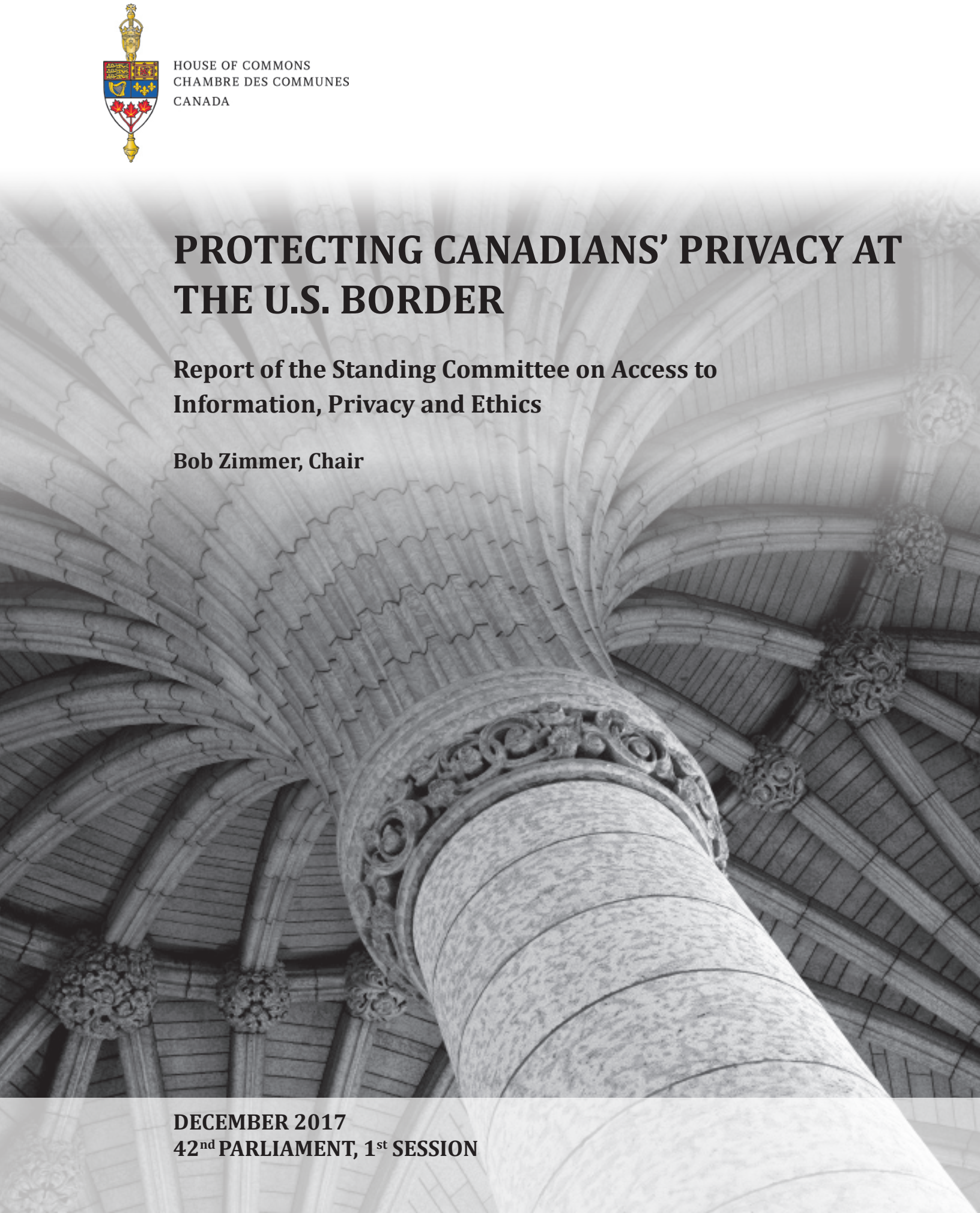

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# PROTECTING CANADIANS' PRIVACY AT THE U.S. BORDER

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

**Bob Zimmer, Chair**

**DECEMBER 2017**
**42nd PARLIAMENT, 1st SESSION**

# PROTECTING CANADIANS' PRIVACY AT THE U.S. BORDER

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

**Bob Zimmer**
**Chair**

**DECEMBER 2017**

**42nd PARLIAMENT, 1st SESSION**

## NOTICE TO READER

**Reports from committee 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**

Bob Zimmer

**VICE-CHAIRS**

Nathaniel Erskine-Smith

Nathan Cullen

**MEMBERS**

Frank Baylis

Emmanuel Dubourg

Mona Fortier

Jacques Gourde

Hon. Peter Kent

Joyce Murray*

Michel Picard

Raj Saini

**OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED**

Bill Blair

Hon. Steven Blaney

Sylvie Boucher

Blaine Calkins

Matthew Dubé

Ali Ehsassi

Peter Fragiskatos

Matt Jeneroux

Pat Kelly

Linda Lapointe

Wayne Long

Robert-Falcon Ouellette

Brenda Shanahan

Scott Simms

Karine Trudel

Erin Weir

* Non-voting member, pursuant to Standing Order 104(5).

**CLERK OF THE COMMITTEE**

Hugues La Rue

**LIBRARY OF PARLIAMENT**

**Parliamentary Information and Research Service**

Chloé Forget

Maxime-Olivier Thibodeau

Michael Dewing

# THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

**TENTH REPORT**

Pursuant to its mandate under Standing Order 108(3)(*h*)(vii), the Committee has studied the Privacy of Canadians at Airports, Borders and Travelling in the United States and has agreed to report the following:

# TABLE OF CONTENTS

# 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.*

# PROTECTING CANADIANS' PRIVACY AT THE U.S. BORDER

## INTRODUCTION

On 30 May 2017, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) concurred in the second report of the Subcommittee on Agenda and Procedure, which included the following recommendation: "That the Committee undertake a study of Canadians' privacy at airports and borders." The report specified "that this study include the privacy of Canadians travelling in the United States."[1]

The Committee held three meetings and heard from 15 witnesses. The Committee also received two briefs on the subject.

This report examines five main themes covered during the study:

1) Strengthening privacy protections by writing the guidelines of the Canada Border Services Agency (CBSA)'s policy on the examination of digital devices at the border into the Act;

2) The importance of tracking examinations of electronic devices at border crossings and compiling statistics in this regard;

3) The examination of electronic devices at the U.S. border and preclearance;

4) Recourses available to Canadians and the possibility that Canada be added to the countries listed in the U.S. *Judicial Redress Act;*

5) CBSA's oversight.

The report concludes each theme with recommendations by the Committee to the federal government.

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Minutes of Proceedings*, 1st Session, 42nd Parliament, 30 May 2017.

## PART 1: STRENGTHENING MEASURES TO PROTECT CANADIANS' PRIVACY BY WRITING THE GUIDELINES OF THE CANADA BORDER SERVICES AGENCY'S POLICY ON THE EXAMINATION OF DIGITAL DEVICES AT THE BORDER INTO THE ACT

The Government of Canada has an overarching duty to protect the border and ensure national security. When Canadians and other travellers cross borders or are in airports, they are subject to strict security oversight and monitoring. In Canada, the *Customs Act*[2] provides far-reaching search and examination powers to CBSA officers. This is due to the country's interest in protecting its borders by preventing unauthorized individuals and goods from entering the country.

