HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

PROTECTING THE PRIVACY OF CANADIANS: REVIEW OF THE *PRIVACY ACT*

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

Blaine Calkins
Chair

DECEMBER 2016

42nd PARLIAMENT, 1st SESSION

PROTECTING THE PRIVACY OF CANADIANS: REVIEW OF THE *PRIVACY ACT*

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

Blaine Calkins
Chair

DECEMBER 2016

42nd PARLIAMENT, 1st SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

BLAINE CALKINS

VICE-CHAIRS

DANIEL BLAIKIE
JOËL LIGHTBOUND

MEMBERS

BOB BRATINA
NATHANIEL ERSKINE-SMITH
MATT JENEROUX
PAT KELLY
WAYNE LONG
RÉMI MASSÉ
RAJ SANI

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

WILLIAM AMOS
MEL ARNOLD
RENÉ ARSENEAULT
KERRY DIOTTE
MATTHEW DUBÉ
PIERRE-LUC DUSSEAULT
JULIE DZEROWICZ
MICHAEL V. MCLEOD
MARC MILLER
PIERRE PAUL-HUS
MICHEL PICARD
HON. MICHELLE REMPEL
FRANCIS SCARPALEGGIA
MARK STRAHL
DAVID TILSON

CLERKS OF THE COMMITTEE

Hugues La Rue
Michel Marcotte

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Michael Dewing
Chloé Forget
Maxime-Olivier Thibodeau

THE STANDING COMMITTEE ON ACCES TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

FOURTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*h*)(vi), the Committee has studied the *Privacy Act* and has agreed to report the following:

TABLE OF CONTENTS

PROTECTING THE PRIVACY OF CANADIANS: REVIEW OF THE *PRIVACY ACT*

CHAPTER 1: INTRODUCTION

1.1 Mandate

On 23 February 2016, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "Committee") agreed: "That, pursuant to Standing Order 108 (3)(*h*)(vi) the Committee undertake a study on the *Privacy Act*."[1]

The Committee began its study on 10 March 2016. It held 12 meetings during which it heard from 45 witnesses. The witnesses included ministers, the Privacy Commissioner of Canada, provincial information and privacy commissioners, public officials and privacy experts from legal firms, academia and advocacy groups. The Committee also received five briefs.

The Committee wishes to thank all those who participated in this study.

1.2 Review of the *Privacy Act*

The *Privacy Act*[2] (the "Act"), which took effect on 1 July 1983, "is the law that governs the personal information handling practices of federal government institutions. The Act applies to all of the personal information the federal government collects, uses and discloses – be it about individuals or federal employees. The Act also gives individuals the right to access and request correction of personal information held by these federal government institutions."[3]

Section 75 of the Act provides for permanent parliamentary review of the Act, as well as a one-time review to begin in 1986.[4] Accordingly, the Standing Committee of Justice and Solicitor General conducted a review and in 1987 tabled a report entitled *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. In 2008-2009, the Standing Committee on Access to Information, Privacy and Ethics conducted a study of the Act and tabled a report entitled *The* Privacy Act*: First Steps Towards Renewal*.[5] Neither of these studies resulted in any legislative amendments.[6]

---

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Minutes of Proceedings*, 42nd Parliament, 1st Session, 23 February 2016.

2 *Privacy Act*, R.S.C., 1985 (*Privacy Act*), c. P-21.

3 Office of the Privacy Commissioner of Canada, *The* Privacy Act.

4 *Privacy Act*, s. 75.

5 ETHI, *The* Privacy Act: *First Steps Towards Renewal*, June 2009.

6 Office of the Privacy Commissioner of Canada, Privacy Act *Reform in an Era of Change and Transparency*, 22 March 2016.

On 22 March 2016, the Privacy Commissioner of Canada, Daniel Therrien, sent a letter to the Committee in which he made 16 recommendations for amendments to the Act.[7] On 16 September, he submitted further input on the role of the Office of the Privacy Commissioner of Canada (OPC) and order-making provisions.[8] On 1 November, he submitted revised recommendations (see Appendix A).[9] These recommendations, which he grouped under the themes of technological changes, legislative modernization and enhanced transparency, form the basis of this study.

