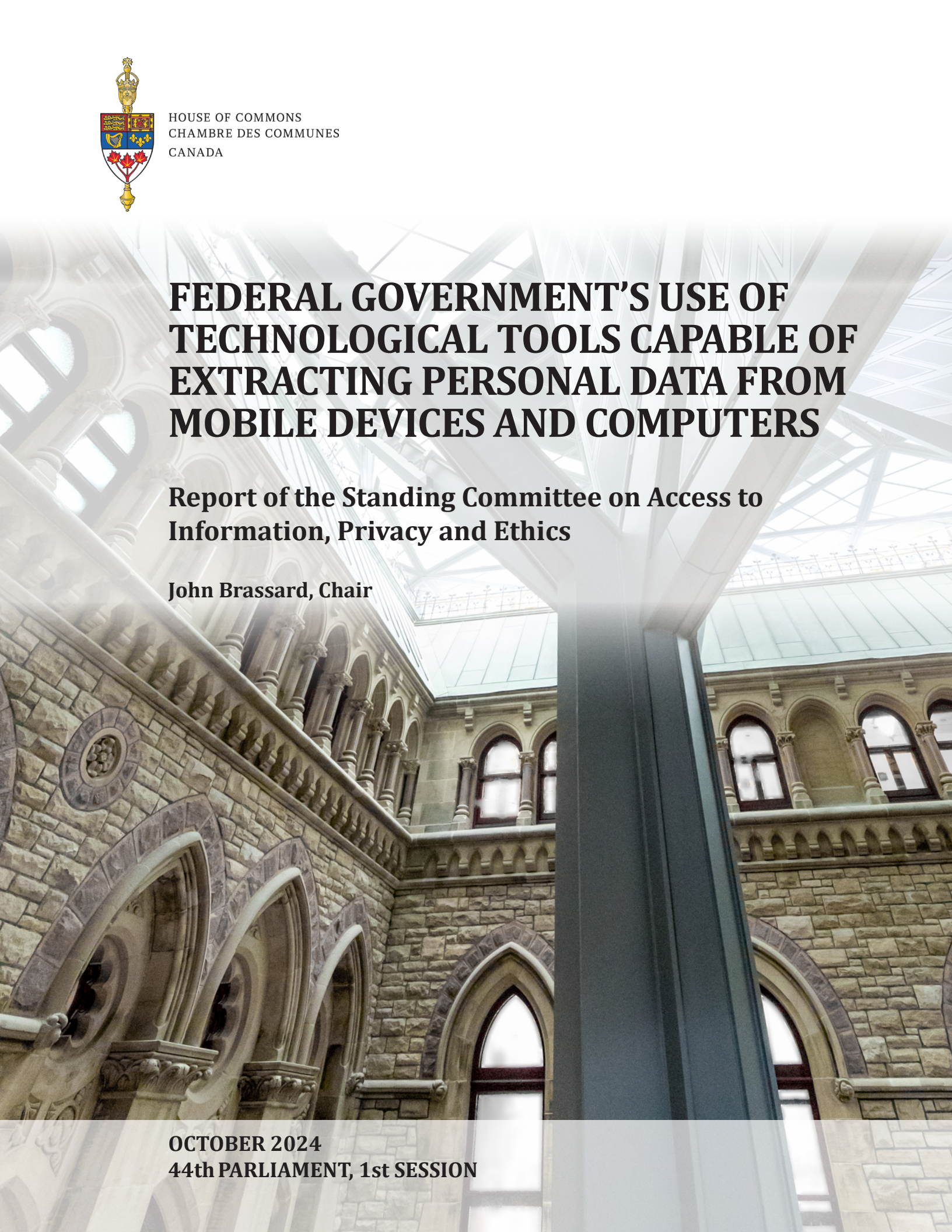

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

FEDERAL GOVERNMENT'S USE OF TECHNOLOGICAL TOOLS CAPABLE OF EXTRACTING PERSONAL DATA FROM MOBILE DEVICES AND COMPUTERS

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

John Brassard, Chair

OCTOBER 2024
44th PARLIAMENT, 1st SESSION

FEDERAL GOVERNMENT'S USE OF TECHNOLOGICAL TOOLS CAPABLE OF EXTRACTING PERSONAL DATA FROM MOBILE DEVICES AND COMPUTERS

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

John Brassard
Chair

OCTOBER 2024

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

Darren Fisher

René Villemure

MEMBERS

Parm Bains

Michael Barrett

Frank Caputo

Michael Cooper

Matthew Green

Anthony Housefather

Iqra Khalid

Brenda Shanahan

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Pam Damoff

Nathaniel Erskine-Smith

Hon. Mona Fortier

Lori Idlout

Mike Kelloway

Damien C. Kurek

Stephanie Kusie

Viviane Lapointe

Eric Melilo

Glen Motz

Hon. Robert Oliphant

Francesco Sorbara

CLERK OF THE COMMITTEE

Nancy Vohl

LIBRARY OF PARLIAMENT

Research and Education

Alexandra Savoie, Analyst

Maxime-Olivier Thibodeau, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

THIRTEENTH REPORT

Pursuant to Standing Order 108(3)(h) the committee has studied the federal government's use of technological tools capable of extracting personal data from mobile devices and computers and has agreed to report the following:

TABLE OF CONTENTS

SUMMARY

In February 2024, the Committee undertook a study on the use, by certain federal government institutions, of technological tools capable of extracting data from mobile devices and computers, known as digital forensic tools.

Given the capacity of these tools, some stakeholders raised concerns about the possibility that they could be misused. In particular, they questioned how these tools might be used in internal administrative investigations involving federal employees.

The Privacy Commissioner of Canada noted that, in an era where technology is increasingly changing how personal information is collected, used and disclosed, federal government institutions must pay close attention to how their activities affect privacy, particularly by ensuring that they respect the principles of necessity and proportionality. One way of assessing how a program or activity affects privacy is to carry out a privacy impact assessment before it is implemented.

The federal government institutions' representatives who appeared before the Committee said that their use of digital forensic tools was necessary to keep pace with changes in technology in recent years. These tools ensure that they can obtain the evidence they need to fulfill their mandate. This evidence is no longer found in physical spaces, but rather in the filing cabinets of the modern era: mobile devices and computers.

The matter of knowing whether a privacy impact assessment should be carried out when a powerful new technological tool is used for the first time or rather at the program level was a common topic of discussion during the study. The Committee noted that clarity appeared to be lacking on this matter in the *Directive on Privacy Impact Assessment*. The President of the Treasury Board indicated that this directive was being updated to clarify requirements for these assessments.

In light of the testimony it heard, the brief it received and the supplementary information provided to it by certain witnesses, the Committee makes nine new recommendations and reiterates five recommendations from its 2022 report on device investigation tools used by the Royal Canadian Mounted Police, including one to make privacy impact assessments mandatory under the *Privacy Act*.

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.

FEDERAL GOVERNMENT'S USE OF TECHNOLOGICAL TOOLS CAPABLE OF EXTRACTING PERSONAL DATA FROM MOBILE DEVICES AND COMPUTERS

INTRODUCTION

Background

On 29 November 2023, Radio-Canada published an article stating that contracts obtained under the *Access to Information Act* had revealed that tools capable of extracting personal data from mobile phones or computers were being used by at least 13 federal departments and agencies.[1] The article also stated that the use of that technology had not undergone a privacy impact assessment (PIA), despite the *Directive on Privacy Impact Assessment* (Directive on PIA) of the Treasury Board of Canada (Treasury Board).[2] An English version of the article was published on 1 December 2023.[3]

On 6 December 2023, in response to this article, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) adopted a unanimous motion to undertake a study on the federal government's use of technological tools capable of extracting personal data from mobile phones and computers.

Between 1 February and 21 March 2024, the Committee held six public meetings and heard 32 witnesses. The Committee invited the institutions named in the article to appear so they could clarify the situation. It invited other relevant witnesses, such as the President of the Treasury Board, to appear as well. It also received one brief. The Committee would like to thank all those who participated in the study.

1 Brigitte Bureau, *Des outils potentiellement intrusifs utilisés par au moins 13 ministères fédéraux*, *Radio-Canada*, 29 November 2023.

2 Ibid.

3 Brigitte Bureau, *Tools capable of extracting personal data from phones being used by 13 federal departments, documents show*, *CBC News*, 1 December 2023.

Structure of the Report

The report is divided into four chapters. Chapter 1 provides an overview of the legislative framework and Treasury Board policies and directives that apply to privacy in the federal public sector. Chapter 2 explains the distinction between tools capable of extracting personal data from mobile devices or computers, or "digital forensic tools," and spyware.[4] It also provides an overview of what officials from the federal government institutions who appeared before the Committee said about using digital forensic tools and conducting PIAs.

Chapter 3 discusses the privacy of employees of federal government institutions and the possibility of digital forensic tools being used for internal administrative investigations. Lastly, Chapter 4 focuses on measures, legislative or other, that would provide the Government of Canada with a better framework for the use of powerful technological tools by federal government institutions.

The Committee's recommendations are found at the very end of chapters 3 and 4. Two appendices at the end of the report provide additional information on the use of digital forensic tools by federal government institutions.

CHAPTER 1: PRIVACY AND FEDERAL GOVERNMENT INSTITUTIONS

Privacy Act

The *Privacy Act* (PA) applies to privacy in the federal public sector. It outlines rules for collecting, using and disclosing personal information under the control of a federal government institution. The PA does not contain any provisions requiring federal government institutions to conduct a PIA.

Treasury Board Policies and Directives

In addition to the PA, the Treasury Board approves directives, policies, standards and guidelines. These instruments are not legally binding, but the expectation is that they will be complied with by federal government institutions. Some of them address privacy in particular.

4 Several terms are used to describe the tools capable of extracting personal data from mobile phones that the Committee is studying. The most common term used by witnesses is "digital forensic tool," which the Committee has chosen to use in its report.