In *R v. Simmons*, the Supreme Court of Canada ruled that there is a lower degree of personal privacy reasonably expected at customs. "People do not expect to be able to cross international borders free from scrutiny."[3] The Court recognized, moreover,

> that sovereign states have the right to control both who and what enters their boundaries. For the general welfare of the nation the state is expected to perform this role. Without the ability to establish that all persons who seek to cross its borders and their goods are legally entitled to enter the country, the state would be precluded from performing this crucially important function. Consequently, travellers seeking to cross national boundaries fully expect to be subject to a screening process. This process will typically require the production of proper identification and travel documentation and involve a search process beginning with completion of a declaration of all goods being brought into the country. Physical searches of luggage and of the person are accepted aspects of the search process where there are grounds for suspecting that a person has made a false declaration and is transporting prohibited goods.[4]

However, to maintain Canadians' confidence in the CBSA, it is equally important that measures be put in place to strike the right balance between protecting Canadians' privacy at the border and national security and border protection. While many witnesses

2 *Customs Act*, R.S.C. 1985, c. 1 (2nd Supp.).

3 *R. v. Simmons*, [1988] 2 SCR 495, para 52.

4 Ibid.

acknowledged the fact that there is a lower expectation of privacy at the border, it does not mean an absence of expectation of privacy.[5]

One of the key issues considered by the Committee is the examination of electronic devices at the border by CBSA officers. There is no doubt that electronic devices, such as telephones, tablets and computers, often contain a great deal of sensitive personal information, including correspondence, contacts, photos, travel history, financial information, health information, social media information, etc. In its brief, the Barreau du Québec illustrated this by citing a paragraph from the Supreme Court of Canada's ruling in *Fearon*:

> The devices which give us this freedom also generate immense stores of data about our movements and our lives. Ever-improving GPS technology even allows these devices to track the locations of their owners. Private digital devices record not only our core biographical information but our conversations, photos, browsing interests, purchase records, and leisure pursuits. Our digital footprint is often enough to reconstruct the events of our lives, our relationships with others, our likes and dislikes, our fears, hopes, opinions, beliefs and ideas. Our digital devices are windows to our inner private lives.[6]

The examination of electronic devices by CBSA officers therefore raises issues relating to protecting Canadians' privacy. Although the CBSA established a policy on the examination of electronic devices, several witnesses pointed out that this type of examination is a serious concern given the lack of clear rules in the *Customs Act*.

## A. CBSA policy on the examination of digital devices and media at the port of entry

CBSA developed an operational bulletin entitled *Examination of Digital Devices and Media at the Port of Entry – Guidelines* (see Appendix A).[7] The purpose of the bulletin is

---

5 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1535 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1720 (Mr. David Fraser, Executive Member, Privacy and Access Law Section, Canadian Bar Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1655 (Ms. Micheal Vonn, Policy Director, British Columbia Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1710 (Mr. David Fraser, Executive Member, Privacy and Access Law Section, Canadian Bar Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1710 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa, As an Individual); Barreau du Québec, Brief, *Privacy and Personal Information Protection at Border Crossings and Airports*, 18 October 2017.

6 Barreau du Québec, Brief, *Privacy and Personal Information Protection at Border Crossings and Airports*, 18 October 2017; *R. v. Fearon*, 2014 CSC 77, paras. 101–102.

7 Canada Border Services Agency, Operational Bulletin: PRG-2015-31, Examination of Digital Devices and Media at the Port of Entry – Guidelines, 30 June 2015.

to "provide guidance on a CBSA officer's authority to examine digital devices or media at ports of entry." It also provides clarification on "when such examinations should and can be performed, and will explain limitations to these authorities."

Under the policy, digital devices, digital media, digital documents and software are considered "goods" in the context of the border.[8] The term "goods" is defined in the *Customs Act* as follows: "for greater certainty, includes conveyances, animals and any document in any form."[9]

A CBSA officer's authority to search and examine goods is specified under the *Customs Act* and the *Immigration and Refugee Protection Act* (IRPA). Furthermore, according to CBSA's bulletin, paragraph 99(1)(a) of the *Customs Act* and subsection 139(1) of the IRPA authorize their examination under certain circumstances:

> Paragraph 99(1)(a) of the Customs Act provides CBSA officers with the legislative authority to examine goods, including digital devices and media, for customs purposes only. Although there is no defined threshold for grounds to examine such devices, CBSA's current policy is that such examinations should not be conducted as a matter of routine; they may only be conducted if there is a multiplicity of indicators that evidence of contraventions may be found on the digital device or media.
>
> Subsection 139(1) of the IRPA allows for the search of digital devices and media at the ports of entry where there are reasonable grounds to believe that the person has not revealed their identity or has hidden, on or about their person, documents that are relevant to their admissibility; or has committed or possesses documents that may be used in the commission of people smuggling, human trafficking, or document fraud. The purpose of this search must be confined to identifying the person, finding documents relevant to admissibility or that may be used in the specified offences, or finding evidence of the specified offences.
>
> Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods, plants and animals. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament. Officers must be able to explain their reasoning for examining the device, how each type of information, computer/device program and/or application they examine may reasonably be

8 Please note that the terms "digital devices", "digital media", "digital documents", and "software" are used interchangeably in this section of the report.

9 *Customs Act*, R.S.C. 1985, c. 1 (2nd Supp.), s. 2.

> expected to confirm or refute those concerns. The officer's notes shall clearly articulate the types of data examined, and their reason for doing so.[10]

The policy also states that, prior to examination of digital devices, CBSA officers must "disable wireless and Internet activity (i.e. set to airplane mode) to limit the ability of the device to connect to remote hosts or services."[11]

The policy also provides that, if a traveller refuses to provide the customs officer with the password to access an electronic device, the CBSA may detain the device under section 101 of the *Customs Act*.[12] However, the policy states that "CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist in the digital or media being examined."[13] CBSA officers must not request passwords giving access to various accounts such as social media accounts or files stored remotely or online.[14]

In his appearance before the Committee, Mr. Martin Bolduc, Vice-President, Programs Branch, CBSA, gave an overview of the guidelines applying to CBSA officers when examining digital devices, which are consistent with the principles set out in the policy.[15]

Mr. Bolduc said that "officers are instructed not to [examine goods] unless there are a number of indicators that a device may contain evidence of a contravention."[16] He also said that a "multiplicity of indicators that evidence of contraventions may be found on the digital device or media" in the policy means, for example, "your behaviour, the way you answer a question asked by the officer, the coding you have on your suitcase that doesn't match where you are coming from, or the fact that your ticket was purchased the day before."[17]

---

10 Canada Border Services Agency, Operational Bulletin: PRG-2015-31, Examination of Digital Devices and Media at the Port of Entry – Interim Guidelines, 30 June 2015.

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1540 (Mr. Martin Bolduc, Vice-President, Programs Branch, Canada Border Services Agency).