A number of witnesses were in general agreement with all of the Commissioner's recommendations, albeit with some comments and suggestions for improvement. These witnesses included:

- Teresa Scassa, professor at the University of Ottawa and Canada Research Chair in Information Law;[10]
- David Lyon, professor at Queen's University in Kingston, Ontario;[11]
- Tamir Israel, staff lawyer at the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC);[12, 13]
- Brenda McPhail, Director, Privacy, Technology and Surveillance at the Canadian Civil Liberties Association (CCLA);[14]
- Colin Bennett, professor with the Department of Political Science at the University of Victoria in British Columbia;[15]
- Michael Geist, Canada Research Chair in Internet and E-commerce Law and professor of law at the University of Ottawa;[16]

---

7 Ibid.

8 Office of the Privacy Commissioner of Canada, "Letter to the Standing Committee on Access to Information, Privacy and Ethics about the study of the Privacy Act*," 13 September 2016.*

9 Office of the Privacy Commissioner of Canada, "Review of the Privacy Act - Revised recommendations," 1 November 2016.

10 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0855 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, as an individual).

11 Ibid., 0905 (Mr. David Lyon, Professor, Queen's University, as an individual).

12 Based at the Centre for Law, Technology & Society at the Faculty of Law of the University of Ottawa.

13 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1135 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

14 Ibid., 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

15 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1100 (Professor Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual)

16 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1100 (Dr. Michael Geist Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, as an individual).

- David Fraser, a partner with the Halifax, Nova Scotia law firm of McInnes Cooper;[17]

- Catherine Tully, Information and Privacy Commissioner for Nova Scotia;[18]

- Donovan Molloy, Information and Privacy Commissioner of Newfoundland and Labrador;[19]

- Chantal Bernier, Counsel, Privacy and Cybersecurity with the law firm Dentons Canada and former Interim Privacy Commissioner of Canada;[20] and

- Michael Karanicolas, senior legal officer with the Centre for Law and Democracy (CLD).[21]

Gary Dickson of the Canadian Bar Association's (CBA) Privacy and Access Law Section[22] and Michel Drapeau, professor in the Faculty of Common Law at the University of Ottawa[23] agreed with most of the recommendations but had disagreements or questions about others.

1.3 The need for reform

In his initial appearance on this study, Commissioner Therrien said there was a "very crucial need to overhaul the *Privacy Act*,"[24] which he described as "antiquated." Noting that technology has not stood still, he said: "in the digital world, it is infinitely easier to collect, store, analyze, and share huge amounts of personal information, making it far more challenging to safeguard all of that data and raising new risks for privacy."[25]

In his final submission, Commissioner Therrien spelled out some of the risks of not modernizing the Act:

> In the public sector, these consequences include, first, risks of data breaches that are not properly mitigated; second, excessive collection and sharing of personal information,

---

17 Ibid., 1100 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

18 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1105 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

19 Ibid., 1105 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

20 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1100 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

21 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1100 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

22 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1120 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

23 Ibid., 1100 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Common Law, As an Individual).

24 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

25 Ibid.

> which may affect trust in government; and more specifically, third, a reduced trust in online systems that may undermine the government's efforts to modernize its services and coordinate its digital communications with Canadians.
>
> Some governments have already moved forward to strengthen their privacy protection frameworks, most notably the European Union. There is a risk, in my view, that if European authorities no longer find Canada's privacy laws essentially equivalent to those protecting EU nationals, commerce between Canada and Europe may become more difficult.[26]

Witnesses generally agreed with the need for reform. Mr. Lyon pointed out that the Act "is premised on some rather fixed ideas about personal information in terms of who collects it and where, if at all, it travels. Today, fluidity rather than fixity is the order of the day."[27] Mr. Bennett made similar points, and said, "The lack of reform has also meant that a good deal of the content of the regulation is contained in an accumulation of Treasury Board Secretariat guidance that can sometimes be ignored or selectively interpreted."[28]

Mr. Israel of the CIPPIC described some of today's challenges:

> The era of data-driven decision-making, colloquially referred to as 'big data', increasingly pushes state agencies to cast wide nets in their data collection efforts. Additionally, more often than not, the Act is applied in review of activities motivated by law enforcement and security considerations that are far removed from the administrative activities that animated its initial introduction.[29]