Policy on Privacy Protection

The Treasury Board's *Policy on Privacy Protection* provides guidance to federal government institutions to ensure that the PA is respected. One of its objectives is to ensure that Canadians have confidence that their personal information under the control of federal government institutions is effectively protected and managed.[5] Philippe Dufresne, the Privacy Commissioner of Canada, reminded the Committee that section 4.2.2 of this policy, states that a federal government institution is responsible for

> Notifying the Privacy Commissioner of any planned initiatives (legislation, regulations, policies, programs) that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of Canadians. This notification is to take place at a sufficiently early stage to permit the Commissioner to review and discuss the issues involved.[6]

Another requirement of the *Policy on Privacy Protection* is to ensure that, when applicable, PIAs are developed, maintained and published.[7]

Directive on Privacy Impact Assessment

The objective of the Treasury Board's *Directive on Privacy Impact Assessment* is to ensure that careful consideration is given to privacy risks with respect to the creation, collection and handling of personal information as part of government programs or activities. The directive provides that PIAs be conducted in a manner that is commensurate with the level of privacy risk identified prior to establishing any new or substantially modified program involving personal information.[8]

Mr. Dufresne explained that the *Directive on PIA* provides that federal government institutions must conduct a PIA in the following circumstances:

- when personal information may be used as part of a decision-making process that directly affects the individual;

5 Treasury Board of Canada, *Policy on Privacy Protection*, s. 3.1.

6 Ibid., s. 4.2.2.

7 Ibid., s. 4.2.4.

8 Treasury Board of Canada, *Directive on Privacy Impact Assessment*, ss. 5.1 and 5.2.

- when there are major changes to existing programs or activities where personal information may be used for an administrative purpose;

- when there are major changes to existing programs or activities as a result of contracting out or transferring programs or activities to another level of government or to the private sector; and

- when new or substantially modified programs or activities will have an impact on overall privacy, even where no decisions are made about individuals.[9]

Mr. Dufresne noted that, when the Office of the Privacy Commissioner of Canada (OPC) meets with federal government institutions, it promotes the use of PIAs as an effective risk management process. PIAs ensure that potential privacy risks are identified and mitigated across programs and services that collect and use personal information.

With regard to the decision to conduct a PIA, Mr. Dufresne noted that, with technology increasingly changing the manner in which personal information is collected, used and disclosed, federal government institutions must carefully consider and assess the privacy implications of their activities to determine if and when PIAs are required. He acknowledged that the use of a new tool does not always trigger the need for a PIA; it depends on how the tool is being used and what is being done with the information that it collects.

The *Directive on PIA* states in section 3.3 that, "if not properly framed within an institution's broader risk management framework, conducting a PIA can be a resource-intensive exercise." Mr. Dufresne conceded that discipline is required to conduct a PIA. It requires that federal government institutions look into their program and answer some questions. Therefore, he believes that it is legitimate to have criteria to determine whether a PIA is required. However, he said that they "are not so resource-intensive that they're not worth doing."

Lastly, Mr. Dufresne said that PIAs are mandatory under Treasury Board policies, but not under the PA. However, he acknowledged that a directive is more than just an encouragement.

9 Ibid., ss. 6.3.1 and 6.3.2.

Directive on Privacy Practices

The *Directive on Privacy Practices* provides guidance to federal government institutions on how to implement effective privacy practices. One of its objectives is to facilitate the implementation and public reporting of consistent and sound privacy management practices for the protection of personal information throughout its lifecycle. For example, it outlines training requirements for employees of federal government institutions about privacy protection and on the process for creating personal information banks.[10]

Personal Information Banks

Some witnesses mentioned personal information banks (PIBs).[11] PIBs are descriptions of personal information under the control of a federal government institution that describe how personal information is collected, used, disclosed, retained or disposed of in the administration of a federal government institution's program or activity.[12]

Pursuant to section 10(1) of the PA, the head of a federal government institution must cause to be included in PIBs all personal information under the control of their institution that has been used or is being used for an administrative purpose.

Mr. Dufresne clarified that the PIBs indicate what information the federal government institution holds, why it collected it and what the purpose of that collection is. It is a type of proactive disclosure.

CHAPTER 2: USE OF DIGITAL FORENSIC TOOLS BY FEDERAL GOVERNMENT INSTITUTIONS

Distinction Between Spyware and Digital Forensic Tools

Mr. Dufresne explained that digital forensic tools are used to extract and examine large numbers of files from laptops, hard drives or mobile devices. They are typically used in

10 Treasury Board of Canada, *Directive on Privacy Practices*, s. 4.

11 House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Evidence*, 44th Parliament, 1st Session: Aaron McCrorie (Vice-President, Intelligence and Enforcement, Canada Border Services Agency [CBSA]); and Pierre Pelletier (Chief Information Officer, Department of Natural Resources [NRCan]).

12 Treasury Board of Canada, *Standard personal information banks*.

investigations or technical analysis, they require physical access to the device, and they often are used with the knowledge of the device owner.[13]

As for spyware, Mr. Dufresne said that, unlike digital forensic tools, such software is typically installed remotely on a person's device without their knowledge. It can then covertly collect personal information, such as keylogging and web-browsing history. Spyware is often used illegally or without authorization.

With regard to the capacities of digital forensic tools, Mr. Dufresne indicated that they could, in certain instances, unlock a locked smart phone or access password-protected laptops and tablets. However, he reiterated the fact that these tools are not used remotely, meaning that the investigator must have the device in their possession. That is one of the distinctions between these tools and spyware.[14]

Mr. Dufresne also explained that digital forensic tools can be used for a number of purposes, such as analyzing the metadata of a file, determining when an operating system was changed or recovering deleted data. In his view, they are useful investigative tools that can help preserve the integrity of the chain of evidence.[15]

Mr. Dufresne added that the OPC had itself used digital forensic tools in its investigations of privacy breaches to determine the nature, scale and scope of the incident. He does not consider their use to be completely unacceptable or a practice to be stopped altogether. However, a privacy lens is needed to reap the benefit of the tool while ensuring that our fundamental rights are protected.

Of the federal government institutions' representatives who appeared before the Committee, only those from the Royal Canadian Mounted Police (RCMP) said that they use "on-device investigative tools" (ODITs) in certain circumstances, as part of criminal investigations. ODITs are used to intercept information on a device without the owner's knowledge. They are deployed on devices or computer networks via remote, near or close access to allow electronic monitoring.[16] ODITs are different from the digital forensic tools that are the object of the Committee's study.

---

13 ETHI, *Evidence*, Philippe Dufresne (Privacy Commissioner, Office of the Privacy Commissioner of Canada).

14 ETHI, *Evidence*, Dufresne.

15 ETHI, *Evidence*, Dufresne.

16 ETHI, *On-Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues*, Report, 44th Parliament, 1st Session, November 2022, pp. 19–20; and Royal Canadian Mounted Police (RCMP), *Q&A with an expert in electronic surveillance on the challenges and opportunities of collecting evidence*, 27 July 2022.

Mr. Dufresne noted that ODITs, which are used to obtain data covertly and remotely from targeted devices, are a form of spyware. However, he said that, in a law enforcement context, legal authorization is required before ODITs can be used. In these cases, ODITs are legal and appropriate.[17] They are not being used illegally or without authorization. Bryan Larkin, Deputy Commissioner of Specialized Policing Services with the Royal Canadian Mounted Police, confirmed that the RCMP had completed a PIA on ODITs in September 2023, which it submitted to the Privacy Commissioner and the Treasury Board.[18]

Of note, the Committee carried out a study in 2022 about on-device investigative tools used by the Royal Canadian Mounted Police and it presented a report to the House of Commons. The current report focuses on digital forensic tools, not ODITs.

Key Points Regarding the Use of Digital Forensic Tools by Federal Government Institutions

Representatives of 12 of the 13 federal government institutions named in the article that led to the Committee's study appeared as part of the study.[19]

Purchase of Digital Forensic Tools

Overall, the federal government institutions' representatives who appeared before the Committee indicated that it was necessary for them to purchase digital forensic tools in order to keep pace with recent technological changes. The evidence they need to obtain to fulfill their mandate is no longer always found in physical places, but rather on mobile devices or computers.

For example, Brent Napier, Acting Director General of Conservation and Protection with the Department of Fisheries and Oceans (Fisheries and Oceans Canada), indicated that historically the harvesting and reporting of fisheries resources was all done using paper forms. Today, harvesters have adopted new technology—such as chart plotters, electronic logs and electronic communication devices—into their harvesting operations. He said that electronic devices are the modern-day equivalent of filing cabinets, and these digital tools are the key to opening them.

17 ETHI, *Evidence*, Dufresne.

18 RCMP, Letter to the Committee, 21 December 2023; and RCMP, *Covert Access and Intercept Team privacy impact assessment*.

19 Global Affairs Canada was invited, but it did not appear before the Committee.

Donald Walker, Chief Enforcement Officer at Environment and Climate Change Canada (ECCC), noted that, "in order to retrieve the information we might get out of a filing cabinet in previous times, we actually needed to gain access to electronic devices to develop the evidence necessary to pursue the investigation."

Aaron McCrorie, Vice-President of Intelligence and Enforcement at the Canada Border Services Agency (CBSA), said that CBSA would have had a locksmith open a box with receipts in another era. Today, receipts for cases involving firearms smuggling are electronic and kept on a cellphone or computer. Therefore, CBSA needs a way to access this information and translate it into a format that can be used in a court of law.

On the topic of whether the use of these tools is truly necessary and proportionate to the intended objectives, many witnesses said that, without these tools, they would not have access to the evidence they need to fulfill their mandate.[20] In their view, these tools are therefore necessary.