16 Ibid.

17 Ibid.

## B. Witnesses' views on the examination of digital devices at the Canadian border

During the Committee's study, several witnesses commented that the examination of electronic devices at the border is a serious concern given the lack of clear rules in the *Customs Act*. Technology has evolved considerably since the *Customs Act* was first enacted, and nowadays electronic devices contain very sensitive personal information. The law should therefore recognize this new reality and redress the balance between border protection, national security and the protection of Canadians' privacy.

Privacy Commissioner Daniel Therrien said that, under existing *Canadian Charter of Rights and Freedoms* jurisprudence, "greater latitude is given to state authorities at the border to enforce sovereignty and territorial integrity and to regulate immigration."[18] However, Commissioner Therrien also noted that the "Supreme Court has found in many other contexts that searching of electronic devices is extremely intrusive."[19] He believes that groundless searches of electronic devices would be unconstitutional.[20] Mr. David Fraser, of the Canadian Bar Association (CBA) shares this belief:

> The Customs Act provisions that are at issue were drafted before the 1980s, before laptops, before smart phones, and before thumb drives. In the meantime, the Supreme Court of Canada has said very strongly that all Canadians have an extremely acute privacy interest in the contents of computers, laptops, and smart phones. This has apparently fallen on deaf ears within the CBSA. People travel with a huge quantity of personal information, and the CBSA say that they can go through it legally on a whim. They say they don't, but the law, if applied as they say it is, would allow them to do it on a whim. We say this is likely unconstitutional and needs to be very closely examined by Parliament.[21]

In this regard, many witnesses argued that electronic devices should not be considered "goods" under the *Customs Act* and should therefore not be subject to groundless

18 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1555 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

19 Ibid.

20 Ibid.

21 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1635 (Mr. David Fraser, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

searches under this same act.[22] Commissioner Therrien argued that the "idea that electronic devices should be considered as mere goods and therefore be subject to border searches without legal grounds is clearly outdated and does not reflect the realities of modern technology."[23] Ms. Meghan McDermott, Policy Officer, British Columbia Civil Liberties Association (BCCLA) agrees. Similarly, Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association (CCLA), argued that electronic devices should not be included in a "legal and regulatory structure created at a time when both these devices and the quantity and quality of information they can contain was inconceivable."[24] She said it was long past time to "recognize the distinction between a bagful of underwear and a device that contains or provides access to our most intimate, personal conversations, our political musings and affiliations, our religious faith, our financial records, our commercial secrets, our health information, and many more types of information."[25]

Many witnesses argued that CBSA's policy diverges from the statute law on the search of goods under the *Customs Act* and creates specific rules on the search of electronic devices. The Privacy Commissioner argued that the CBSA's policy restricts this act such that electronic devices "can be searched only if the Canadian customs official has grounds to suspect something related to an offence."[26] The Commissioner added that, in his opinion, the CBSA's policy is not as permissive "as the law […] because the government and CBSA sense that the courts would not uphold the use of powers without grounds as the statute law allows."[27] Similarly, Ms. Meghan McDermott with BCCLA said that the CBSA's policy appears to "acknowledge that it is not appropriate to classify digital devices as 'mere goods'", stating that "searches may be conducted if there

22 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1555 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1535 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1550 (Ms. Meghan McDermott, Policy Officer, British Columbia Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1655 (Ms. Esha Bhandari, Staff Attorney, Speech, Privacy, and Technology Project, American Civil Liberties Union); ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1655 (Mr. David Fraser, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

23 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1555 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

24 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1535 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association).

25 Ibid.

26 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1635 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

27 Ibid.

are a 'multiplicity of indicators', that 'evidence of contraventions' may be found on the digital device."[28]

With a view to protecting Canadians' privacy, many witnesses made recommendations to make the guidelines in the CBSA's policy rules of law. As CBA's Mr. Fraser and BCCLA's Ms. Vonn argued, because the policy does not have the force of law, it cannot be enforced.[29] Commissioner Therrien recommended that the principle in the CBSA's policy under which "specific grounds need to be satisfied, namely that 'evidence of contraventions may be found on the digital device or media'[30] be made a rule of law. BCCLA representatives said their organization supported the Commissioner's recommendation and hoped that the Customs Act would be amended as a result.[31] Ms. Vonn suggested that, if the Commissioner's recommendation were retained, that the expression "multiplicity of indicators" in the policy be translated into a legal standard in the *Customs Act*.[32] As well, CBA recommended that the expression "multiplicity of indicators" in the CBSA's policy be replaced with reasonable grounds "to suspect that a crime – or it could be also a violation of the Customs Act – has been, is being, or is about to be committed, and that searching the device would provide evidence of that."[33] CCLA's Ms. McPhail also believes that there needs to be a clear legal framework on searches of electronic devices at the border that impose thresholds to "ensure that the search itself is reasonable, that it's conducted in a reasonable manner, and that it's otherwise charter-compliant, usually by requiring prior judicial authorization – a warrant – and adequate grounds on which to base the search."[34]

---

28 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1550 (Ms. Meghan McDermott, Policy Officer, British Columbia Civil Liberties Association).

29 Ibid., 1720 (Ms. Micheal Vonn, Policy Director, British Columbia Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1715 (Mr. David Fraser, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

30 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1555 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

31 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1550 (Ms. Meghan McDermott, Policy Officer, British Columbia Civil Liberties Association), ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1700 (Ms. Micheal Vonn, Policy Director, British Columbia Civil Liberties Association.

32 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1720 (Ms. Micheal Vonn, Policy Director, British Columbia Civil Liberties Association).

33 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1700 (Mr. David Fraser, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

34 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1535 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association).

The Committee believes that specific rules on electronic devices should be written into the *Customs Act*. The Committee argues that the *Customs Act* should be updated to recognize that electronic devices contain sensitive personal information and that electronic devices are not "goods" within the meaning of the *Customs Act*.
The Committee believes that electronic devices should not be examined without reasonable grounds and is encouraged that the CBSA's policy provides a threshold stating that examinations of electronic devices may only be conducted if there is a "multiplicity of indicators that evidence of contraventions may be found on the digital device or media." However, the Committee recognizes that the policy does not carry the same weight as if it were a law and supports witnesses' recommendations that CBSA's policy be given the force of law.

Therefore, the Committee recommends:

**Recommendation 1**

**That the guidelines in the operational bulletin of the Canada Border Services Agency entitled *Examination of Digital Devices and Media at the Port of Entry – Guidelines* be written into the *Customs Act*.**

**Recommendation 2**

**That the threshold of "multiplicity of indicators" required for the search of electronic devices set out in the operational bulletin of the Canada Border Services Agency entitled *Examination of Digital Devices and Media at the Port of Entry – Guidelines* be replaced with the threshold defined in law of "reasonable grounds to suspect."**

## PART 2: THE IMPORTANCE OF TRACKING EXAMINATIONS OF ELECTRONIC DEVICES AT BORDER CROSSINGS AND COMPILING STATISTICS IN THIS REGARD

During the appearance of CBSA officials, the Committee asked for how many years CBSA had been checking travellers' electronic devices.[35] CBSA officials were not able to provide clarity on the question, but said they would gather this information and provide it to the Committee.[36] In fact, Mr. Bolduc of CBSA specified that the *Customs Act* provides agents with the power to examine goods and that goods are "defined in section 2(1) of the act to include 'any document in any form,' which therefore encompasses

35 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1545.

