the RCMP to obtain judicial authorization before using an ODIT.[31]

Minister Mendicino explained that it is up to a superior court judge who "has to take a look at the facts in very meticulous detail, which will offer some evidence or information of a very specific offence that is being breached." Authority to use ODITs is limited to a very specific list of serious offences under Part VI of the *Criminal Code*, specifically section 183. According to the Minister,

> the judge has to engage in a balancing exercise to determine, among other things, whether the interception, the technique, is necessary and whether it's pressing and urgent enough that it requires the technique to be afforded to the state for the purposes of acquiring information that could then be potentially used as evidence in a subsequent criminal proceeding.

Sgt. Cobey said that the use of ODITs requires several warrants, often all included in an omnibus order. For example, requirements include an interception of private communication warrant to cover Part VI of the *Criminal Code*; a general warrant for the deployment and use of the ODIT and the technology in the background; a transmission data recorder warrant to collect the transmission data to operate them; and a tracking

---

29 Pursuant to section 183 of the *Criminal Code*, offence means "an offence contrary to, any conspiracy or attempt to commit or being an accessory after the fact in relation to an offence contrary to, or any counselling in relation to an offence contrary to" one the specific provisions of the *Criminal Code* enumerated in that section.

30 Royal Canadian Mounted Police, RCMP Response, *Document submitted to Committee*, 15 September 2022. The document was prepared by the RCMP in response to a motion by the Committee requesting "a list of warrants obtained, if any, for each use of such software, as well as the scope of the warrants and the reasons for the monitoring."

31 ETHI, *Evidence*, Marco Mendicino; ETHI, *Evidence*, Bryan Larkin; ETHI, *Evidence*, Mark Flynn; ETHI, *Evidence*, Dave Cobey; ETHI, *Evidence*, Michel Juneau-Katsuya.

warrant if the ODIT is being used to collect information related to the location of the device. A sealing order and an assistance order must also be sought at the same time.

Sgt. Cobey explained that each order also contains terms and conditions on how to deal with non-pertinent information related to third parties and others, as well as privileged communications, such as between a solicitor and their client, and other private information. Sgt. Cobey added that for solicitor-client communications, the terms and conditions are clear. These communications must be sealed and cannot be looked at without a further order of the court. He said that, once judicial authorization is granted "monitors and analysts assigned to do the first review would be responsible to make sure that the condition [of the warrant] is followed."

Sgt. Cobey also described in details the RCMP's internal process for using ODITs:

> Initially we have a consultation with investigators who are considering these tools. During that consultation we explain to them—we demystify these tools and explain—just how complicated they are and the fact that they aren't necessarily going to be able to deliver the evidence they want, and we really encourage them to consider other, less invasive tools if possible.
>
> Step one, we make sure they really understand what they're getting themselves into and have the resources to do it. Following that consultation, they have to submit an official request from their chain of command to our technical investigative services so there is executive awareness and oversight of their request to make sure it's been properly monitored.
>
> After that request, and if it's approved on our side, then we have a second consultation involving their Crown prosecutor. Or, if they don't have a Crown prosecutor, we insist that a Crown be assigned so that a Crown understands the risks and the potential rewards of using these tools.
>
> One thing we make clear during that consultation is that these are new technologies and we fully expect they will be litigated. We make sure they understand the litigation risk and the types of sensitive information that we're not able to share and would seek to protect under section 37 or section 38 of the *Canada Evidence Act*.
>
> That whole process to date is really intended to make sure they understand that if there's another tool that works, they should use it, because these tools are complicated …
>
> After all of those consultations, we do an engagement memo between our unit and the requesting unit to memorialize all the conversations, to set out the need to protect the tools. Only after that engagement memo is acknowledged by the commissioned officer overseeing that investigation would the assistance be provided. Of course, all that doesn't matter a whit unless judicial authorization has been granted through the

> process that we've described earlier in terms of a Crown agent, a proper authorization with all the terms and conditions we've included.