Use of Digital Forensic Tools

Mr. Dufresne said that, when he examined the responses from the 13 federal government institutions with which he had corresponded, he did not identify any inappropriate purposes or uses of the digital forensic tools that could be cause for concern.[21] The institutions appear to all be using these tools to fulfill their mandates, apply their enabling legislation or conduct investigations. He clarified that some departments may use digital forensic tools to investigate contraventions of the law by Canadians.[22]

Representatives of the federal government institutions indicated that a mobile device or computer must be physically in their possession in order to use a digital forensic tool on it.[23] Most said that they could gain physical access to a device as part of an investigation; through a court order or a search warrant that identifies what information can be

20 ETHI, *Evidence*: Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission [CRTC]); McCrorie (CBSA); France Gratton (Assistant Commissioner, Correctional Operations and Programs, Correctional Service of Canada [CSC]); Nicolas Gagné (Superintendent, RCMP); Bryan Larkin (Deputy Commissioner, Specialized Policing Services, RCMP); Donald Walker (Chief Enforcement Officer, Department of the Environment [ECCC]); Hannah Rogers (Director General, Environmental Enforcement, ECCC); Kathy Fox (Chair, Transportation Safety Board of Canada [TSB]); and Eric Ferron (Director General, Criminal Investigations Directorate, Compliance Programs Branch, Canada Revenue Agency [CRA]).

21 ETHI, *Evidence*, Dufresne.

22 ETHI, *Evidence*, Dufresne.

23 ETHI, *Evidence:* Gagné (RCMP); McCrorie (CBSA); Gratton (CSC); Ferron (CRA); Harroun (CRTC); Larkin (RCMP); Scott Jones (President, Shared Services Canada [SSC]); and Fox (TSB).

collected; or through powers conferred by an act.[24] Some witnesses reminded the Committee that only information expressly targeted by the court order or search warrant is shared with the investigator by the digital forensic expert.[25]

Representatives of the federal government institutions also confirmed that their institutions are not using spyware to carry out surveillance on the general Canadian population and are not carrying out mass surveillance.[26] Many witnesses clarified that no technological tools are left on the device to carry out long-term surveillance once the federal government institution's investigation has been completed and the device is returned to the owner.[27]

Various representatives of the federal government institutions also explained that the digital forensic tools are used only by a small number of digital forensics analysts within their institution.[28] Many raised the point that data collected from technological devices that had been seized were kept in secure areas, such as in specialized laboratories and on computers that do not have network or Internet access.[29]

With regard to the potential use of digital forensic tools on mobile devices or computers provided to government employees, a few federal government institutions' representatives confirmed that they may do so as part of internal administrative investigations. This use is covered in Chapter 3.

---

24 ETHI, *Evidence*: McCrorie (CBSA); Larkin (RCMP); Ferron (CRA); Ferron (CRA); Harroun (CRTC); Harroun (CRTC); Harroun (CRTC); Brett Napier (Acting Director General, Conservation and Protection, Department of Fisheries and Oceans [DFO]); Walker (ECCC); Walker (ECCC); Gratton (CSC); Larkin (RCMP); Mario Mainville (Chief Digital Officer, Competition Bureau Canada [CB]); Jones (SSC); Fox (TSB); and Office of the Privacy Commissioner of Canada, *Letter to the Committee*, 8 March 2024. Mr. Larkin said that the RCMP may use these tools under exigent circumstances when it is not possible to obtain a warrant, but in that case the use is pursuant to the *Criminal Code*. Correctional Service Canada, Transportation Safety Board and Shared Services Canada invoked their statutory authority in using these tools.

25 ETHI, *Evidence*: Rodgers (ECCC); Larkin (RCMP); Gagné (RCMP); and Mainville (CB).

26 ETHI, *Evidence:* Francis Brisson (Assistant Deputy Minister and Chief Financial Officer, NRCan); Dave Yarker (Director General, Cyber and Command and Control Information Systems Operations, Department of National Defence [DND]); Sophie Martel (Acting Chief Information Officer, DND); Walker (ECCC); Larkin (RCMP); Ferron (CRA); Napier (DFO); Harroun (CRTC); Harroun (CRTC); Napier (DFO); Walker (ECCC); Larkin (RCMP); Jones (SSC); Fox (TSB); and Mainville (CB).

27 ETHI, *Evidence*: Fox (TSB); Gagné (RCMP); McCrorie (CBSA) Gratton (CSC); and Mainville (CB). In the case of Correctional Service Canada, the devices seized are contraband, so they are not returned to the owners.

28 ETHI, *Evidence*: Ferron (CRA) Walker (ECCC); Walker (ECCC); Rogers (ECCC); Napier (DFO); Gratton (CSC); Fox (TSB); and Mainville (CB).

29 ETHI, *Evidence*: Gratton (CSC); Pelletier (NRCan); McCrorie (CBSA); McCrorie (CBSA); Napier (DFO); Mainville (CB); Jones (SSC); and Mainville (CB).

The table in Appendix A of the report provides additional information on the use of digital forensic tools by the 12 federal government institutions whose representatives appeared before the Committee. The table in Appendix B indicates whether other federal government institutions purchased or have access to software that could be used to extract information from electronic devices.

Privacy Impact Assessments

Although the article that led to the study indicated that none of the federal government institutions in question had conducted a PIA on the use of digital forensic tools, some federal government institutions' representatives clarified before the Committee that a PIA had in fact been carried out at the program level. A separate PIA for the digital forensic tool itself had not been conducted.

Other federal government institutions' representatives indicated that a PIA on the use of these tools was underway: either they had already committed to conducting one shortly, or they were in the process of studying the possibility of conducting one. One federal government institution representative said that his institution would conduct a PIA if it decided to use the digital forensic tool that was purchased.

Mr. Dufresne acknowledged that, in some cases, the federal government institutions that had not done a PIA on their use of digital forensic tools were not compliant with the Treasury Board's *Directive on PIA*.

Privacy Impact Assessments at the Program Level

With regard to the Canada Revenue Agency (CRA), Mr. Ferron, the Director General of the Criminal Investigations Directorate at the Compliance Programs Branch, indicated that a PIA has been in place for the CRA's entire Criminal Investigations Program since 2016.[30] It was updated recently. He confirmed that this PIA was for the program as a whole, and not for the tools that are used. He said that the PIA conducted by the CRA indicates that, when electronic devices are seized, CRA experts use tools to extract information.

Anne-Marie Laurin, Acting Director General and Deputy Chief Privacy Officer at the CRA, added that this PIA had been submitted to the Privacy Commissioner at the time, and it did not elicit any comments.

30 ETHI, *Evidence:* Ferron (CRA); and Ferron (CRA).

On behalf of the CRTC, Mr. Harroun indicated that, when Canada's anti-spam legislation (CASL) came into force in 2014, three PIAs were conducted.[31] One PIA specifically references CASL's section 19, which addresses search warrants and the use of digital forensic tools. He said that a valid PIA has been in place since 2014 for the tools the CRTC is currently using.[32] Mr. Harroun confirmed that the PIA had been conducted at the program level and not at the level of a specific tool. In his view, the PIA at the program level is sufficient, because the program is very clear that digital forensic tools will be used to collect evidence.

For Fisheries and Oceans Canada, Sam Ryan, Director General of Information Technology Operations, indicated that a PIA had been carried out for the Conservation and Protection program around 2010. No PIAs were conducted for a specific digital forensic tool.[33] He highlighted that the tool is only one part of the program, and that when digital forensic tools were purchased, they were considered to be an extension of existing programs. However, Mr. Napier acknowledged that, at this stage, it was warranted for Fisheries and Oceans Canada to review its processes to ensure that the department is protecting privacy appropriately. The department made a commitment to submit an updated PIA for the program in question to the Privacy Commissioner in December 2023.[34]

Luc Casault, the Director General of Corporate Services at the Transportation Safety Board (TSB), clarified that a PIA had been in place for the investigation program since it was established, but that an assessment had not been conducted for the digital forensic tool itself. In the same vein as Fisheries and Oceans Canada, TSB Chair Kathy Fox said that, because this type of data extraction was an established practice, and because a PIA had already been conducted at the program level, the TSB did not believe it was necessary to conduct a separate assessment for the digital forensic tool itself.

However, she said that, following a discussion with the Privacy Commissioner, the TSB had committed to updating the PIA for its investigation program to ensure that it is inclusive of all the current technologies being used to deliver on its mandate. Mr. Casault said that the Privacy Commissioner "definitely recommended updating the assessment for our program."

---

31 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23.

32 ETHI, *Evidence*, Harroun.

33 ETHI, *Evidence:* Sam Ryan (Director General, Information Technology Operations, DFO); and Napier (DFO).

34 ETHI, *Evidence*, Sam Ryan (DFO).

Privacy Impact Assessments Already Underway, Upcoming or Under Consideration

With regard to the RCMP, Mr. Larkin said that a PIA on digital forensic tools was underway and would be completed by mid-2024.

For the CBSA, Mr. McCrorie noted that it began working with its internal partners to do a PIA on the entire CBSA Criminal Investigations Program in 2022.[35] The CBSA will continue to conduct this assessment, and it hopes to do so in collaboration with the OPC.[36] He confirmed that the CBSA's PIA is at the program level, not the tool level. He explained that the CBSA had determined that, rather than doing a PIA for each individual device, it needed to do a PIA that takes into account how the devices are being used in the context of the program.

In the case of Correctional Service Canada, (CSC), France Gratton, the Assistant Commissioner of Correctional Operations and Programs, explained that, once a digital forensic tool had been purchased in 2010, CSC conducted a series of verifications to determine if a PIA was required. At the time, based on the program CSC was setting up, the tool that was being used and the way in which the information was going to be managed, it was determined that a PIA was not necessary. However, she said that, "[a]s the use of enhanced tools to combat criminal activity has expanded over the past few years, CSC has committed to renewing the initial assessment and to completing an updated checklist."

With regard to the Department of National Defence (DND), Mr. Yarker, the Director General of Cyber and Command and Control Information Systems Operations, said that no PIA had been done on the use of a digital forensic tool. However, Sophie Martel, Acting Chief Executive Officer, said that DND had a number of PIAs on the go, and gave the example of a PIA on Microsoft 365. She said that DND is studying the need for a PIA on its use of digital forensic tools.