36 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1545 (Mr. Martin Bolduc, Vice-President, Programs Branch, Canada Border Services Agency).

electronic documents."[37] Consequently, Mr. Bolduc explained that examinations of electronic devices were not tracked separately by CBSA from other examinations of goods.[38]

CBSA officials were also asked if they compiled statistics on the frequency of examinations of electronic devices at border crossings.[39] Mr. Bolduc of CBSA said that he had asked his team to find the mechanism to gather that information and that he had asked to be able to keep statistics rigorously in order to make the information public.[40] He provided the following explanation:

> The data I can provide is more anecdotal rather than rooted in the reality that our officers experience on a daily basis. However, the agency is committed to computing that data and making it public. I'm talking about the number of inspections of cellular or other electronic devices, and the types of devices that are checked.[41]

CBSA officials committed to provide the Committee with statistics on the number of searches of electronic devices over a six-month period, starting "a few weeks" before their appearance on 27 September 2017.[42]

On 30 October 2017, CBSA officials sent the Committee a response.[43] In this document, CBSA replied as follows:

> The CBSA has identified both a short-term and long-term solution to allow for the systematic tracking of examinations of electronic goods at the border.
>
> In the short term, officers are filling out an electronic form when an examination has been conducted. This approach will be in place until June 2018, when a permanent solution is scheduled to be implemented in the CBSA's information technology systems.[44]

---

37 Ibid., 1540.

38 Ibid., 1600.

39 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1545.

40 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1545 (Mr. Martin Bolduc, Vice-President, Programs Branch, Canada Border Services Agency).

41 Ibid.

42 Ibid., 1600.

43 Canada Border Services Agency. *Standing Committee on Access to Information, Privacy and Ethics (ETHI)*, 27 September 2017.

44 Ibid., p. 4.

The Committee noted that CBSA started compiling statistics on examinations of electronic devices at border crossings only a few weeks before its appearance. The Committee considers that a more rigorous tracking of examinations of electronic devices at border crossings and at airports – and the compilation of statistics on these examinations – is needed. In addition, the Committee believes that updates on this tracking should be regularly given to the Privacy Commissioner.

For these reasons, the Committee recommends:

**Recommendation 3**

**That the Government of Canada track the examination of electronic devices at border crossings and in airports, that statistics be compiled on these examinations and that updates be regularly given to the Privacy Commissioner of Canada in this regard.**

## PART 3: SEARCHES OF ELECTRONIC DEVICES BY U.S. CUSTOMS OFFICERS AND PRECLEARANCE

The United States as a sovereign state has jurisdiction to enact the rules it deems appropriate at its border.[45] As Ms. Esha Bhandari, Staff Attorney, Speech, Privacy, and Technology Project, with the American Civil Liberties Union (ACLU) explained, in the United States officers can currently search electronic devices at the border "without a warrant, probable cause, or any suspicion whatsoever."[46] However, Ms. Bhandari said that U.S. courts have not yet ruled on the matter and that the "ACLU's position is that border agents should not be able to search electronic devices without probable cause at a minimum."[47] Moreover, the Privacy Commissioner has advised Canadians "to limit the number of devices they bring to the U.S. and to review and limit the information that is found on the devices they're bringing with them to the United States."[48]

45 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1555 and 1605 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

46 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1555 (Ms. Esha Bhandari, Staff Attorney, Speech, Privacy, and Technology Project, American Civil Liberties Union).

47 Ibid.

48 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1615 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

Although concerns have been raised about the rules surrounding the search of electronic devices by U.S. customs officers, including privacy concerns, the United States can impose the rules it deems fit to protect its borders.[49]

However, many witnesses argued that the Government of Canada can take measures to protect Canadians' privacy during preclearance.[50] For example, witnesses mentioned Bill C-23, An Act respecting the preclearance of persons and goods in Canada and the United States (short title: Preclearance Act, 2016), which was introduced in June 2016.[51] The bill would implement the *Agreement on Land, Rail, Marine, and Air Transport Preclearance between the Government of Canada and the Government of the United States of America*, signed in Washington in March 2015.[52] Bill C-23 gives search powers to U.S. officers[53] conducting preclearance in Canada of travellers and goods bound for the United States.

Commissioner Therrien raised some concerns about the bill:

> Bill C-23 establishes that U.S. pre-clearance officers in Canada are subject to Canadian law as they perform their duties or exercise any powers. The Canadian government reminds us that this would include the Canadian Charter of Rights and Freedoms, the Canadian Bill of Rights, and the Canadian Human Rights Act. However, these protections

---

49 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1605 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada); ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1650 (Mr. Kris Klein, Partner, nNovation LLP, As an Individual); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1535 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1555 (Ms. Esha Bhandari, Staff Attorney, Speech, Privacy, and Technology Project, American Civil Liberties Union).

50 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1555 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1540 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1550 (Ms. Meghan McDermott, Policy Officer, British Columbia Civil Liberties Association); Canadian Bar Association, Brief, *Privacy of Canadians at Airports and Borders*, September 2017; Barreau du Québec, Brief, *Privacy and Personal Information Protection at Border Crossings and Airports*, 18 October 2017.

51 Bill C-23, An Act respecting the preclearance of persons and goods in Canada and the United States, 1st Session, 42nd Parliament.

52 *Agreement on Land, Rail, Marine, and Air Transport Preclearance between the Government of Canada and the Government of the United States of America* [Agreement on Land, Rail, Marine, and Air Transport Preclearance], Tabled in the House of Commons, Parliament of Canada, Sessional Paper 8532-412-50, 22 April 2015.

53 Bill C-23 defines "preclearance officer" as a person authorized by the Government of the United States to conduct preclearance in Canada.

> are somewhat hollow, as they would be severely limited by the principle of state immunity, meaning that they could not be enforced in a court of law.[54]

The Commissioner reiterated a recommendation made to the Standing Committee on Public Safety and National Security during its study on Bill C-23: preclearance border searches of electronic devices should require reasonable grounds to suspect an offence, a threshold similar to the one applying to searches of persons under Bill C-23.[55] Ms. McDermott of BCCLA supports the Commissioner's recommendation.[56] In the same vein, CBA expressed concerns about the consequences of Bill C-23 on privacy rights and freedoms.[57]

Specifically, CBA, Ms. McPhail of CCLA and Ms. McDermott of BCCLA raised concerns about the powers given U.S. officers to conduct a strip search under Bill C-23.[58] CBA and the Barreau du Québec also raised concerns about the requirement for travellers to answer questions from U.S. officers.[59]

The Committee wishes to make clear that its study did not deal in depth with Bill C-23. However, the Committee shares witnesses' concerns about searches of electronic devices, whether by CBSA officers or by US officers in preclearance areas. The Committee believes that the Government of Canada should ensure that its preclearance includes privacy protections and that the law recognizes the sensitive nature of personal information that may be found on electronic devices. Therefore, the Committee recommends:

---

54 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1555 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

55 Ibid.

56 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1550 (Ms. Meghan McDermott, Policy Officer, British Columbia Civil Liberties Association).