He went on to say, "[T]he general task here is to amend the law in such a way that the basic privacy principles remain intact, which embraces the more contemporary ideas about how to protect personal data in a networked environment in which personal data can be shared instantaneously and easily between and within organizations."[30]

In the same vein, Drew McArthur, Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia, said that this was a good time to bring the Act "into alignment with the other activities that are going on around the country and internationally."[31] Likewise, Vincent Gogolek, executive director of the B.C. Freedom of Information and Privacy Association (BC FIPA), said that the reform of the Act should be done to bring it, "into closer harmony with not just the more modern and more protective

---

26 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1105 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

27 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0905 (Mr. David Lyon, Professor, Queen's University, as an individual).

28 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1100 (Professor Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual)

29 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1135 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

30 Ibid.

31 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1215 (Mr. Drew McArthur, Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia).

privacy laws, but also with its federal private sector equivalent, PIPEDA [the *Personal Information Protection and Electronic Documents Act*]."[32]

CHAPTER 2: TECHNOLOGICAL CHANGES

2.1 Purpose clause and definition of personal information

2.1.1 Purpose clause

To keep the *Privacy Act* relevant in the face of ever-changing technology, several witnesses suggested that the purpose clause in section 2 of the Act be amended to spell out technologically neutral privacy principles. Section 2 currently reads:

> The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.[33]

Mr. Israel of the CIPPIC said the purpose clause,

> should be updated to explicitly recognize the objectives of the Act: to protect the right to privacy of individuals, and to enhance transparency and accountability in the state's use of personal information. Express recognition of these purposes, as is done in provincial counterparts to the *Privacy Act*, will assist in properly orienting the legislation around its important quasi-constitutional objectives, and will help to secure its proper and effective application if ambiguities arise in the future, as they surely will.[34]

He went on to say it is important that the principles of necessity and proportionality be explicitly recognized in the Act.[35] Ms. McPhail of the CCLA agreed with him about the need for the Act to be grounded in principles[36] and also said that it "needs to encompass contemporary and future uses of personal information."[37] Along these lines, Mr. Gogolek of BC FIPA stressed "the importance for legislators of writing laws at a relatively high level, keeping them principle-based and technology-neutral."[38] Mr. Karanicolas of the CLD agreed,[39] as did Michael Peirce, Assistant Director Intelligence at the Canadian Security Intelligence Service (CSIS).[40]

---

32 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1110 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

33 *Privacy Act*, s. 2.

34 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1135 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

35 Ibid.

36 Ibid., 1200 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

37 Ibid., 1105.

38 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1130 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

39 Ibid., 1130 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

40 Ibid., 1230 (Mr. Michael Peirce, Assistant Director Intelligence, Canadian Security Intelligence Service).

Ms. Tully, Information and Privacy Commissioner for Nova Scotia, said that having a detailed purpose clause in Nova Scotia's *Freedom of Information and Protection of Privacy Act* had "served the courts well in their interpretation of the Act."[41] She suggested adding such a clause to the *Privacy Act*.[42]

Several witnesses said an expanded purpose clause could be based on the approach used in PIPEDA. For example, Mr. Fraser said:

> PIPEDA is a real model of how you can come up with a privacy statute that's based on principles, bedrock principles that I think most Canadians can get on board with. That's the skeleton on which you put the meat, but you want to make sure that it will in fact stand the test of time.[43]

Mr. Geist also suggested looking at PIPEDA as an example of an approach that is based on international privacy principles. [44]

Some witnesses had specific suggestions for principles that could be included in an amended purpose clause. Lisa Austin, associate professor at the University of Toronto Faculty of Law, recommended:

> that the *Privacy Act* should include a reference to privacy rights protected by the *Canadian Charter of Rights and Freedoms*. Put a reference to it in the purpose section to allow for arguments to be made in reference to the *Charter of Rights and Freedoms*.[45]

Ken Rubin, an investigative researcher and advocate, agreed with this position.[46]

More specifically, Ms. Scassa said that a reformed *Privacy Act* should include the principle of data minimization,[47] in other words, "a reduction of the amount of information that is collected in the first place."[48]

The Committee agreed with the idea of including technologically neutral privacy principles in the purpose clause of the Act and therefore recommends:

---

41 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1105 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

42 Ibid., 1230.

43 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1150 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

44 Ibid., 1125 (Dr. Michael Geist Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, as an individual).

45 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0915 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, as an individual).