ECCC representatives confirmed that no PIAs had been conducted for its use of a digital forensic tool.[37] Mr. Walker explained that the department had established its digital forensics unit in 2013, which was viewed as a natural extension of the search warrant process.[38] He added that, at the time the program was established, it was determined

35 ETHI, *Evidence*, McCrorie (CBSA).

36 ETHI, *Evidence*, McCrorie (CBSA).

37 ETHI, *Evidence*, Walker (ECCC).

38 ETHI, *Evidence*, Walker (ECCC).

that a PIA was not necessary, since the program's purpose was not to collect, store or treat personal information.[39]

However, Mr. Walker said that, as ECCC was "going through a modernization exercise with respect to implementing a risk-based approach to our enforcement activities and a periodic review of our directives," it had determined that it would be prudent to engage in new PIAs to cover not only a specific tool, but also the activities that ECCC undertakes in order to take into account the context in which the various tools are used.[40]

Mr. Walker said that ECCC is in the process of conducting new PIAs, with priority given to those that focus on operational activities. Its intentions were communicated to the Privacy Commissioner in June 2022. Hannah Rodgers, the Director General of Environmental Enforcement, said that the PIA relating to ECCC's operational activities would be completed within the coming year.

The President of Shared Services Canada (SSC), Scott Jones, confirmed that no PIAs were carried out at the program level when SSC was established or in association with any digital forensic tools used by SSC, but that SSC had begun an assessment.[41] He clarified that, in the context where SSC is only purchasing a tool on behalf of another federal government institution, it is not SSC's responsibility to assess the institution's use of the tool.

For the Competition Bureau, Mario Mainville, Chief Digital Officer, said that no PIA had been conducted at the program level for which the digital forensic tool had been used. He explained that the program had been in place since before the *Directive on PIA* was issued, and that when the directive came into force, it was determined that the program had not undergone any major changes since it had been established in 1996.[42] According to the Competition Bureau, adding new, more advanced devices did not constitute a radical change.[43]

However, Mr. Mainville said that, after the Privacy Commissioner's testimony and the news article that was published in late 2023, the Competition Bureau had contacted the

39 ETHI, *Evidence*, Walker (ECCC).

40 ETHI, *Evidence*, Walker (ECCC).

41 ETHI, *Evidence*, Jones (SSC).

42 ETHI, *Evidence*, Mainville (CB).

43 ETHI, *Evidence*, Mainville (CB).

Office of the Privacy Commissioner and started the process of evaluating its entire computer forensic program.[44]

Privacy Impact Assessments if the Tool Is Used

Francis Brisson, Assistant Deputy Minister and Chief Financial Officer at Natural Resources Canada (NRCan), said that NRCan had never used the digital forensic tool in question, and thus no PIA had been done.[45] He explained that NRCan purchased the tool to add to its toolbox.[46] He said that NRCan uses technological tools to safeguard its technological and data assets. Mr. Brisson also confirmed that a PIA would be conducted if the digital forensic tool purchased by NRCan becomes needed for an investigation. However, he seemed to indicate that NRCan might consider conducting a PIA following his appearance before the Committee.[47]

Observations of the Privacy Commissioner of Canada

Prior Consultation with the Commissioner

Mr. Dufresne confirmed that the OPC had learned in the news that 13 federal government institutions were using digital forensic tools on mobile devices or computers. He said that the OPC was aware of some government programs, but not of all the ways these tools were being used. He said:

> What I would have liked, in a situation like this, is for my office to have been consulted beforehand in the 13 cases and for us to have all the necessary information so that, in response to the media, we could confirm to them what has happened, tell them that we have been notified, that we have given advice, that an assessment has been made and that we have no problem with it, or the opposite, and then present the recommendations we have made.

Mr. Dufresne also noted that the OPC does not know what a department is doing unless that department advises or consults the OPC. Therefore, it is always preferable for a department to reach out proactively. The OPC can then provide input and flag any risks.

Mr. Dufresne confirmed that, when the OPC is consulted ahead of time, it has the opportunity to raise questions that help determine whether a practice is necessary and

44 ETHI, *Evidence*, Mainville (CB).

45 ETHI, *Evidence*, Brisson (NRCan).

46 ETHI, *Evidence*, Brisson (NRCan); and Pelletier (NRCan).

47 ETHI, *Evidence*, Brisson (NRCan).

proportionate, and it could potentially prevent situations where practices are not in line with these important principles. Prior consultation also reassures the Canadian public that the OPC was consulted and gave its opinion on a certain practice.

Mr. Dufresne said that he would like to see departments take a more proactive approach to communicate with the OPC to share information on what they are considering doing and ask the OPC whether a PIA is needed. This would avoid the OPC learning about that information in the news. He noted that departments do not always have the reflex to check whether the OPC has been informed before they set up a program. In his view, there are improvements to be made in that regard.

Mr. Dufresne reminded the Committee that the OPC has a government advisory team that is always on standby to hear from departments and provide them with advice. With regard to the OPC's resources, which ensure that it can review PIAs and provide advice to departments or other federal government institutions that may use similar digital forensic tools, Mr. Dufresne indicated that the OPC prioritizes what comes in based on importance and how it will affect privacy.[48]

Regarding the OPC's capacity to assess the impact of AI on privacy, Mr. Dufresne explained that the Office is well equipped to do so, with a technology laboratory that keeps abreast of the latest technological developments.[49]

Understanding of the *Privacy Impact Assessment Directive*

Mr. Dufresne said that federal government institutions make a distinction between new programs or activities and existing programs or activities. However, sometimes, they may determine that, since all they are doing is using a new, more powerful tool, it is not a new program, as they have not really changed what they are doing. Since the existing program was assessed already for privacy risks, they do not undertake a PIA for the tool itself. He acknowledged that this interpretation is consistent with the policy, in the sense that the directive does not require a new PIA for an existing program. However, he added that, when it comes to very powerful tools—even if they are being used within an existing program—they might change the playing field by expanding capability significantly. In these cases, it raises the question of whether Canadians would benefit from more transparency on that new tool, even if it is being used within an existing program.

48 ETHI, *Evidence*, Dufresne.

49 ETHI, *Evidence*, Dufresne.

In the case of the use of digital forensic tools, Mr. Dufresne said that these tools could be used in ways that raise important privacy risks that would merit a full PIA. For example, he suggested that where these tools are used in an internal investigation about an employee's conduct, where a decision will be made that will directly affect that individual, or in cases where these tools are used as part of an inquiry into alleged criminal or illegal activities, a PIA should be required. In these circumstances, the PIA should address "not only the specific tool being used to collect personal information, but the broader program under which the tool is being used."

Mr. Dufresne also said that digital forensic tools are able to retrieve information from devices and computers, including information that has been deleted, and they are able to obtain personal information as well. That is why, in situations where they are used and directed toward individuals, such as employees, or in other circumstances where they are used in a way that raises privacy risks, a PIA should be done.

Mr. Dufresne also mentioned that the OPC must sometimes remind departments that, even if they are doing something under a warrant or a valid legal authority, the PIA is a separate matter. It is an extra step.[50] He said that the warrant may be based on criteria that are distinct from the privacy considerations that are at the heart of the PIA. Therefore, even if there is a warrant and a legal basis, the federal government institution must still consider whether a PIA is needed.[51]

Some of the federal government institutions' representatives acknowledged that the fact that the tool will be used as part of an investigation, with a search warrant or court order, does not replace a PIA.[52]

As Mr. Dufresne stated, "[s]ome of these tools can be used appropriately—there are good reasons for it—but we need that privacy check. We need that assessment."

Follow-up with the Federal Government Institutions and Limits to the Commissioner's Power

Mr. Dufresne said that the OPC had followed up with the 13 institutions identified in the Radio-Canada news report.[53] He clarified that some institutions seemed to use these tools as a regular part of their activities, while others used them more rarely. He said

50 ETHI, *Evidence*, Dufresne.

51 ETHI, *Evidence*, Dufresne.

52 ETHI, *Evidence:* Mainville (CB); Casault (TSB); and Fox (TSB).

53 ETHI, *Evidence:* Dufresne and Dufresne.

that, whether the tool was used two, three or four times or whether it was used regularly, the OPC looks at the situation in the same way: is the use appropriate, and should the department conduct a PIA or not?

Mr. Dufresne also told the Committee that the OPC would continue to follow up with the 13 federal government institutions to ensure that missing PIAs were conducted and to insist on the need to comply with Treasury Board directives.[54]

However, he said that, without a requirement in the PA, there are limits to what the OPC can do to ensure compliance. Mr. Dufresne explained that there is a distinct difference between a Treasury Board policy or directive and an obligation under the PA. The policy or directive is an internal rule that the government imposes on itself that lays out what is expected of a department. It does not have any binding legal force and therefore does not allow the Privacy Commissioner to carry out an investigation for failure to comply with the rule. In contrast, the obligations in the PA are binding. The OPC may investigate if it has reasonable grounds to believe that a provision of the PA has been contravened.

Given the foregoing, Mr. Dufresne confirmed that the OPC was not conducting any investigations of the federal government institutions listed in the news report regarding non-compliance with the *Directive on PIA*. He reiterated that, since there is no legal requirement to conduct a PIA under the PA, he has no reason to investigate non-compliance with a directive.

CHAPTER 3: PRIVACY OF FEDERAL GOVERNMENT INSTITUTIONS EMPLOYEES

Use of Digital Forensic Tools on Devices of Federal Government Institutions Employees

Mr. Dufresne told the Committee that, when a federal government institution uses digital forensic tools to monitor employees, it must take steps to ensure respect for the fundamental right to privacy. In his opinion, clear rules are needed about when and how monitoring technologies are to be used. The OPC published guidance on privacy in the

54 ETHI, *Evidence*, Dufresne.

workplace in May 2023 and—together with its provincial counterparts—issued a joint resolution on protecting employee privacy in the workplace in October 2023.[55]

In a document he sent to the Committee following his appearance, Mr. Dufresne stated that the guidance document of May 2023 entitled *Privacy in the Workplace* outlines key privacy considerations for employers managing employees' personal information and discusses topical issues such as the monitoring of employees.

With regard to the joint resolution of October 2023, his letter mentions that those with responsibility for privacy oversight were calling for

> a collective effort from governments and employers to address statutory gaps, respect and protect employee rights to privacy and transparency, and ensure the fair and appropriate use of electronic monitoring tools and AI technologies in the modern workplace.[56]

The use of AI in a work context will be addressed later in this report.