A/Commr. Flynn added that additional safeguards in the policies and procedures are in place for using ODITs in certain sectors. These include parliamentarians, journalists, religious institutions, and educational institutions. A higher level of approval is therefore required when a request is made for the electronic surveillance of an individual in those sectors.

In Mr. Juneau-Katsuya's experience, it is not always the same judge that makes decisions to grant warrants, but certain judges are specifically selected because of the secrecy level and national security of the information they will need to consult. However, Dr. Deibert said he has concerns, with all due respect to judges he has confidence in, whether they truly understand the scope, scale, sophistication and power of the type of invasive technology under consideration by the Committee.

Mr. Therrien said he assumes that judges who receive requests for judicial authorization have the technical and legal expertise to make the best decisions. He explained that judges are "bound by the terms of part VI of the *Criminal Code*" when looking at warrant applications, but that the

> Office of the Privacy Commissioner looks at privacy more broadly under its statute, and it can therefore provide additional assurance to the public that privacy writ larger than the *Criminal Code* will be respected when these tools are used.

Mr. Therrien does not think that the RCMP is a "rogue institution." He acknowledges that the RCMP uses ODITs only with judicial authorization but believes that it might be a good idea to have auditing processes to ensure that the police officer who has to perform the task in question does so in compliance with the court's requirements. As indicated above, the RCMP has an internal process to ensure that requests for ODITs are monitored and conditions of the warrant obtained are respected.

For his part, A/Commr. Flynn believes that judges "absolutely do understand privacy." D/Commr. Larkin added that judges "receive and continue to receive supporting material explaining what the ODIT is and its capabilities."

Privacy Impact Assessment

D/Commr. Larkin confirmed that the RCMP had not completed a PIA with respect to its use of ODITs at the time of the RCMP officials' appearance before the Committee.

Mr. Therrien said that a PIA should haven been conducted given the extremely intrusive nature of ODITs. Many other witnesses were of the same view.[32]

With respect to conducting PIAs, A/Commr. Flynn explained that privacy, whether in the context of intercepting an analog communication or an encrypted communication, is mainly in the content of the information, not the method of obtaining the information. Consequently, the trigger for conducting a PIA is not always clear. Over time the RCMP sometimes changes its position on these issues.

A/Commr. Flynn explained that the RCMP believes the actual privacy invasion to be listening to a conversation or physically observing an individual. This type of privacy invasion has been happening for years using various methods, so this is not a new type of privacy invasion. An ODIT is just a new method, not a new privacy invasion.

A/Commr. Flynn repeated that the privacy invasion does not come from the tool used to intercept communications, but from "capturing that audio or capturing that text message or capturing that communication that is occurring between two individuals, and [the RCMP has] evolved in the use of the tools as individuals evolve in the way they communicate."

Sgt. Cobey also noted that protecting innocent third parties' privacy and non-pertinent communications has been an issue ever since wiretapping began and is not unique to ODITs.

Ms. McPhail criticized the fact that the RCMP does not think about doing a PIA just because it is using a new technology, but only whether the technology permits a new kind of invasion. She said that this way of thinking ignores the reality of an ODIT, "which allows all the invasions all at once on a device" such as recording live audio, tracking locations, collecting device identifiers, tracking Internet searches, and tracking application use. She explained:

> Did they do wiretaps before? Of course. Did those wiretaps allow access to the contents of every form of communication written and oral, professional and private, retrospectively and prospectively, including data that's not actually on the device itself but in the cloud? Of course not. Is it the same level of invasion? No. Did police install covert cameras in homes and places of business with warrants in the past? Of course. Did a single camera have the ability to move with an investigative subject from work to

32 ETHI, *Evidence*, Philippe Dufresne; ETHI, *Evidence*, Brenda McPhail; ETHI, *Evidence*, Ronald J. Deibert; ETHI, *Evidence*, Sharon Polsky; and ETHI, *Evidence*, Michel Juneau-Katsuya.

> home, from bedroom to bathroom, 24 hours a day? Of course not. Is it the same level of invasion? No.