46 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1125 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

47 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0855 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, as an individual).

48 Ibid., 0950.

RECOMMENDATION 1

a) That the purpose clause in section 2 of the *Privacy Act* be expanded to reinforce the quasi-constitutional nature of privacy rights by including generally accepted and technologically neutral privacy principles similar to those in contained in the *Personal Information Protection and Electronic Documents Act*, including accountability; identifying purposes; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

b) That the *Privacy Act* be modified to clarify that the privacy principles in the amended purpose clause shall guide the interpretation of the Act.

2.1.2 The definition of "personal information"

Section 3 of the *Privacy Act* defines "personal information" as "information about an identifiable individual that is recorded in any form"[49] and goes on to provide a non-exclusive list of kinds of information.

Commissioner Therrien warned that any changes to the definition of "personal information" would have to be considered carefully, saying:

> the *Access to Information Act* and the *Privacy Act* are to be seen as seamless codes, and changes to one act must consider the impact on the other. Changes to the way in which access and privacy rights are balanced under the current legislation should be carefully thought through, including any changes to the definition of personal information, and changes to the *Access to Information Act*'s public interest override.
>
> In my view, these changes should be considered in the second phase of *Access to Information Act* reform.[50]

Several witnesses suggested changing the definition of "personal information" to remove the reference to recorded information. To quote Mr. Gogolek of BC FIPA, "[I]n 2008 the Commissioner made a recommendation to eliminate the stipulation that the Act apply only to recorded information. We think that was a good idea in 2008, and we still think it's a good idea."[51]

Other witnesses agreed with this position. Mr. Rubin recommended "that unrecorded information such as personal biological samples, including DNA and iris

---

49 *Privacy Act*, s. 3.

50 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1100 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

51 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1115 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

scans, be covered." [52] Mr. Fraser also suggested removing "the requirement that personal information be recorded in order to be subject to the statute."[53] Mr. Israel of the CIPPIC made the same point, saying, "The current definition only applies to personal information that is recorded, whereas many modern data collection and use practices never actively record any personal information, but can still have a very salient privacy impact."[54] He recommended updating the definition of "personal information" so that it aligns with the comparable definition under PIPEDA.[55] This definition states: "that 'personal information' means information about an identifiable individual."[56]

The Committee agrees that the *Privacy Act* needs to apply to all personal information and therefore recommends:

RECOMMENDATION 2

That the definition of "personal information" in section 3 of the *Privacy Act* be amended to ensure that it be technologically neutral and that it include unrecorded information.

2.1.3 The definition of metadata

Several witnesses talked about the challenges posed by metadata, which the Office of the Communications Security Establishment Commissioner describes as:

> [T]he context, but not the content, of a communication. Metadata is information associated with a communication that is used to identify, describe, manage or route that communication. It includes, but is not limited to, a telephone number, an e-mail or an Internet Protocol address, and network and location information.[57]

In his testimony, the President of the Treasury Board, the Honorable Scott Brison, said that metadata meets the definition of personal information in the Act.[58]

As pointed out by Mr. Lyon, there is a debate over whether or not metadata is personal information. He said that while it is "sometimes dismissed misleadingly as phone book-like information rather than content," it "is frequently more revealing, not less."[59]

---

52 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1130 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

53 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1100 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

54 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1135 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

55 Ibid., 1145.

56 Office of the Privacy Commissioner of Canada, "Personal Information," October 2013.

57 Office of the Communications Security Establishment Commissioner, *2015-2016 Annual Report*.

58 ETHI, *Evidence*, 1st Session, 42nd Parliament, 24 November 2016, 1155 (Hon. Scott Brison, President of the Treasury Board).

59 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0910 (Mr. David Lyon, Professor, Queen's University, as an individual).