57 Canadian Bar Association, Brief, *Privacy of Canadians at Airports and Borders*, September 2017.

58 Ibid., ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1540 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1550 (Ms. Meghan McDermott, Policy Officer, British Columbia Civil Liberties Association).

59 Canadian Bar Association, Brief, *Privacy of Canadians at Airports and Borders*, September 2017; Barreau du Québec, Brief, *Privacy and Personal Information Protection at Border Crossings and Airports*, 18 October 2017.

**Recommendation 4**

**That the Government of Canada**

a) **ensure that the act respecting the preclearance of travellers in Canada include privacy protections;**

b) **that the act respecting the preclearance of travellers in Canada require the threshold of "reasonable grounds to suspect" for examinations of electronic devices by officers in preclearance areas.**

# PART 4: CANADA AND THE U.S. *JUDICIAL REDRESS ACT*

## A. Executive Order of 25 January 2017

On 25 January 2017, the President of the United States, Donald Trump, signed Executive Order 13768 that would, among other things, explicitly exclude individuals who are not United States citizens or permanent residents from privacy protections.[60] The order sets out the following measure, among others:

> Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.[61]

The U.S. *Privacy Act of 1974*[62] "provides statutory privacy rights to U.S. citizens and Lawful Permanent Residents."[63] It covers records held by U.S. federal agencies and:

> prohibits the disclosure of a record about an individual from a system of records[64] absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to

60 United States, The White House, Executive Order: Enhancing Public Safety in the Interior of the United States, 25 January 2017.

61 United States, The White House, Office of the Press Secretary, "Executive Order: Enhancing Public Safety in the Interior of the United States," News Release, 25 January 2017.

62 *Privacy Act of 1974*, 5 U.S.C. § 552a.

63 United States, U.S. Immigration and Customs Enforcement, Office of Information Governance and Privacy Frequently Asked Questions (FAQs).

64 A system of records is "a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual."

> seek access to and amendment of their records, and sets forth various agency record-keeping requirements.[65]

According to some authors, non-U.S. persons have a right of judicial review under the *Judicial Redress Act of 2015* as well as "the right to sue conferred by the *Privacy Act* to citizens of 'covered countries' designated by the Attorney General."[66] Under the provisions of the European Union-U.S. Privacy Shield,[67] on 17 January 2017 "the Attorney General designated 26 countries and the European Union as a whole."[68] Canada is not one of those designated countries.

According to the same authors, Presidential Policy Directive (PPD)-28, which was issued on 17 January 2014, also remains in effect. It "provides enhanced privacy protections to all persons regardless of nationality, in the context of U.S. signals intelligence activities."[69]

## B. Letter of 8 March 2017 from the Privacy Commissioner of Canada

On 8 March 2017, the Privacy Commissioner of Canada, Daniel Therrien, wrote to the ministers of Justice, Public Safety and Emergency Preparedness and National Defence regarding the implications of the executive order of 25 January 2017.[70] In his letter, Commissioner Therrien stated that Canadians have some privacy protection in the United States, but that "protection is fragile because it relies primarily on administrative agreements that do not have the force of law."[71]

Commissioner Therrien called on Canadian government officials to ask their U.S. counterparts to strengthen privacy protections for Canadians. He believes this could be done by adding Canada to the list of designated countries under the U.S. *Judicial Redress Act*. This would extend protections under the Act to Canadians, giving them the same level of protection as that granted to the citizens of various European countries.[72]

---

65 United States, Department of Justice, Privacy Act of 1974.

66 Adam Klein and Carrie Cordero, "The 'Interior Security' Executive Order, the Privacy Act, and Privacy Shield," *Lawfare*, 27 January 2017

67 European Commission, "EU-U.S. Privacy Shield: Frequently Asked Questions," *Fact Sheet*, 29 February 2016.

68 Ibid.

69 Ibid.

70 Office of the Privacy Commissioner of Canada, "Commissioner's letter to the ministers of Justice, Public Safety and Defence calling for greater protection of Canadians' privacy rights in the U.S.", 8 March 2017.

71 Ibid.

72 Ibid.

In his letter, Commissioner Therrien asks that the ministers provide his office with copies of the most significant information-sharing agreements between Canada and the United States and that they consult his office on their content so that he may ensure Canadians' personal information is being appropriately protected.[73]

Lastly, Commissioner Therrien asks the ministers to "remain vigilant in monitoring any changes to how information-sharing activities with the US are being operationalized, and that [they] advise [his] Office of any changes in the implementation of the agreements that would adversely impact the privacy of Canadians."[74]

### C. Response from the Canadian Government to the Privacy Commissioner of Canada's letter of 8 March 2017

On 10 November 2017, the Privacy Commissioner sent a letter to the Committee containing the response from the ministers of Justice, Public Safety and Emergency Preparedness and National Defence to his letter of 8 March 2017. In this response, the ministers inform Commissioner Therrien that U.S. authorities have provided them the following written assurances, among others:

- U.S. counterparts will continue to comply with the provisions of both legally binding agreements and non-legally binding arrangements that the U.S. has with Canada bilaterally and in the Five Eyes context. This includes provisions in those arrangements related to access, protection, rectification and redress regarding records containing personally identifiable information;

- the U.S.' longstanding commitment to the principle of protecting personally identifiable information and the related practices for limited use and handling such information remain unchanged;

- the redress rights of Canadians with respect to personal information shared by Canada with the U.S. have not changed because of the Executive Order;

- U.S. counterparts continue to follow other statutory and regulatory obligations, such as the U.S. Freedom of Information Act, which may also provide means of judicial redress concerning access, regardless of citizenship. Specific mechanisms for redress depend on the arrangement or agreement in question;

- with respect to the specific questions you raised in your letter regarding the Beyond the Border (BTB) Privacy Principles, DHS has reaffirmed the U.S. commitment to those principles, highlighting that they align with DHS Fair

73 Ibid.

74 Ibid.

Information Practices Principles (FIIPs) for the protection of personal information; and

- in response to the Executive Order, DHS updated its internal policy guidance on April 25, "Privacy Policy Guidance Memorandum 2017-01", on the collection, use, retention, and dissemination of personally identifiable information (https://www.dhs.gov./sites/default/files/publications/Privacy%20Policy%Guidance%20Memo%202017-01%20-%20FINAL.pdf). This update provides for explicit direction to DHS and its subcomponent organizations to handle personal information of all persons, regardless of immigration status, in a manner consistent with DHS Fair Information Practices Principles.

The ministers add in their response that for these reasons – and because they believe that the "the existing protections and redress mechanisms included in information sharing arrangements with other U.S. security and defence counterparts also remain unchanged" – they do not intend to pursue Canada's inclusion in the list of designated countries under the U.S. *Judicial Redress Act* at this time.

## D. Evidence

In his appearance before the Committee, Commissioner Therrien reiterated the recommendations in his letter of 8 March 2017.[75]

In their appearance before the Committee, representatives of the Canadian Civil Liberties Association[76] and the British Columbia Civil Liberties Association,[77] Mr. Michael Geist, a law professor at the University of Ottawa,[78] and Mr. Kris Klein, a partner at nNovation,[79] all made a similar recommendation to Commissioner Therrien's: to ask the U.S. government to add Canada to the list of countries covered by the U.S. *Judicial Redress Act*.