However, the functions of ODITs used by the RCMP can vary. Some ODITs allow full interactive remote control of the targeted devices. Other types of ODITs call back to a CAIT server and await for commands that are queued for execution. For example, an ODIT may be set to contact the CAIT server every five hours. If there are commands, it will execute them. If not, it will do nothing. With respect the ability to activate the microphone on a targeted device, the control of that function will also differ depending on the ODIT, operating system, device, and telecommunication service.[33]

Mr. Therrien also emphasized the fact that "this particular tool is extremely intrusive. It's more intrusive than traditional wiretap tools." He noted that when such a tool is installed on the digital device of an individual, "the state—the police—has access to everything on that phone. It is extremely intrusive."

Other witnesses agreed that this surveillance technology is far more intrusive than wiretaps or other previously used technologies. Given the nature of these tools, Ms. McPhail said that "[e]ven [a PIA] … is not enough when we're talking about the enormity of the invasion."

CHAPTER 3: MODERNIZATION OF THE LEGISLATIVE FRAMEWORK AND OTHER MEASURES

> **"Privacy and the public interest go hand in hand, they build on and strengthen each other and Canadians and their institutions should not have to choose between one or the other."**
>
> Philippe Dufresne,
> Privacy Commissioner of Canada,
> who appeared before the Committee on 8 August 2022.

Several witnesses noted the importance of making various changes to the legislative framework that applies to the use of spyware and on-device device investigative tools.

33 Royal Canadian Mounted Police, *On-Device Investigative Tool (ODIT) Technical Description Draft for Project*, 8 August 2022, paras. 18(e) and 25.

For example, Minister Mendicino said he was open to suggestions for strengthening transparency mechanisms to build trust with Canadians. Mr. Therrien said that the "fundamental conditions for confidence are clear legal rules, high legal standards and independent oversight."

Modernization and Enhancement of Part VI of the *Criminal Code*

Mr. Dufresne said that Part VI of the *Criminal Code* includes certain conditions that are intended to protect privacy while allowing for criminal investigations. He said that this part of the *Criminal Code* sets out the conditions in which police can use the tools, the obligation to obtain authorization from a judge, the obligation to give notification, and various other conditions.

However, Mr. Dufresne noted that, while Part VI of the *Criminal Code* contains a number of safeguards, it does not "relieve police of the necessity to assess the potential privacy repercussions when they plan to use new tools." He noted that the regime may need to be strengthened to include additional criteria or safeguards.

Mr. Dufresne explained the difference between judicial authorization and a PIA:

> The judicially approved warrant will look at the specific request on the basis of the criteria in the *Criminal Code* and will follow that process. The PIA will look at it from a program perspective. It will look at it broadly in terms of what types of available tools are being used, what are the mechanisms to authorize the use of those tools, and whether the mechanisms are sufficient. For instance, should there be different or additional requirements before they can be judicially authorized, or should there be, in addition to the judicial authorization, mechanisms for the safeguarding of information? Perhaps that's not necessary, but the PIA serves that purpose—to look at it, not with respect to a specific case but with respect to the program as a whole.

Mr. Therrien also noted that Part VI of the *Criminal Code* provides a legal framework comprising strict standards and independent oversight by the courts. However, he was of the view that it is possible to improve the legal framework proactively, particularly with regard to PIAs.[34] He explained that Part VI of the *Criminal Code* sets the standards for privacy that courts must apply when granting a warrant. However, the *Privacy Act* has a much broader definition of privacy. Consequently, while the courts may play their role adequately under the *Criminal Code*, this does not mean that a PIA does not also have a role to play in ensuring better privacy protection for Canadians.

34 ETHI, *Evidence*, Daniel Therrien.

Ms. McPhail, Dr. Deibert and Mr. Juneau-Katsuya all said that Part VI of the *Criminal Code* has not kept pace with advances in technology in the criminal world and that the government needs to update it.