Mr. Geist said the value of metadata is huge and it is "essential that we address it as equivalent to some of the most sensitive privacy information that we potentially have both in our *Privacy Act* and in other legislative instruments where that same data is touched on." [60] In a similar vein, Mr. Fraser said: "The *Privacy Act* is well placed to consider metadata as a concept. The definition of personal information in the statute, if it's fixed in order to deal with the recorded or not recorded thing, is information about an individual."[61]

Mr. Karanicolas of the CLD said that metadata has a high privacy value and needs to be protected, but pointed out there are risks to defining it in the Act: "Metadata means one thing today; it could well mean a totally different thing in five or 10 years."[62] Mr. Gogolek of BC FIPA also mentioned the concern about being too specific in the legislation.[63] Mr. Israel of CIPPIC suggested a way of addressing this issue:

> Maybe something that would refer to regulation, that would allow for a rolling definition that gets adopted through regulation, might be the best way to address that particular problem and make sure that this type of data is kept within the scope of the protections in the *Privacy Act*.[64]

Ms. McPhail of the CCLA said that while the details could be dealt with in regulations, she would still like to see metadata included in "a general purpose statement as part of the kinds of information covered."[65]

In discussing metadata, some witnesses referred to the recent 2014 Supreme Court of Canada decision known as *R. v. Spencer*.[66] This case, "concluded subscriber information linked with specific Internet activity should not be obtained without a warrant, except in very precise circumstances."[67] In his initial appearance, Commissioner Therrien said:

> The *Spencer* decision of the Supreme Court in 2014 helped a lot in regulating what law enforcement can do with metadata in the context of investigations. (…) Clearly, I would not be in favour of reducing the protection that comes from the Spencer decision, and if anything, if there was legislation to adopt on that point, my recommendation would be to codify and confirm the principles of *Spencer*. Would it be a good thing to define

---

60 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1120 (Dr. Michael Geist Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, as an individual).

61 Ibid., 1120 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

62 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1225 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

63 Ibid., 1230 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association):

64 Ibid., 1215 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

65 Ibid. (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

66 *R. v. Spencer*, 2014 SCC 43.

67 Office of the Privacy Commissioner of Canada, "Op-ed: Federal Privacy Commissioner urges caution should Parliament revisit warrantless access," 25 January 2016.

> metadata? I'm less certain of that, but to confirm the principles of *Spencer* would be useful.[68]

In her testimony, Ms. Bernier said that in the *Spencer* decision, "what the court says – and this is very important – is that personal information is not what it is, it's what it reveals. It's a dynamic notion."[69] Mr. Gogolek of BC FIPA also referred to the *Spencer* decision, saying it "provided a very good guideline to us in terms of the importance of metadata and in terms of it being personal information that is protected."[70]

In his final appearance on this study, Commissioner Therrien said:

> I'm looking for some framework, some statutory provisions that would set out certain principles, according to Parliament, according to our elected officials, as to when government institutions would be able to collect metadata, when they would be able to share metadata, under what principles or under what conditions generally speaking, and under what conditions they should retain that information. I'm not looking for something very prescriptive; I'm looking for some basic rules.[71]

He went on to say:

> Should metadata be defined in the *Privacy Act*? That would be helpful.
>
> Is it in the *Privacy Act*? We know that the collection, use and sharing of metadata is not authorized under general privacy legislation alone. We would have to find a way to ensure that the definition and the rules surrounding collection, use and sharing – which is the crux of the matter – apply in all cases where such information is used.[72]

The Committee feels there is the need for greater clarity regarding the definition of metadata and therefore recommends:

RECOMMENDATION 3

That the Government of Canada define metadata in the *Privacy Act*, in a technologically neutral way and with an emphasis on the information it can reveal about an individual.

2.2 Information-sharing agreements

The Privacy Commissioner recommends that information sharing under paragraphs 8(2)(a) and (f) of the *Privacy Act* be governed by written agreements (see Recommendation 1 in Appendix A). These paragraphs state:

---

68 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 1005 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

69 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1130 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

70 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1230 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

71 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1145 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

72 Ibid., 1215.

> Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
>
> > (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;
> >
> > (f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the council of the Westbank First Nation, the council of a participating First Nation – as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act –, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;[73]

In his initial appearance before the Committee on this study, Commissioner Therrien said:

> Technological change has allowed government information sharing to increase exponentially. Existing legal rules are not sufficient to regulate this kind of massive data sharing. We would therefore recommend that the *Privacy Act* be amended to require that all information sharing be governed by written agreements and that these agreements include specified elements.[74]