The representative from the American Civil Liberties Union (ACLU) shared her concerns about the executive order with the Committee. She said that, practically speaking, it is

75 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1600 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

76 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1535 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association).

77 Ibid., 1545 (Ms. Micheal Vonn, Policy Director, British Columbia Civil Liberties Association).

78 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1640 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa, As an Individual).

79 Ibid., 1650 (Mr. Kris Klein, Partner, nNovation LLP, As an Individual).

not clear what repercussions the order will have.[80] However, she said that a "large concern remains that non-U.S. persons' private information, sensitive information about immigration status, and health information may now be subject to public disclosure because the Privacy Act protections no longer exist."[81]

The Committee acknowledges the Canadian government's response to the letter of 8 March 2017 from the Privacy Commissioner in which the relevant ministers state their intention not to ask the United States to add Canada to the list of designated countries under the U.S. *Judicial Redress Act*. Notwithstanding this response, the Committee agrees with the recommendation made by the witnesses regarding the U.S. *Judicial Redress Act*. Therefore, the Committee recommends:

**Recommendation 5**

**That the Government of Canada ask the Government of the United States to add Canada to the list of designated countries under the U.S. *Judicial Redress Act*.**

**Recommendation 6**

**That the Government of Canada work with its American counterparts to monitor the application of existing information sharing agreements with the United States in order to ensure that Canadian personal information remains protected following the signing of Executive Order 13768 and inform the Privacy Commissioner of any changes.**

Additionally, the Privacy Commissioner raised "concerns over issues such as retention periods applicable to data collected from travellers and the risk that data collected for border purposes is then used for secondary purposes."[82] He recommended that the retention period for personal information be dependent on the reason for which the information is being collected, as well as the government's objectives.[83]

The Committee shares the Privacy Commissioner's concerns and recommends:

80 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1600 (Ms. Esha Bhandari, Staff Attorney, Speech, Privacy, and Technology Project, American Civil Liberties Union).

81 Ibid.

82 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 September 2017, 1600 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

83 Ibid., 1650.

**Recommendation 7**

**That the retention period for personal information be dependent on the Government's policy objectives in collecting the information.**

## PART 5: CANADA BORDER SERVICES AGENCY OVERSIGHT

Several witnesses argued that, regarding the CBSA, there is a need for transparency and for monitoring its activities. Indeed, several witnesses mentioned that the public's confidence in the CBSA depends on greater transparency related to the enforcement of the *Customs Act*, as well as on oversight mechanisms.

The CCLA recommended "greater public transparency and accountability in the way in which our current laws, including the *Customs Act* and the *Immigration and Refugee Protection Act*, are being interpreted at the border, especially as they pertain to privacy-invasive searches and questions."[84] Citizens should have access to the policies and procedures that are supposed to be followed for searches, as is the case in the United States, where policy documents regarding searches – including electronic searches – are available on the Internet.[85] The CCLA also mentioned the lack of independent oversight of the CBSA.[86]

Mr. Michael Geist, a law professor at the University of Ottawa, indicated that there is a need for transparency in terms of the standards applied by the CBSA. Indeed, according to him, Canadians' reasonable expectations of privacy at the border depend on "far better disclosure and clarity about what is permitted and what is not."[87]

In its brief, the CBA urged "the federal government to put effective CBSA oversight and complaints mechanisms in place to ensure that security is balanced with meaningful protection of privacy rights for Canadians at the border."[88] Consequently, the CBA recommended:

> that the federal government put effective CBSA oversight and complaints mechanisms in place to ensure that national security is balanced with meaningful protection of

84 ETHI, *Evidence*, 1st Session, 42nd Parliament, 15 June 2017, 1535 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance Project, Canadian Civil Liberties Association).

85 Ibid.

86 Ibid.

87 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1710 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa, As an Individual).

88 Canadian Bar Association, Brief, *Privacy of Canadians at Airports and Borders*, September 2017.

> privacy rights for Canadians at the border. According to the CBA, an agency other than the CBSA should be responsible for oversight pertaining to searches of electronic devices at the border and solicitor-client privilege.
>
> that the CBSA oversight model incorporate essential elements, including robust review at an agency level, effective cooperation between the national review bodies, and a higher-level review of the national security infrastructure as a whole.
>
> that the CBSA develop a transparent process for travellers to challenge the appropriateness of methodology for collecting information about them at the border. Improperly obtained information should be expunged from all government databases.[89]

Mr. Kris Klein, a partner at nNovation, also expressed concerns regarding the lack of CBSA oversight: "The problem with the Privacy Commissioner being the only body that really oversees CBSA right now is that under the *Privacy Act* there are a few shortfalls."[90] According to Mr. Klein, to ensure adequate oversight of CBSA activities, the Privacy Commissioner's powers should be increased, particularly so that they are not solely complaint-driven. Also, the standard for collecting personal information established by the *Privacy Act* should be strengthened such that federal institutions can only collect personal information if it is necessary for a program or activity.[91]

The Committee shares the witnesses' concerns and believes that the CBSA should be monitored to ensure that a balance is established between privacy protection and border protection. In that regard, the Committee believes that the oversight model established within the U.S. Department of Homeland Security (DHS) represents a relevant example to follow. Appendices B and C contain information on the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the DHS. For these reasons, the Committee recommends:

**Recommendation 8**

**That the Government of Canada consider establishing internal privacy and civil liberties officers within the Canada Border Services Agency to monitor privacy issues at the agency level.**

---

89 Ibid.

90 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2017, 1705 (Mr. Kris Klein, Partner, nNovation LLP, As an Individual).

91 Ibid.

# APPENDIX A: EXAMINATION OF DIGITAL DEVICES AND MEDIA AT THE PORT OF ENTRY – GUIDELINES


**OPERATIONAL BULLETIN: PRG-2015-31**

**TITLE : Examination of Digital Devices and Media at the Port of Entry – Guidelines**

| **Date of Issue:** | **Mode(s) :** | **Target Audience:** | **Area of Interest:** |
|---|---|---|---|
| 2015-06-30 | All | National | Port of Entry |

**Details:**

- The purpose of this operational bulletin is to provide guidance on a CBSA officer's authority to examine digital devices or media at ports of entry. Clarification will be provided on when such examinations should and can be performed, and will explain limitations to these authorities.

**Authorities:**

- Digital devices and media, along with digital documents and software, continue to be classified as 'goods' in the context of the border. A CBSA officer's authority to examine goods is specified under the *Customs* Act and the *Immigration and Refugee Protection* Act (IRPA).
- Paragraph 99(1)(*a*) of the *Customs* Act provides CBSA officers with the legislative authority to examine goods, including digital services and media, for customs purposes only. Although there is no defined threshold for grounds to examine such devices, CBSA's current policy is that such examinations should not be conducted as a matter of routine; they may only be conducted if there is a multiplicity of indicators that evidence of contraventions may be found on the digital device or media.