For example, Ms. McPhail said it was "worth looking at part VI of the *Criminal Code*, which … had its last very significant amendments slightly more than 20 years ago." She added that it would be useful for experts in the use of this part of the *Criminal Code* to be invited to comment on the ways Part VI should be enhanced to take into account that the technology has changed so fundamentally.

Modernizing the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*

Several witnesses said that Canada's privacy laws should be improved. For example, Ms. McPhail said that there are gaps in the laws protecting privacy in both the private and public sectors.

Mr. Therrien said that in 2022, information is shared between the private and public sectors extensively, so it is important that public sector and private sector laws are compatible and interoperable. He believes that, "[i]deally, they should be adopted in one statute, because data does not know frontiers between the public sector and the private sector." Mr. Therrien acknowledged that the "contexts are somewhat different" but that "the statutes should be based on similar, if not identical, principles" in the public and private sectors.

However, Mr. Therrien doesn't believe that such reform is feasible within a reasonable time, noting that it took 40 years to revise the *Privacy Act* and 20 years for amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[35] He is concerned that the "risk involved in combining it all in a single act in Canada today is that it might delay passage of the act respecting the private sector [Bill C-27], which is currently before Parliament."[36]

Mr. Therrien added that

35 ETHI, *Evidence*, Daniel Therrien.

36 Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, 44th Parliament, 1st Session. The bill was introduced in the House of Commons on 16 June 2022.

> [w]e should ensure that the Office of the Privacy Commissioner, for both the public and the private sectors, has the authority to not just make recommendations, but make orders for the private sector and the public sector when it sees violations of the law. There should also be financial sanctions, certainly in the private sector, to ensure that these laws are respected.

Mr. Dufresne, Mr. Therrien and Ms. McPhail recommended that federal privacy laws recognize privacy as a fundamental right.

Mr. Therrien suggested that including clear legal standards, such as a fundamental right to privacy, in the preamble to the *Privacy Act*, would better define Canada's approach to privacy protection. He added that, while the preamble to a statute is not binding in itself, it is a helpful interpretative tool. He explained, for example, with respect to the *Privacy Act*:

> For a preamble to say that privacy is a fundamental right essential for the preservation of the dignity of individuals, when the RCMP, the health department or whatever institution proceeds with a PIA, they have that important message in mind.

Mr. Dufresne also supported the idea of inserting a preamble in the *Privacy Act* that would highlight the fundamental importance of privacy to the dignity and rights of Canadians. In his view, there should be a culture of privacy in federal institutions.

Mr. Therrien suggested that privacy by design should be standard practice in the adoption of all new technologies and for all institutions. Mr. Therrien described privacy by design as a process that incorporates privacy considerations before a particularly intrusive technology is used. The benefit of privacy by design is to assure the public that it is not after the fact that violations are found and that violations will be reduced greatly in number because of the processes put in place.

Mr. Dufresne also mentioned that "it should be privacy by design." This would ensure that where new tools are considered, priority is given to considering the impacts they may have on privacy.

Mr. Dufresne noted that, although the Treasury Board directive[37] requires PIAs in its policies, "the Privacy Act does not require the RCMP or any government institution to prepare privacy impact assessments." He said he hopes that this requirement will be included as a legal obligation in a modernized version of the *Privacy Act*.

37 Treasury Board, *Directive on Privacy Impact Assessment*.

Mr. Dufresne said that considering privacy impacts at the front end, for example by consulting with the OPC, would help prevent privacy harms and improve tools that further public interest, whether it be preventing crime, protecting national security, or advancing Canada's competitiveness.

For example, in the case of the use of ODITs by the RCMP, Mr. Dufresne explained:

> Once we receive the PIA, we will review it to ensure that it includes a meaningful assessment of the program's privacy compliance and measures to mitigate privacy risks. We will also review it to ensure that any privacy-invasive programs or activities are legally authorized and necessary to meet a specific need, and that the intrusion on privacy caused by the program or activity is proportionate to the public interest at stake. This would require the RCMP to consider whether there is a less privacy-intrusive way of achieving the same objective. If we find shortcomings in terms of privacy protections, we will provide the RCMP with our recommendations. We would expect them to make the necessary changes.