Mr. Dufresne also said that, to respect employees' privacy rights, institutions must ensure that a technological tool is used for a purpose that is linked to the one that has been identified; that it is transparent; that it is proportional; and that a PIA has been conducted, where appropriate. In his view, each institution must assess the tool according to the principles of necessity and proportionality in association with its use.

As the OPC indicated, the principles of necessity and proportionality "ensure that privacy-invasive practices are carried out for a sufficiently important objective, and that they are narrowly tailored so as not to intrude on privacy rights more than is necessary."[57]

Mr. Dufresne gave an example of an investigation carried out under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), after which the OPC concluded that a trucking company using a monitoring device in the cab of its trucks to record audio and video 24/7 was not complying with PIPEDA principles. The OPC found

---

55 Office of the Privacy Commissioner of Canada, *Privacy in the Workplace*, revised on 29 May 2023; and *Protecting Employee Privacy in the Modern Workplace*, Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight, 4 to 5 October 2023. In the case of private-sector organizations, the *Personal Information Protection and Electronic Documents Act* applies only to employees of organizations under federal jurisdiction. Otherwise, it is provincial legislation, or the common law that applies.

56 Privacy Commissioner of Canada, *Letter to Committee*, 23 February 2024, p. 3.

57 Privacy Commissioner of Canada, *Privacy guidance on facial recognition for police agencies*, May 2022, para. 60.

that it was legitimate to use the monitoring device only while truck drivers were driving, for safety reasons.[58]

With regard to employers accessing employees' personal information, Mr. Dufresne mentioned the principle of limiting collection, which is linked to the principles of necessity and proportionality. An employer must not collect and use more information than they need for their stated purpose. When accessing an employee's personal information on an electronic device, an employer must be transparent and ensure that the employee is aware that it is a work device. The employer must also describe its expectations of what it will have access to and explain why it needs access to that information.[59] On this topic, Mr. Dufresne gave an example of health information that an employee might have on a mobile device that they are using for work. Before accessing the data, the employer must first consider whether it needs to access this information.

Mr. Dufresne said that, generally speaking, digital forensic tools used by federal government institutions as part of administrative investigations involving employees would be used only on devices provided to the employee by the employer.

Furthermore, CSC, NRCan, CBSA, CRA, CRTC, Fisheries and Oceans Canada, ECCC and RCMP representatives all confirmed that digital forensic tools are not used to monitor employees without their knowledge.[60] If digital forensic tools are used for internal investigations, the employees know about it, because it requires having physical access to the device.

For CSC, Ms. Gratton specified that digital forensic tools are used only on seized, contraband cellular phones that were introduced into a CSC institution illegally.

Expectations are different for DND employees than for other federal public servants. Ms. Martel explained that there is only a limited expectation of privacy when it comes to using DND's IT systems and mobile devices, because they are subject to monitoring for the purposes of system administration, maintenance and security, as well as to ensure policy compliance.

Ms. Martel clarified that, when an account is created on the DND network, employees must sign to confirm that they will use the device only to do government work in order

58 Office of the Privacy Commissioner of Canada, *Investigation into Trimac's use of an audio and video surveillance device in its truck cabins*, PIPEDA Findings #2022-006, 27 July 2022.

59 See: Office of the Privacy Commissioner of Canada, *Privacy in the Workplace*, 29 May 2023.

60 ETHI, *Evidence*: Gratton (CSC); Pelletier (NrCan); McCrorie (CBSA); Ferron (CRA); Harroun (CRTC); Ryan (DFO); Walker (ECCC); and Larkin (RCMP).

to have access to their account. However, she recognized that some employees do use these devices for personal use.

With regard to how the RCMP uses digital forensic tools with its own employees, Mr. Larkin noted that using its digital forensics program for administrative investigations is governed by legislation and policies. He said that the collection of evidence through these tools is based on necessity and proportionality, considering the allegations that led to the internal conduct investigation. He clarified that the RCMP would perform an examination only on RCMP-owned devices, and that any personal device would require a judicial warrant.

Mr. Larkin said that the RCMP uses digital forensic tools on employees' phones only when there is a specific allegation relating to a code of conduct and an internal investigation is taking place, or when an employee is involved in a criminal investigation. In the latter case, the RCMP will seek judicial authorization. In the case of internal misconduct, the investigator will consult with the RCMP's digital forensics experts and assess whether it is necessary to use the digital forensic tool in question.

Mr. Larkin clarified that the RCMP had used a digital forensic tool on only one occasion as part of an internal matter. It was a departmental security investigation, and the tool was used with the RCMP employee's consent.[61]

With regard to the CRA's Criminal Investigations Program, use of digital forensic tools is limited to external investigations, meaning the tool would not be used as part of an internal investigation of CRA employees, said Mr. Ferron.

For Fisheries and Oceans Canada, Mr. Napier and Mr. Ryan confirmed that digital forensic tools may be used for internal administrative investigations, such as investigations into violations of Government of Canada policies and cybersecurity incidents.

Mr. Pelletier said that it was possible that software similar to those being studied by the Committee had been used by NRCan in the past to investigate employee misconduct, but that NRCan would not necessarily need such tools. Mr. Brisson said that, if a digital forensic tool was to be used, it would be for an internal investigation. He noted that all NRCan monitoring systems are used for internal and administrative purposes, in line with security requirements following a clear security mandate.

Mr. Jones said that federal government institutions, including SSC, use digital forensic tools to support administrative investigations that happen only when there is a credible

61 ETHI, *Evidence*, Larkin.

allegation of employee wrongdoing and to ensure the security of government networks. He explained that these investigations involve cases where an employee is suspected of inappropriate website browsing, of having installed malicious software, or of using departmental electronic networks and devices contrary to the policy.

Ms. Fox said that the TSB does not use digital forensic tools on its employees' phones at all, whether they are issued by the government or not.

The CBSA stated, in a document it submitted to the Committee, that it does not use tools or software programs to actively monitor employee use of CBSA devices.[62] In that document, the CBSA explained how it uses these tools within an investigation:

> [E]mployees from the Professional Integrity Division (PID) have the authority to access any relevant CBSA information systems, documents and records as legally permitted. When applicable to an investigation, the PID has retrieved CBSA devices from employees and extracted and reviewed data, files and information stored on the devices to help determine the extent to which alleged behaviours or events occurred.[63]

However, in a brief to the Committee, representatives of the Public Service Alliance of Canada (PSAC) said that they had

> several concerns about the use of tools that are capable of extracting personal data from devices, should there not be robust processes around the appropriate use of these tools, the protection of employees' personal information, and the disclosure of all reasons why the tools may be deployed.[64]

Their greatest concern was that so many departments had failed in their responsibilities to conduct PIAs. This concern was shared by Nathan Prier, President of the Canadian Association of Professional Employees, and by Jennifer Carr, President of the Professional Institute of the Public Service of Canada (PIPSC).

The Matter of Employee Consent

Some representatives of federal government institutions emphasized that employees subject to an internal investigation consented to having their personal information

---

62 Canada Border Services Agency, *Standing Committee on Access to Information, Privacy and Ethics (ETHI) – Use of Tools Capable of Extracting Personal Data from Mobile Devices and Computers – February 6, 2024*, p. 1.

63 Ibid.

64 Public Service Alliance of Canada [PSAC], *Brief to the Standing Committee on Access to Information, Privacy and Ethics – For the study on – Federal Government's Use of Technological Tools Capable of Extracting Personal Data from Mobile Devices and Computers*, 3 March 2024, p. 1.

verified using digital forensic tools. Mr. Jones said that SSC employees are always made aware of the conduct of these investigations by federal government institutions and that procedural fairness is ensured.

With regard to the RCMP, Mr. Larkin said that each employee signs a consent form about the use of any device they are given. As indicated above, the one time a digital forensic tool was used on the device of an RCMP employee as part of an internal administrative investigation, it was with the individual's consent.

As for Ms. Martel, she explained that to use a government device and have a DND network account, employees must fill out a questionnaire, and they are informed that they will be monitored for network security reasons.

According to Mr. Pelletier of NRCan, employees that use a federal government institution's networks have an obligation to ensure that their use complies with government policies. He added that NRCan regularly reminds employees of this obligation, with a reminder popping up automatically every time an employee connects to the department's virtual private network.

Similarly, Mr. Ryan said that the Government of Canada's acceptable use policy is displayed every time an employee connects to the network at Fisheries and Oceans Canada. In his view, it means that employees are agreeing to comply with this policy. Mr. Ryan also said that Fisheries and Oceans Canada employees who are subject to an internal administrative investigation are fully aware of the process and are informed of the scope of the investigation.

Ms. Fox confirmed that, although it is possible for the TSB to issue a warrant after a request to a justice of the peace to use a digital forensic tool, the TSB has never had to do so because the devices in question are usually obtained through consent, on site or through first responders.

Similarly, Mr. Mainville confirmed that the Competition Bureau uses digital forensic tools only with a search warrant that has been authorized by a judge. There has been only one exception, when the individual gave their consent and a consent agreement was drafted.

Evan Light, Associate Professor at Toronto Metropolitan University, gave a different perspective on the matter of consent. In his view, it is difficult, if not impossible, for employees to give informed consent when they are the subject of an internal investigation, as "there's an imbalance of power, and there's an imbalance of knowledge."

In a document submitted to the Committee, Mr. Light outlined two factors that he believes must be considered in discussions of consent: "1) whether the subject is capable of informed consent based on the information provided to them, and 2) whether they are capable of informed consent given the power dynamics at play."[65]

According to Mr. Light, consent is not enough, because people do not necessarily know what they are consenting to, and PIAs are not effective tools for self-regulation. In his view, an external body like the Office of the Privacy Commissioner should decide whether these tools should be used, and what sort of processes need to be put in place for people to give informed consent around the examination of their devices.