- Subsection 139(1) of the IRPA allows for the search of digital devices and media at the ports of entry where there are reasonable grounds to believe that the person has not revealed their identity or has hidden, on or about their person, documents that are relevant to their admissibility; or has committed, or possesses documents that may be used in the commission of people smuggling, human trafficking, or document fraud. The purpose of this search must be confined to identifying the person, finding documents relevant to admissibility or that may be used in the specified offences, or finding evidence of the specified offences.
- Examination of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods, plants and animals. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament. Officers must be able to explain their reasoning for examining the device, and how each type of information, computer/device program and/or application they examine may reasonably be expected to confirm or refute those concerns. The officer's notes shall clearly articulate the types of data they examined, and their reason for doing so.

**Actions required by CBSA officers:**

- Where there is a multiplicity of indicators, or further to the discovery of undeclared, prohibited, or falsely reported goods, officers are authorized to conduct progressive examinations of digital devices and media for evidence of contraventions or to support allegations.
- Evidence may include, for example, electronic receipts for goods; information that refers to the acquisition or origin of the goods; or information that may afford evidence of a contravention to CBSA-mandated legislation that governs the admissibility of people and goods, plants and animals into and out of Canada. Such evidence may, for example, uncover the following: a confirmation of identity; receipts and invoices for imported goods; contraband smuggling; or, the importation of obscenity, hate propaganda or child pornography.
- Where the identity or admissibility of a traveller is in question, officers are justified in performing examinations of digital devices and media to discover the traveller's true identity, evidence of false identities, or other documentary evidence pertaining to admissibility.
- Where evidence of a criminal offence is discovered during the examination process, officers must be cognisant of where the regulatory examination crosses over to the realm of a criminal investigation. Officers must determine on a case-by-case basis, through consultation with their supervisor, whether or not to continue the regulatory examination and

identify any possible impacts on potential criminal investigations.

- Officers must follow the CBSA Enforcement Manual, Part 9. Instructions on securing evidence and on referrals to Criminal Investigations, as well as following regional requirements for referrals to Inland Enforcement or Intelligence.
- CBSA officers shall conduct examination of digital devices and media with as much respect for the traveller's privacy as possible, considering that these examinations are usually more personal in nature than baggage examinations.

*Examination Progression*

- Prior to examination of digital devices and media, and where possible, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) to limit the ability of the device to connect to remote hosts or services. This will reduce the possibility of triggering remote wiping software; inadvertently accessing the Internet or other data stored externally; or changing version numbers or dates.
- Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators.
- CBSA officers shall only examine what is stored within the device. Officers not to read emails on digital devices and media unless the information is already downloaded and has been opened (usually marked as read).
- CBSA officers shall notate in their notebooks the indicators that led to the progressive search of the digital device or media; what areas of the device or media were accessed during the search; and why. This is to protect both the integrity of the information within the digital device and the officer.

*Passwords and Enforcement*

- With the exception of devices that are biometrically (i.e. fingerprint) protected, CBSA officers shall not allow a traveller to input a password into digital device or media themselves. This practice reduces the risk of any contents being altered and allows for the continuity of evidence.
- In instances where access to digital devices and media are password protected, officers are to request the password to access the device and record it, as well as any alternate passwords provided, in their officer notebook.
- In cases where the device is biometrically protected, CBSA officers may allow the traveller to input the biometric information while the officer monitors and controls the device (for example, the officer may hold the device while the traveller allows the device to read their fingerprint).

Should the CBSA officer find information that provides evidence of a contravention, they should then deactivate the password protection on the device or media.

- Passwords are not to be sought to gain access to any type of account (including any social, professional, corporate, or user accounts), files or information that might potentially be stored remotely or on-line. CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist within the digital device or media being examined.

**Contact Information:**

Program Compliance and Outreach Division, Traveller Programs Directorate

If you have any further questions, please forward them through the regional Corporate and Program Services Divisions, which (if required) will then send an email to the Port of Entry Operations' generic inbox: CBSA-ASFC_Ops_Travellers-Voyageurs.

**Approved by :** Barry Kong, Director
Programs Compliance and Outreach Division
Traveller Programs Directorate
Programs Branch

| | |
|---|---|
| **Effective Date:** 2015-06-30 | **Updated:** 2017-02-28 |

Autres bulletins : http://atlas/ob-dgo/bso-asf/bulletin/index_eng.asp

# APPENDIX B: CHIEF PRIVACY OFFICER (DEPARTMENT OF HOMELAND SECURITY OF THE UNITED STATES)

## Authorities and Responsibilities of the Chief Privacy Officer

The activities of the Privacy Office serve to build privacy into departmental programs. The following is a framework of privacy laws through which the Privacy Office accomplishes its activities and mission:

- Privacy Act of 1974, as amended (5 U.S.C. § 552a): Embodies a code of fair information principles that governs the collection, maintenance, use, and dissemination of personally identifiable information by federal agencies;
- E-government Act of 2002 (Public Law 107-347): Mandates Privacy Impact Assessments (PIAs) for all Federal agencies when there are new collections of, or new technologies applied to, personally identifiable information;
- Freedom of Information Act of 1966, as amended (5 U.S.C § 552): Implements the principles that persons have a fundamental right to know what their government is doing;
- Homeland Security Act of 2002, as amended (6 U.S.C. 552): Creates the Chief Privacy Officer at DHS with responsibilities to ensure privacy and transparency in government are implemented throughout the Department; and
- Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53): Amends the Homeland Security Act to give new authorities to the Chief Privacy Officer.

The responsibilities of the Chief Privacy Officer, as set forth in Section 222 of the Homeland Security Act of 2002, as amended:

### SEC. 222. [6 U.S.C. 142] PRIVACY OFFICER.

**(a) APPOINTMENT AND RESPONSIBILITIES.—**The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports on such programs, policies, and procedures; and

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.

**(b) AUTHORITY TO INVESTIGATE.—**

(1) IN GENERAL.—The senior official appointed under subsection (a) may—

(A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;

(B) make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable;

(C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the responsibilities of the senior official under this section; and

(D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section.

(2) ENFORCEMENT OF SUBPOENAS.—Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.

(3) EFFECT OF OATHS.—Any oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an employee of the Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.

**(c) SUPERVISION AND COORDINATION.—**

(1) IN GENERAL.—The senior official appointed under subsection (a) shall—

(A) report to, and be under the general supervision of, the Secretary; and

(B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.

(2) COORDINATION WITH THE INSPECTOR GENERAL.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.

(B) COORDINATION.—

(i) REFERRAL.—Before initiating any investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.

(ii) DETERMINATIONS AND NOTIFICATIONS BY THE INSPECTOR GENERAL.—

(I) IN GENERAL.—Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—

(aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and

(bb) notify the senior official of that determination.

(II) INVESTIGATION NOT INITIATED.—If the Inspector General notifies the senior official under subclause (I)(bb) that the Inspector General intended to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this subclause shall be made not later than 3 days after the end of that 90-day period.

(iii) INVESTIGATION BY SENIOR OFFICIAL.—The senior official may investigate a matter referred under clause (i) if—

(I) the Inspector General notifies the senior official under clause (ii)(I)(bb) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or

(II) the Inspector General provides a further notification under clause (ii)(II) relating to that matter.

(iv) PRIVACY TRAINING.—Any employee of the Office of Inspector General who audits or investigates any matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).