Mr. Dufresne indicated that PIAs are an important tool for a culture of privacy because they create the habit of asking questions, such as whether the use of a certain tool is necessary or whether so much information is needed to achieve a goal.

Other witnesses also felt that it was important to incorporate the requirement for a PIA into the legislation.[38]

Mr. Therrien suggested that not only should there be a legal obligation to consult with the OPC, but the law should also specify the circumstances in which PIAs must be conducted. He noted, for example, that with respect to the use of ODITs the RCMP said its use of this technology is nothing new. There is a responsibility to state, in general terms,

> when they must be conducted and for what purpose. That way you can ensure proactively that the act is being complied with. There wouldn't simply be an ex *post facto* review but also a preliminary examination to ensure statutory compliance.

Mr. Juneau-Katsuya and Dr. Deibert also noted the importance of involving the OPC in the process leading to the use of new technology by law enforcement. For example, Dr. Deibert said that he was "very disappointed to hear that the [OPC] was not informed about these investigative techniques prior to the recent revelations." He recommended

38 ETHI, *Evidence*, Brenda McPhail; ETHI, *Evidence*, Ronald J. Deibert; ETHI, *Evidence*, Sharon Polsky.

that privacy commissioners be equipped with greater capabilities and resources to act as watchdog over Canadian security agencies.[39]

Mr. Dufresne also noted the importance of properly weighing the risks and the necessity of using a certain tool, and recommended adopting necessity and proportionality as criteria to justify such use.

Finally, several witnesses raised the importance of incorporating a transparency obligation into the legislation. Dr. Deibert felt that law enforcement should disclose information about the technology they are procuring. Mr. Therrien suggested the adoption of the following transparency standard: "that the government and the police … have an obligation of transparency, subject only to what is necessary to protect police methods and the integrity of investigations."

Moratorium or Ban

Some witnesses commented on a possible moratorium on the use of spyware in Canada.

Ms. McPhail stated that a moratorium is needed. Ms. Polsky was not opposed to a moratorium but noted that it is only a temporary measure. She said that with spyware "the risk [is] greater than the reward." She argued that using spyware needs to be made unlawful except in specific exceptional situations under the law. She said a ban on police use alone of the tool does not go far enough.

Ms. McPhail noted that briefly pausing the use of a so-called "last-resort" tool would not pose much of a risk to public safety when weighed against privacy rights, law enforcement and social and diplomatic impacts. She added that, if a moratorium is not imposed, serious legislative changes are needed. She also believes that Canada should follow the lead of the United States and Europe in banning the state purchase of spyware.

Ms. McPhail also said that Canada should consider creating a list of banned spyware vendors similar to that of the United States. Such a list would provide the public with some assurance that their tax dollars are not supporting these dangerous and mercenary companies. On that point, Minister Mendicino said he was prepared to ban Pegasus software in Canada.

39 As indicated above, the Office of the Privacy Commissioner has a Technology Analysis Directorate since 2011.

Other witnesses did not support a complete ban on spyware. For example, Mr. Therrien said that there should be laws regulating the sale, import and export of these technologies, but not an outright ban.

However, Mr. Therrien said that while "he could see compelling grounds for the government, the state and the police to use this type of technology exceptionally with judicial authorization" , he could not "really see any compelling reason that someone in the private sector should be able to use this technology." Ms. Polsky and Mr. Juneau-Katsuya agreed.

Ms. Polsky said that it is not just a matter of banning police use of these tools, which may be legitimate. The problem is that these tools are commercially available. Mr. Juneau-Katsuya said:

> If I may add one element, we're spending a lot of time talking about law enforcement, which is the leitmotif of this discussion, but one area that has been neglected is the private world. Private companies are using this kind of technology far more than law enforcement, which is much more surveilled.