Mr. Light argued that public servants have a reasonable expectation of privacy on the phones provided to them by the government. He explained that PIAs do not necessarily play a standard role in how federal government institutions manage their relationships with their employees. Mr. Light said that PIAs push institutions through a line of questioning that helps them think about how to find the balance between privacy violations and privacy protections, but that this process is not necessarily clear to employees. He summed up his position by saying that the directives are there for guidance at a high level, not for understanding at the ground level.

Ms. Carr said that the applicable policies were developed at a time when cloud-based activities and encrypted data did not exist, so consent given based on these policies—which need to be updated, in her view—does not correspond to the reality today.

With regard to how a public servant gives their consent and what training they receive when they are given a government device, Ms. Carr and Mr. Prier noted that practices vary widely from institution to institution. In general, employees must sign off on the institution's values and ethics, but decentralizing responsibilities has allowed departments to adopt their own policies, said Ms. Carr.

Use of Artificial Intelligence in the Employment Sector

Starting from the premise that technological advances support the recommendation to make conducting PIAs a legal requirement—as addressed in Chapter 4 of this report—Mr. Dufresne observed on a related note that, at the conference of the Global Privacy

65 Evan Light, *To the Standing Committee on Access to Information, Privacy and Ethics*, Reference document submitted to the Committee, 5 February 2024, p. 4.

Assembly (GPA), privacy officials from around the world adopted a resolution on artificial intelligence (AI) in the area of employment.[66]

This resolution calls for governments and parliamentarians to understand the importance of setting limits on the use of AI and calls on the GPA to work with organizations that develop or implement AI tools in the employment context, such as surveillance and data collection and retention tools, to ensure that employee privacy is considered at all stages.[67]

Considering the above, the Committee makes the following recommendation.

Recommendation 1

That the Government of Canada ensure that federally regulated institutions and organizations involved in the development or use of artificial intelligence tools in an employment context guarantee that employee privacy is considered at all stages in the development or use of such tools.

CHAPTER 4: LEGISLATIVE IMPROVEMENTS AND OTHER PROPOSED MEASURES

Some witnesses recommended amending the PA to ensure greater transparency in federal government institutions' practices and to ensure that they conduct PIAs more consistently, while aligning with the concepts of necessity and proportionality. Other recommendations were also made, particularly with regard to potential amendments to Treasury Board directives.

Proposed Legislative Improvements

Mr. Dufresne reminded the Committee of the recommendation he had made in 2022 when the Committee was studying ODITs used by the RCMP—a recommendation the Committee supported—to include a legal obligation in the PA for federal government institutions to conduct PIAs.[68] Mr. Light held a similar view, specifying that in his view,

66 Global Privacy Assembly, *Resolution on AI and Employment*, Adopted Resolutions, 45th Global Privacy Assembly, Hamilton, Bermuda, 2023.

67 Privacy Commissioner of Canada, *Letter to the Committee*, 23 February 2024, p. 4.

68 ETHI, *On-Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues*, November 2022.

PIAs should be conducted before any technology is purchased. Ms. Carr, of PIPSC, also made a similar recommendation.

Mr. Dufresne explained why he believes this amendment to the PA is important:

> My vision for privacy is one where privacy is treated as a fundamental right, where privacy supports the public interest and innovation, and where Canadians trust that their institutions are protecting their personal information. Conducting a PIA and consulting my office before a privacy-impactful new technology is used would strengthen privacy, support the public interest and generate trust. This is why it should be a legal obligation for government institutions under the *Privacy Act*.

According to Mr. Dufresne, this addition should also be made to PIPEDA, so that the obligation to conduct a PIA would apply to private-sector organizations as well.[69] In support of this recommendation, Mr. Dufresne also recommended that the Privacy Commissioner be given the mandate and authority to make sure that institutions respect their obligation to carry out a PIA when required.

Mr. Dufresne also recommended that the concept of privacy by design be included at the front end when new technology is being used. He noted that a PIA is often conducted after a tool has been developed and used, and that it will always be more economical and more prudent to bring privacy from the start. This observation forms the basis of his recommendation to make PIAs mandatory under the PA.

Mr. Dufresne reminded the Committee that conducting a PIA is provided for in a Treasury Board directive. Since it is not a legal obligation, the Commissioner does not have the power to stop an institution from implementing a certain technological tool. The Commissioner's role is limited to flagging to the Treasury Board that the use of a certain tool may not comply with the PA.

Furthermore, according to Mr. Dufresne, making PIAs mandatory under the PA could ensure a more standardized approach and prevent situations such as the one that led the Committee to carry out this study, where the public discovers from the news that federal government institutions are using these tools. In his view, knowing that federal government institutions have conducted PIAs will ensure that Canadians have more trust in these institutions.

---

69 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, introduced in Parliament in June 2022, is currently at committee stage. It would replace Part I of the *Personal Information Protection and Electronic Documents Act* with a new act: the Consumer Privacy Protection Act.

The *Directive on PIA* makes distinctions between a new program and the update of an existing program, or between the assessment of a program and the assessment of the tool itself, as Mr. Dufresne mentioned. Given these distinctions, an institution can say—in good faith—that a PIA is not necessary because the directive does not require it. However, in his opinion, with technology becoming increasingly powerful, it would be preferable for PIAs to be required when new tools could affect privacy in order to reassure Canadians that assessments are being done in an even more proactive manner.

In fact, according to Mr. Dufresne, moving away from the notion of assessing the program itself, a PIA must be considered if there is a new tool that changes the context. He noted that the context of use and the safeguards in place are important points to consider in conducting a PIA. For all these reasons, he believes it would be preferable to make conducting a PIA a legal obligation under the PA.

With regard to the content of this proposed obligation, Mr. Dufresne recommended that the PA require that relevant details be provided to the OPC within a prescribed period before a program is established. He suggested that these details could be set out either in the PA or in regulations made under the PA.

Mr. Dufresne also recommended that the concepts of necessity and proportionality be included in the PA.[70] With regard to necessity, he said that the PA requires simply that the use be related to the federal government institution's mandate, while the Treasury Board directive provides that the use must be necessary to achieve the desired objective.[71] In his view, even if there is a legitimate purpose, it is important to ask whether the institution is going too far in how it is achieving it.

As for proportionality, Mr. Dufresne explained that, the more powerful the technology is and the broader the scope, the more important it is to be careful and have privacy protections in place, and the more privacy considerations there are to take into account. In other words, when it is a more intrusive tool, a more rigorous protection mechanism is needed.

Mr. Dufresne told the Committee that innovation and technology offer many advantages in multiple fields, and it is not a matter of refusing to use it. It is more a matter of

70 ETHI, *Evidence*, 1 February 2024, Dufresne.

71 *Privacy Act*, s. 4. This section provides that "[n]o personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution"; and Treasury Board Secretariat, *Directive on Privacy Practices*, s. 4.2.9 provides that a federal government institution must "[limit] the collection of personal information to what is directly related to and demonstrably necessary for the government institution's programs or activities."

ensuring that Canadians do not have to choose between benefiting from the advantages of technology and maintaining their privacy. Canadians should know that institutions are there to protect them and advise them.

Mr. Dufresne also recommended granting the Privacy Commissioner the power to issue orders and the ability to impose administrative monetary penalties under the PA, as is the case for the Commission d'accès à l'information du Québec under Law 25, for instance.[72]

Other Proposed Measures

In a document he sent to the Committee following his appearance, Mr. Light made a series of recommendations grouped into four themes: safeguarding the fundamental human right to privacy; access to information and proactive disclosure; data sovereignty and the safeguard of democratic institutions; and procurement.[73]

Mr. Light recommended giving the Privacy Commissioner of Canada judicial authority, saying that the OPC "must have the mandate and resources of a proactive regulator that aims to safeguard the fundamental human right to privacy with relation to the federal government and with relation to the private sector."

With regard to procurement, he recommended that the OPC play a central role in procurement and be given veto power over procurement. According to Mr. Light, the OPC should be tasked with approving any technological purchases, be they software or hardware. Furthermore, to gain approval, these technologies should be subject to PIAs conducted by the OPC, not the institutions that intend to use them. Mr. Light also recommended that, "[i]n the spirit of open government, transparency and accountability," the Government of Canada carry out a full examination of its procurement and reporting processes.

The PSAC brief recommended that the Treasury Board implement a specific directive that creates a remedial process in case senior bureaucrats do not conduct appropriate PIAs, or do not use the technology appropriately, and that the remedial process be

72 ETHI, *Evidence*, 1 February 2024, Dufresne. If Bill C-27 is adopted, it will give the Privacy Commissioner the power to make orders under the new Consumer Privacy Protection Act, but not the power to impose administrative penalties.

73 Evan Light, *To the Standing Committee on Access to Information, Privacy and Ethics*, Reference document submitted to the Committee, 22 February 2024.

strong enough to discourage such behaviour.[74] Ms. Carr and Mr. Prier held similar views, recommending that there be clear repercussions for failing to abide by Treasury Board directives and clear actions to ensure that federal government institutions comply more in the future.

Mr. Prier outlined CAPE's three priorities to the Committee as follows:

> First, we're calling on the government to stop the use of spyware on federal devices outside of its own established rules, and to use the least invasive measures necessary. All public sector workers deserve due process during investigations.
>
> Second, we want to know when the government plans to conduct privacy impact assessments at all affected departments and to publicly release the results of these assessments to help public workers rebuild trust in their employer after these breaches. Spyware use represents an erosion of privacy rights that no public worker should accept on its face.
>
> Finally, we call on the government to conduct a thorough review of all its digital policies to ensure that the existing policy framework is adequately robust to protect employees' digital rights, including their right to reasonable privacy, their right to be informed about any digital surveillance tools being used in the workplace and their right to disconnect from work at the end of the day.

The Committee notes that the federal government institutions' representatives who appeared before the Committee insisted on the fact that their institution uses digital forensic tools and not spyware.

Ms. Carr, from PIPSC, recommended that the government provide clearer guidelines on what new or modified programs will require new PIAs and that current guidelines be updated. "Technology is moving at a fast pace, and our practices need to reflect that reality," she said.