**(d) NOTIFICATION TO CONGRESS ON REMOVAL.—** If the Secretary removes the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department, the Secretary shall—

(1) promptly submit a written notification of the removal or transfer to Houses of Congress; and

(2) include in any such notification the reasons for the removal or transfer.

(e) REPORTS BY SENIOR OFFICIAL TO CONGRESS.—The senior official appointed under subsection (a) shall—

(1) submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget; and

(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—

(A) 30 days after the Secretary disapproves the senior official's request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or

(B) 45 days after the senior official's request for a subpoena under subsection (b)(1)(C), if that subpoena has not either been approved or disapproved by the Secretary.

Last Published Date: March 29, 2017

# APPENDIX C:
# OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES (DEPARTMENT OF HOMELAND SECURITY OF THE UNITED STATES)

Homeland Security

## Office for Civil Rights and Civil Liberties

*The Office for Civil Rights and Civil Liberties (CRCL) supports the Department of Homeland Security (DHS) as it secures the Nation while preserving individual liberty, fairness, and equality under the law.*

CRCL integrates civil rights and civil liberties considerations into all of the Department's activities by:

- Advising Department leadership and personnel and consulting with federal partners;
- Providing training, technical assistance, and best practices to state and local partners;
- Communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities;
- Investigating civil rights and civil liberties complaints regarding Department policies, programs, activities, or actions and issuing formal policy, practice, and training recommendations; and
- Leading the Department's equal employment opportunity (EEO) programs and promoting workforce diversity and merit system principles.

CRCL was created by the **Homeland Security Act of 2002** (6 U.S.C. § 345) and came into existence with the rest of the Department in 2003. It is housed within the Office of the Secretary and Executive Management.[1] The **Officer for Civil Rights and Civil Liberties** is an assistant secretary-level, non-Senate confirmed Presidential appointee who reports directly to the Secretary. The Officer is supported by two career SES deputies: the Deputy Officer for Programs and Compliance and the Deputy Officer for Equal Employment and Diversity, who is also the Department's Equal Employment Opportunity (EEO) Director.[2]

The **Equal Employment Opportunity and Diversity Division** leads the Department's efforts to ensure that all employees and applicants receive equal employment opportunity. The Division directs EEO complaints management and adjudication, diversity management, and alternative dispute resolution, and processes employment discrimination and harassment claims brought against DHS Headquarters units.

The **Programs Branch** works with DHS Components and leadership to ensure that policies, programs, and practices are created and implemented in a manner that protects civil rights and civil liberties. This work includes providing policy formulation and implementation advice, training, program review, and engagement with DHS stakeholders. The Programs Branch operates through its five sections in the following ways:

- **Community Engagement:** CRCL performs critical outreach for DHS with the public, by convening routine stakeholder roundtable meetings for DHS in cities across the country, distinct town halls on current issues, and subject-specific events focusing on DHS priorities—some 100 events per year. CRCL also convenes national incident community coordination team (ICCT) calls with stakeholders and relevant government leadership in the immediate aftermath of homeland security incidents.
- **Department-Wide Policy Development and Implementation:** CRCL leads the Department's policy development and implementation for the protection of civil rights and civil liberties. Projects include: immigration detention policy review; big data projects; information sharing processes and agreements, particularly in support of counterterrorism, cybersecurity, vetting, and screening activities; social media; and, the implementation of the Prison Rape Elimination Act. CRCL also plays an important role in safeguarding DHS' requirement to provide equal access for persons with disabilities; ensuring language access for limited English proficient individuals, and applying the privacy provisions of the Violence Against Women Act. Further, CRCL plays a critical leadership role on the DHS Council on Combatting Violence Against Women and serves as the Department's lead in implementing human rights treaties.

1 List of authorities available upon request.
2 Organization chart available upon request.

- **Intelligence Review:** CRCL reviews over 1000 substantial Department intelligence products each year for civil rights and civil liberties impacts and ensures that intelligence-based targeting activities are appropriately based on current intelligence and comport with individual rights and liberties.
- **Civil Rights Compliance by DHS and Recipients of DHS Financial Assistance:** CRCL has responsibility to assure nondiscrimination in the Department's federally conducted and assisted programs in accordance with federal nondiscrimination laws prohibiting discrimination based on race, color, national origin, disability, sex, age, or religion in DHS programs and activities.

The **Compliance Branch** investigates complaints from the public, media reports, and other sources, alleging civil rights or civil liberties violations by Department personnel or programs, including disability discrimination prohibited by the Rehabilitation Act of 1973, inappropriate use of force by DHS officers or agents, inadequate conditions of detention, violation of right to due process, and racial or ethnic profiling. In 2016, CRCL received over 2000 allegations, resulting in over 500 complaint investigations. CRCL makes formal recommendations stemming from its investigations to DHS Component leadership to rectify gaps in civil rights or liberties protections related to DHS policies, practices, and training. CRCL does not order individual relief or redress for a complainant except for disability accommodation claims under the Rehabilitation Act of 1973.

*Visit CRCL at www.dhs.gov/crcl, or contact us at crcl@hq.dhs.gov.*

*Follow CRCL on Facebook at: www.facebook.com/CivilRightsAndCivilLiberties*

# APPENDIX D
# LIST OF WITNESSES

| Organizations and Individuals | Date | Meeting |
|---|---|---|
| **American Civil Liberties Union**<br>Esha Bhandari, Staff Attorney<br>Speech, Privacy, and Technology Project | 2017/06/15 | 65 |
| **British Columbia Civil Liberties Association**<br>Micheal Vonn, Policy Director<br>Meghan McDermott, Policy Officer | | |
| **Canadian Civil Liberties Association**<br>Brenda McPhail, Director Privacy,<br>Technology and Surveillance Project | | |
| **Office of the Privacy Commissioner of Canada**<br>Daniel Therrien, Privacy Commissioner of Canada<br>Lara Ives, Acting Director<br>General Audit and Review<br>Patricia Kosseim, Senior General Counsel and Director General<br>Legal Services, Policy, Research and Technology Analysis Branch | 2017/09/18 | 66 |
| **As an individual**<br>Michael Geist, Canada Research Chair in Internet and<br>E-commerce Law<br>Faculty of Law, University of Ottawa<br>Kris Klein, Partner<br>nNovation LLP | 2017/09/27 | 69 |
| **Canada Border Services Agency**<br>Martin Bolduc, Vice-President<br>Programs Branch<br>Robert Mundie, Acting Vice-President<br>Corporate Affairs Branch | | |

| Organizations and Individuals | Date | Meeting |
|---|---|---|
| **Canadian Air Transport Security Authority**<br>John Stroud, Vice-President<br>Corporate Services and Corporate Secretary<br>Natalie Sabourin, Manager<br>Information Management, Privacy and ATIP | 2017/09/27 | 69 |
| **Canadian Bar Association**<br>David Fraser, Executive Member<br>Privacy and Access Law Section<br>Cyndee Todgham Cherniak, Member-at-Large, Commodity Tax, Customs and Trade | | |

# APPENDIX E
# LIST OF BRIEFS

## Organizations and Individuals

**Barreau du Québec**

**Canadian Bar Association**

# 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. 65, 66, 69, 70, 78 and 81) is tabled.

Respectfully submitted,

Bob Zimmer
Chair