Mr. Dufresne would not comment on imposing a moratorium because of the lack of information on the software used by the RCMP. He rather reminded the Committee the importance of determining "what the repercussions and implications of using the tools are, and to make recommendations based on the information provided by the RCMP." The RCMP was scheduled to meet with the OPC at the end of August 2022 for a demonstration on the use of ODITs. No further information was provided to the Committee regarding that demonstration following Mr. Dufresne's appearance.

Lastly, A/Commr. Flynn said that the laws of Canada have protected the right to privacy, regardless of the level of sophistication required by the RCMP to perform their duty. He believes that these protections are valid today, as they were back in the 1960s. He therefore opposes a moratorium on the use of spyware.

Other Measures

Some witnesses recommended non-legislative measures to better control the sale and use of spyware and increase privacy awareness.

For example, Ms. Polsky suggested that a pan-Canadian education strategy be developed to help students, whether at school or university, understand the basics of online privacy, how it can be undermined and how to protect themselves.

Dr. Deibert emphasized the need to inform Canadians and hold public hearings on the threats of the mercenary spyware industry.

Dr. Deibert also suggested that Canada develop strong export controls for the Canadian surveillance industry, as currently there are none. He believes that Canada should also impose penalties on spyware firms that are known to facilitate human rights abuses abroad modelled after those in the United States. According to him, Canada should also develop procurement guidelines for Canadian agencies so they never contract with firms linked to human rights abuses abroad.

Mr. Juneau-Katsuya recognized that the House of Commons has established a permanent committee on security and intelligence "capable of going across the board in every department to follow the traces of certain cases." He noted that the challenge with such a committee is that sitting members are elected and each election may change. However, he criticized the Security Intelligence Review Committee, "which went from watchdog to lapdog over time" because it is not doing as much work as is needed to observe, criticize, and bring solutions to some of the problems.

In the same vein, Ms. McPhail said that, to counter the persistent pattern of police acquiring and using sophisticated and potentially controversial surveillance technologies without public disclosure, the Canadian government should follow the lead of New York State and New Zealand in putting together an independent advisory panel composed of relevant stakeholders from the legal community, government, police, national security, civil society and, of course, relevant regulatory bodies like the OPC.

According to Ms. McPhail, this advisory panel can

> act as a national standard setting body, an advisory body, to take a proactive look at the kinds of technologies that our police forces want to use to modernize their investigative techniques and look at them across a range of considerations, including ethical considerations, legal considerations and considerations around Canadian norms and values. It can then make standard setting, gold standard, recommendations for police organizations, not just nationally but provincially and territorially—because of course policing is also a provincial and territorial matter—so that we would have consistency and the public could be assured that rights were being respected while police had the tools they need to do their difficult jobs.

Ms. McPhail stated that because policing is a provincial/territorial responsibility, there is a patchwork of legislation that is relevant. That makes it more difficult to assure that all police forces across the country adhere to the best standards when it comes to uses of surveillance technologies. The federal advisory committee she proposed could remedy that problem by establishing best practices.

Dr. Deibert said that members of the highest levels of the Canadian government, such as senior officials, the Prime Minister, the Minister of Public Safety, and the Minister of Foreign Affairs, should make clear, forceful statements that the surveillance technology industry is a threat to human rights, democracy, and national security. This statement should affirm that Canada plans to take measures aligned with its allies in the United States, Europe and elsewhere to hold the worst actors in the industry more accountable and to be more transparent and publicly accountable if the technology is to be used domestically.

Finally, Dr. Deibert recommended that Canada impose a lifetime ban on individuals who have worked in Canadian national security agencies from ever working with mercenary spyware firms.

COMMITTEE OBSERVATIONS AND RECOMMENDATIONS

First, most members of the Committee would like to note the lack of cooperation shown by the RCMP in this study. The Committee is not satisfied with responses they provided to its questions.

The Committee recognizes that there is a legislative gap regarding the use of new technological investigative tools. It therefore believes that a better legislative framework for the use of on-device investigative tools by the RCMP is needed to ensure the appropriate use of these tools and the protection of Canadians' privacy rights.