Ms. Carr also called on the government to acknowledge that it does not own the personal data on devices used by employees and to improve privacy protections to keep pace as the technological tools used by federal government institutions become more powerful and invasive.

With regard to updating the applicable policies, the President of the Treasury Board, the Honourable Anita Anand, announced that the Treasury Board had made a commitment

74 PSAC, *Brief to the Standing Committee on Access to Information, Privacy and Ethics – For the study on – Federal Government's Use of Technological Tools Capable of Extracting Personal Data from Mobile Devices and Computers*, 3 March 2024, p. 1.

to update privacy policies and the *Directive on PIA*, which would include streamlining PIAs and looking for ways to improve the directive. She made the following statement:

> We've undertaken government-wide action, we've consulted with privacy experts on changes to the directive on privacy impact assessment and we are engaging with the Office of the Privacy Commissioner. We intend to publish the updated directive this summer.[75]

Dominic Rochon, Deputy Minister and Chief Information Officer of Canada at the Treasury Board Secretariat, said that the current wording of the *Directive on PIA* gave departments some leeway in deciding whether to update the PIAs if a new technological tool was used, leaving room for interpretation. He said that the updated directive would include components that specifically explain that the use of new technological tools requires updated PIAs.

Ms. Anand gave the following example of what could be clarified in the updated directive:

> We want to specify that if you change your software, for example, you're going to need a PIA going forward. You can't rely on previous PIAs once new software or new tools are being used. Those are the types of clarifications we want to make.

A Treasury Board of Canada Secretariat document sent to the Committee before Ms. Anand's appearance stated that the updated *Directive on PIA* will clarify the requirements for PIAs while expanding the directive's scope of application to a wider range of initiatives and that, broadly speaking, the updated directive will seek to streamline and standardize the assessment process among institutions to make it easier for institutions to submit PIAs.[76]

The document also states that the proposed changes to the *Directive on PIA* will support greater accountability and transparency, and that the expansion of PIA requirements to systems and software strengthens the current directive and will assist institutions in remaining compliant with sections 4 to 8 of the PA.[77]

---

75 At the time of adoption of this report on 24 September 2024, an updated *Directive on Privacy Impact Assessment* had not been published.

76 Treasury Board of Canada Secretariat, *Brief: Outlining the role of the President of the Treasury Board on the use of Tools Capable of Extracting Personal Data from Mobile Devices and Computers*, Reference document submitted to the Committee, p. 1 (TBS Reference Document).

77 TBS Reference Document, p. 2.

When asked about the possibility of adding an obligation to conduct PIAs in the PA, Ms. Anand gave the following response:

> I spoke with Minister Virani last night. I know he is examining the *Privacy Act* as a whole from a Minister of Justice standpoint. We are updating our own directive, which is solely within Treasury Board's authority. That is my realm, so I want to make sure that the checklist of items—the PIAs and the risk analysis that will be done by departments—will occur. Consultations are ongoing. We need to make sure we do this right. That is a systematic process, and I will come forward this summer with more to say on an updated directive.

Ms. Anand added that she was coordinating with the Minister of Justice and the Privacy Commissioner to ensure consistency with the review of the PA that is currently underway, and that she does not want to rush into making major changes to the *Directive on PIA* or the PA when the release date for the revised directive is just a few months away.

In her view, making it mandatory to conduct a PIA under the PA does not fall within her department's purview: it is a matter for the Minister of Justice. She said she would inform him of the possibility of including this component in the bill, and the necessary considerations regarding this issue.

The document submitted to the Committee by the Treasury Board of Canada Secretariat states the following:

> The Department of Justice is also currently leading a review of the *Privacy Act* with the goal of modernizing it to ensure it meets the requirements of the digital age and the privacy expectations of individuals. This review includes consideration to elevate the requirement of undertaking PIAs to legislation. Substantial policy development and engagement work has taken place in support of the Department of Justice initiative.[78]

No bill to substantively amend the PA has been introduced in Parliament since it came into force in 1983.

Conclusions and Recommendations

The Committee agrees with Mr. Dufresne's suggestion to reiterate the recommendations it made in its 2022 report on the use of ODITs by the RCMP, which called for amending the preamble of the PA to indicate that privacy is a fundamental right, adding the concept of privacy by design and including explicit transparency obligations for federal government institutions.

78 TBS Reference Document, p. 1.

In the document he sent to the Committee following his appearance, Mr. Dufresne—at the Committee's invitation—made a series of recommendations for legislative amendments and restated the recommendations he made during his appearance.[79] The Committee took his input into account when drafting the new recommendations in this report.

In light of the foregoing, the Committee reiterates the following recommendations made in its 2022 report on the use of on-device investigative tools used by the RCMP, which it believes are still relevant within the framework of the current study.[80]

Recommendation 2

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 3

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 4

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 5

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.

---

79 Privacy Commissioner of Canada, *Letter to the Committee*, 23 February 2024, pp. 1–2.

80 ETHI, *On-Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues*, Report, 44th Parliament, 1st Session, November 2022. Recommendations 2, 3, 4, 5 and 6 of the current report appeared as recommendations 1, 4, 6, 7 and 9, respectively, of the 2022 report.

Recommendation 6

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.

The Committee also makes the following new recommendations:

Recommendation 7

That the obligation for federal government institutions to conduct privacy impact assessments under the *Privacy Act*, as provided for in Recommendation 2, apply in particular when a federal government institution plans to use a powerful new technological tool that could have an impact on privacy.

Recommendation 8

That the Government of Canada amend the *Privacy Act* to require federal government institutions—before they launch an initiative, activity or program that could have an impact on privacy—to consult the Office of the Privacy Commissioner of Canada; to provide the relevant details about their initiative, activity or program to the Office within a set time frame; and to take into account the Office's opinion following this consultation.

Recommendation 9

That the Government of Canada amend the *Privacy Act* to include the concepts of necessity and proportionality by requiring federal government institutions to demonstrate that any activities and programs they pursue that could have an impact on privacy are necessary to achieve a pressing and substantial purpose and that the intrusion on privacy is proportional to the benefits to be gained.

Recommendation 10

That the Government of Canada update its *Directive on Privacy Impact Assessment* to ensure compliance.

Recommendation 11

That the Government of Canada impose an obligation on federal government institutions to consult with the Office of the Privacy Commissioner of Canada when dealing with privacy risk evaluations of their programs and tools.

Recommendation 12

That the Government of Canada impose an obligation on federal government institutions to perform regular reviews of existing privacy impact assessments.

Recommendation 13

That the Government of Canada impose an obligation on federal government institutions to continue to proactively remind employees of their obligations and to continue to keep employees up to date about device security.

Recommendation 14

That the Government of Canada review and implement stricter safeguards to limit any unnecessary access to any extracted data.

CONCLUSION

While the federal government institutions' representatives who appeared before the Committee said that privacy is important to their institution and that the use of digital forensic tools complies with the applicable rules and the authority granted to that institution by the applicable legislation, the Committee's study has shown that obligations under the *Directive on PIA* could be clearer, and compliance could be higher.

The President of the Treasury Board has already indicated that this directive is being updated. The Committee hopes that this update will strengthen the obligation for federal government institutions to conduct a PIA at the appropriate time.

Modernizing the PA could also include the addition of an obligation in the legislation to carry out PIAs. It could also clarify the need to consider the necessity and proportionality of collecting any personal information in order to limit the collection of data by federal government institutions to what is absolutely necessary to achieve their objectives.

The Committee believes that the recommendations, if implemented, would increase Canadians' trust in federal government institutions when it comes to the protection of their personal information.

APPENDIX A: USE OF DIGITAL FORENSIC TOOLS BY FEDERAL GOVERNMENT INSTITUTIONS THAT APPEARED BEFORE THE COMMITTEE

Table 1 gives some information about the use of digital forensic tools by the 12 federal government institutions that appeared before the Committee as part of this study: under which government program or in what context the tool is used; the relevant legislation under which they carry out investigations and can seize electronic devices; and the year in which the tool was purchased, if available.

Table 1—Key Facts About the Use of Digital Forensic Tools by 12 Federal Government Institutions

Federal Institution	Question	Answer
Canada Border Services Agency	Government program under which the tools are used or context of use	The Canada Border Services Agency is responsible for investigating allegations of violations of border legislation.
Canada Border Services Agency	Relevant legislation	The acts under which it can conduct investigations include the *Customs Act* and the *Immigration and Refugee Protection Act*.
Canada Border Services Agency	Year the digital forensic tool or tools were purchased	2019 (GrayKey, now known as Magnet Axiom) 2021 (Cellebrite Premium)
Canada Revenue Agency	Government program under which the tools are used or context of use	Canada Revenue Agency's Criminal Investigations Program.
Canada Revenue Agency	Relevant legislation	*Criminal Code* (ss. 2 and 487) and powers of search under the acts it is responsible for enforcing.

Federal Institution	Question	Answer
Canada Revenue Agency	Year the digital forensic tool or tools were purchased	2012
Canadian Radio-television and Telecommunications Commission	Government program under which the tools are used or context of use	CRTC's digital investigative tools program.
Canadian Radio-television and Telecommunications Commission	Relevant legislation	Canada's anti-spam legislation.
Canadian Radio-television and Telecommunications Commission	Year the digital forensic tool or tools were purchased	2014
Competition Bureau	Government program under which the tools are used or context of use	Competition Bureau's computer forensic program.
Competition Bureau	Relevant legislation	*Competition Act*
Competition Bureau	Year the digital forensic tool or tools were purchased	Not specified.
Correctional Service Canada	Government program under which the tools are used or context of use	Seizure of contraband items (contraband items in correctional institutions) pursuant to its enabling legislation.
Correctional Service Canada	Relevant legislation	*Corrections and Conditional Release Act*.
Correctional Service Canada	Year the digital forensic tool or tools were purchased	2010
Department of Fisheries and Oceans	Government program under which the tools are used or context of use	Fisheries and Oceans Canada's Conservation and Protection Program has a national digital forensics service and a cybersecurity digital forensic investigator service.

Federal Institution	Question	Answer
Department of Fisheries and Oceans	Relevant legislation	The acts under which it can conduct investigations include the *Fisheries Act* and the *Endangered Species Act*.
Department of Fisheries and Oceans	Year the digital forensic tool or tools were purchased	2013
Department of National Defence	Government program under which the tools are used or context of use	Departmental program on information and communication technology.
Department of National Defence	Relevant legislation	*Financial Administration Act*.
Department of National Defence	Year the digital forensic tool or tools were purchased	Not specified.
Environment and Climate Change Canada	Government program under which the tools are used or context of use	Digital forensics program of Environment and Climate Change Canada's Enforcement Branch.
Environment and Climate Change Canada	Relevant legislation	The acts under which it can conduct investigations include the *Canadian Environmental Protection Act*, provisions involving pollution prevention under the *Fisheries Act*, as well as the *Greenhouse Gas Pollution Pricing Act*.
Environment and Climate Change Canada	Year the digital forensic tool or tools were purchased	2013
Natural Resources Canada	Government program under which the tools are used or context of use	n/a
Natural Resources Canada	Relevant legislation	n/a

Federal Institution	Question	Answer
Natural Resources Canada	Year the digital forensic tool or tools were purchased	2018 (purchased but never used)
Royal Canadian Mounted Police	Government program under which the tools are used or context of use	Used as part of criminal investigations or internal administrative investigations.
Royal Canadian Mounted Police	Relevant legislation	*Criminal Code*.
Royal Canadian Mounted Police	Year the digital forensic tool or tools were purchased	Not specified.
Shared Services Canada	Government program under which the tools are used or context of use	Shared Services Canada's administrative investigations program.
Shared Services Canada	Relevant legislation	*Financial Administration Act*.
Shared Services Canada	Year the digital forensic tool or tools were purchased	Tools obtained by Shared Services Canada when it was established in 2011.
Transportation Safety Board of Canada	Government program under which the tools are used or context of use	Transportation Safety Board of Canada's investigation program.
Transportation Safety Board of Canada	Relevant legislation	*Canadian Transportation Accident Investigation and Safety Board Act*.
Transportation Safety Board of Canada	Year the digital forensic tool or tools were purchased	Not specified.

Source: House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Evidence*, 1 February 2024; (ETHI), *Evidence*, 6 February 2024; (ETHI), *Evidence*, 8 February 2024; (ETHI), *Evidence*, 13 February 2024; (ETHI); Shared Services Canada, Response to the Committee, 23 April 2024 [NO HYPERLINK AVAILABLE].

APPENDIX B: ACCESS BY OTHER FEDERAL INSTITUTIONS TO SOFTWARE USED TO EXTRACT INFORMATION FROM DIGITAL DEVICES

On 1 February 2024, the Committee adopted the following motion:

> That, in relation to the study on the use of tools capable of extracting personal data from telephones and computers by government institutions, the committee write to each federal department and agency not already named in the study and request that they confirm whether or not they have procured or have access to software used for extracting information off of electronic devices; and request that the response be sent to the committee no later than 10 business days after receipt.

The following table summarizes the responses received by the Committee from 54 federal institutions, some of which responded on behalf of a department and its agencies. Of these federal institutions, 17 responded in the affirmative when asked whether they have purchased or have access to software to extract information from electronic devices.

It is important to note that the software the institutions either purchased or reported having access to does not necessarily correspond to the specific digital forensic tools mentioned by the representatives of federal institutions who appeared before the Committee during the study, the most common being Cellebrite and Magnet Axiom/GrayKey.

Of the 17 institutions that said yes, only the Office of the Privacy Commissioner of Canada, the Courts Administration Service and Employment and Social Development Canada (ESDC) have purchased Magnet Axiom. ESDC indicated that it had purchased the software but had never used it. The Department of Justice and ESDC reported having purchased Cellebrite but, as with Magnet Axiom, ESDC reported that it had never used it. Other software that these institutions reported having access to included X-Ways, EnCase, FTK and RECON ITR.

Table 2—Access to a Digital Forensic Tool

Federal government Institution	Purchase or access to software used for extracting information off of electronic devices
Atlantic Canada Opportunities Agency (ACOA)	No
Bank of Canada	Yes
Canada Deposit Insurance Corporation (CDIC)	No
Canada Economic Development for Quebec Regions	No
Canadian Food Inspection Agency	No
Canadian Institutes of Health Research (CIHR)	Yes
Canadian Northern Economic Development Agency (CanNor)	No
Canadian Security Intelligence Service (CSIS)	Cannot respond
Agriculture and Agri-Food Canada	Yes
Farm Credit Canada	Yes
Canadian Dairy Commission	No
Canadian Grain Commission	No
Farm Products Council of Canada	No
Department of Canadian Heritage and its portfolio (except CRTC)	No
Immigration, Refugees and Citizenship Canada	Yes
Indigenous Services Canada	Yes

Federal government Institution	Purchase or access to software used for extracting information off of electronic devices
Canada Crown-Indigenous Relations and Northern Affairs Canada	Yes
Employment and Social Development Canada (ESDC)	Yes
Health Canada	Yes
Innovation, Science and Economic Development Canada (ISED) and its agencies	Yes
Department of Justice	Yes
Courts Administration Service	Yes
Office of the Information Commissioner of Canada	Yes
Office of the Privacy Commissioner of Canada	Yes
Military Grievances External Review Committee	No
Military Police Complaints Commission of Canada	No
National Defence and Canadian Armed Forces Ombudsman	No
Public Services and Procurement Canada (PSPC)	Yes
Transport Canada	No
Veterans Affairs Canada	Yes
Superintendent of Financial Institutions	No
Privy Council Office	No
Public Health Agency of Canada	Yes

Federal government Institution	Purchase or access to software used for extracting information off of electronic devices
Royal Canadian Mint	No
Treasury Board Secretariat	No
Canada School of Public Service	No
Communications Security Establishment (CSE)	Cannot respond
Federal Economic Development Agency for Southern Ontario	No
Federal Economic Development Agency for Northern Ontario	No
Department of Finance	No
Infrastructure Canada	No
Mortgage and Housing Corporation	No
Canada Infrastructure Bank	No
Windsor-Detroit Bridge Authority	No
Jacques Cartier and Champlain Bridges Incorporated	No
Public Prosecution Service of Canada	No
Agencies under Natural Resources Canada's portfolio	No
Prairies Economic Development Canada	No
Canada Development Investment Corporation	No
Women and Gender Equality Canada	No

Federal government Institution	Purchase or access to software used for extracting information off of electronic devices
Financial Consumer Agency of Canada	No
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	No
Parks Canada	No
Impact Assessment Agency of Canada	No

Source: Table prepared by the Library of Parliament using responses obtained by the House of Commons Standing Committee on Access to Information, Privacy and Ethics from various federal institutions and Shared Services Canada.

APPENDIX C:
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	2024/02/01	100
Lara Ives, Executive Director, Policy, Research and Parliamentary Affairs Directorate		
Offices of the Information and Privacy Commissioners of Canada	2024/02/01	100
Philippe Dufresne, Privacy Commissioner of Canada		
Canada Border Services Agency	2024/02/06	101
Aaron McCrorie, Vice-President, Intelligence and Enforcement		
Correctional Service of Canada	2024/02/06	101
France Gratton, Assistant Commissioner, Correctional Operations and Programs		
Tony Matson, Assistant Commissioner and Chief Financial Officer, Corporate Services		
Department of National Defence	2024/02/06	101
Sophie Martel, Acting Chief Information Officer		
Dave Yarker, Director General, Cyber and Command and Control Information Systems Operations		
Department of Natural Resources	2024/02/06	101
Francis Brisson, Assistant Deputy Minister and Chief Financial Officer		
Pierre Pelletier, Chief Information Officer		
Royal Canadian Mounted Police	2024/02/06	101
Nicolas Gagné, Superintendent		
Bryan Larkin, Deputy Commissioner, Specialized Policing Services		

Organizations and Individuals	Date	Meeting
Canada Revenue Agency	2024/02/08	102
Eric Ferron, Director General, Criminal Investigations Directorate, Compliance Programs Branch		
Anne Marie Laurin, Acting Director General and Deputy Chief Privacy Officer, Access to Information and Privacy Directorate, Public Affairs Branch		
Canadian Radio-television and Telecommunications Commission	2024/02/08	102
Steven Harroun, Chief Compliance and Enforcement Officer		
Anthony McIntyre, General Counsel and Deputy Executive Director, Legal Services		
Department of Fisheries and Oceans	2024/02/08	102
Brent Napier, Acting Director General, Conservation and Protection		
Sam Ryan, Director General, Integrated Technical Services		
Department of the Environment	2024/02/08	102
Hannah Rogers, Director General, Environmental Enforcement		
Donald Walker, Chief Enforcement Officer		
Competition Bureau Canada	2024/02/13	103
Pierre-Yves Guay, Deputy Commissioner, Cartels Directorate		
Mario Mainville, Chief Digital Officer		
Shared Services Canada	2024/02/13	103
Scott Jones, President		
Daniel Mills, Assistant Deputy Minister, Enterprise IT Procurement and Corporate Services Branch		
Transportation Safety Board of Canada	2024/02/13	103
Luc Casault, Director General, Corporate Services		
Kathy Fox, Chair		
As an individual	2024/02/15	104
Evan Light, Associate Professor		

Organizations and Individuals	Date	Meeting
Canadian Association of Professional Employees	2024/02/15	104
Nathan Prier, President		
Laura Shantz, Senior Advisor, Advocacy and Campaigns		
The Professional Institute of the Public Service of Canada	2024/02/15	104
Jennifer Carr, President		
Stéphanie Montreuil, Manager, Public Affairs		
Treasury Board Secretariat	2024/03/21	109
Hon. Anita Anand, President of the Treasury Board		
Dominic Rochon, Deputy Minister and Chief Information Officer of Canada		

APPENDIX D:
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.

Public Service Alliance of Canada

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. 100, 101, 102, 103, 104, 109 and 128) is tabled.

Respectfully submitted,

John Brassard
Chair