In light of the above, the Committee recommends:

Recommendation 1

That the Government of Canada amend the *Privacy Act* to include an explicit obligation for government institutions to conduct privacy impact assessments before using high-risk technological tools to collect personal information and to submit them to the Office of the Privacy Commissioner of Canada for assessment.

Recommendation 2

That the Government of Canada create a list of banned spyware vendors and establish clear rules on export controls over surveillance technologies.

Recommendation 3

That the Government of Canada review Part VI of the *Criminal Code* to ensure that it is fit for the digital age.

Recommendation 4

That the Government of Canada amend the preamble to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to indicate that privacy is a fundamental right.

Recommendation 5

That the Government of Canada regularly remind former elected or appointed members or any individuals who have previously worked for a national security agency of their lifetime obligations under the *Security of Information Act* and obtain acknowledgment of their understanding of these obligations.

Recommendation 6

That the Government of Canada grant the Office of the Privacy Commissioner of Canada the power to make recommendations and issue orders in both the public and private sectors when it finds violations of the laws for which it is responsible.

Recommendation 7

That the Government of Canada amend the *Privacy Act* to include the concept of privacy by design and an obligation for federal institutions subject to the Act to meet this standard when developing and using new technologies.

Recommendation 8

That the Government of Canada establish an independent advisory body composed of relevant stakeholders from the legal community, government, police and national security, civil society, and relevant regulatory bodies, like the Office of the Privacy Commissioner of Canada, to review new technologies used by law enforcement and to establish national standards for their use.

Recommendation 9

That the Government of Canada amend the *Privacy Act* to include explicit transparency requirements for government institutions, except where confidentiality is necessary to

protect the methods used by law enforcement authorities and ensure the integrity of their investigations.

CONCLUSION

Any intrusive technology such as on-device investigative tools must be regulated under Canadian law.

Just as law enforcement agencies have had to adapt their investigative tools to technological advances, so too must our laws.

However, as several witnesses told us, neither Part VI of the *Criminal Code* nor the *Privacy Act* is currently adapted to the digital age. PIPEDA has also not been substantially updated since its adoption in 2000. The Committee's recommendations, if adopted, would allow the government to achieve such necessary update.

The Committee therefore encourages the Government of Canada to implement its recommendations as soon as possible to ensure an essential balance between public protection, privacy protection and public confidence in Canadian institutions.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Office of the Privacy Commissioner of Canada	2022/08/08	30
Philippe Dufresne, Privacy Commissioner of Canada		
Gregory Smolynec, Deputy Commissioner Policy and Promotion Sector		
Department of Public Safety and Emergency Preparedness	2022/08/08	31
Hon. Marco Mendicino, P.C., M.P., Minister of Public Safety		
Royal Canadian Mounted Police	2022/08/08	31
Dave Cobey, Sergeant Technical Case Management Program, Technical Investigation Services		
Mark Flynn, Assistant Commissioner, Federal Policing National Security and Protective Policing		
Bryan Larkin, Deputy Commissioner Specialized Policing Services		
As an individual	2022/08/09	32
Daniel Therrien, Lawyer		
Privacy and Access Council of Canada	2022/08/09	32
Sharon Polsky, President		
As an individual	2022/08/09	33
Ronald J. Deibert, Professor of Political Science, and Director Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto		
Michel Juneau-Katsuya, Expert and Researcher on National Security and Intelligence		

Organizations and Individuals	Date	Meeting
Canadian Civil Liberties Association	2022/08/09	33
Brenda McPhail, Director Privacy, Technology and Surveillance Program		
As an individual	2022/09/28	36
Michel Juneau-Katsuya, Expert and Researcher on National Security and Intelligence		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Privacy and Access Council of Canada

The Citizen Lab

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 30, 31, 32, 33, 36, 43, 44 and 45) is tabled.

Respectfully submitted,

John Brassard
Chair