In its brief to the Committee, the Privacy and Access Law Section of the CBA supported this recommendation.[75] Mr. Bennett also agreed,[76] as did Ms. Bernier, who said,

> I believe the requirement for written agreements to better govern this sharing is needed for two major reasons: the protection of fundamental rights, and the accountability of government agencies in protecting these fundamental rights. The Commissioner's recommendation is therefore very relevant, and even urgent, in this regard.[77]

Ms. Scassa also agreed with the recommendation, which she said

> would also offer a measure of transparency to a public that has a right to know whether, and in what circumstances, information they provide to one agency or department will be shared with another, or whether and under what conditions their personal information may be shared with provincial or foreign governments.[78]

---

73 *Privacy Act*, ss. 8(2)(a) and (f).

74 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

75 Canadian Bar Association, Privacy and Access Law Section, Privacy Act *Amendments*, September 2016, p. 6.

76 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1105 (Professor Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

77 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1100 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

78 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0900 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, as an individual).

Mr. Karanicolas supported the information-sharing recommendation and went further to suggest "that these agreements should be public and should set clear limits as to the purposes for which the disclosures may be made. There should also be a system of disclosure when these conditions are violated and effective remedies for those individuals who are affected."[79] In its brief, BC FIPA agreed with the recommendation on information-sharing agreements and said "they should be publicly posted on the government of Canada website."[80]

Ms. Austin also commented on the recommendation, saying, "[T]he written agreements are a start. Again, I would want Charter compliance built into them, because some of this information sharing can raise Charter issues, and these need to be flagged early on."[81]

Officials from federal institutions who appeared before the Committee raised concerns about requiring written information-sharing agreements. Assistant Commissioner Joe Oliver of the Royal Canadian Mounted Police (RCMP) said,

> It would be very challenging to negotiate an agreement with everybody we share with. That's why we have strict policies that dictate how we share and with whom we share. There's a need to know and there's a right to know. Plus, we assess the relevancy of any request, the reliability of the information we are sharing, and the accuracy of that information before we share it. Then it's shared with the caveat that for any further dissemination, you would have to come back to the originator in order to share onward.[82]

Mr. Peirce of CSIS had other concerns, saying that,

> it would be difficult for CSIS to publicize its relationships with all of the security intelligence agencies around the world with whom we work. That would disclose relationships that are closely guarded by some of our partners at times, relationships that may prove problematic to our ability to gather national security information from them about threats to the security of Canada.[83]

Stefanie Beck, Assistant Deputy Minister for Corporate Services for Immigration, Refugees and Citizenship Canada (IRCC) said, "[I]t's always easier if we have legislative authority to do it without having to negotiate a whole separate agreement…."[84] Dan Proulx, Director of the Access to Information and Privacy Division of the Canada Border Services Agency (CBSA), raised the following point:

---

79 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1100 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

80 BC Freedom of Information and Privacy Association, *Reform of the* Privacy Act:*Past Time for Action*, 20 October 2016, p. 4.

81 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0925 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, as an individual).

82 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1200 (Assistant Commissioner Joe Oliver, Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police).

83 Ibid., 1200 (Mr. Michael Peirce, Assistant Director Intelligence, Canadian Security Intelligence Service).

84 Ibid., 1155 (Ms. Stefanie Beck, Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration).

> [T]he *Privacy Act* is subject to other acts of Parliament that already have governing disclosure provisions, so in terms of consistent use, to have a written agreement for every single one would be very problematic.
>
> Apart from that, when it's not a consistent use, we would agree, and support, that you need a governing framework, an authority, written and signed, to share that information.[85]

On the subject of agreement-sharing agreements with other countries, during his final appearance, Commissioner Therrien said,

> It would be too cumbersome to have agreements on a transactional basis. That's not what we're recommending, but we are recommending that there be umbrella agreements that provide more specificity than the act itself on what type of information in a given context will be shared and for what purpose the information will be shared.[86]

He went on to say that the OPC

> would intervene before the transaction occurs, at the policy level, at the PIA [privacy impact assessment] level. At the transactional level … there's nothing in our recommendations that would require them to consult us on a case-by-case basis. It would occur before the fact, at the policy level, at the content of the agreement level. Then the department would implement the agreement.

The Committee agrees with the Commissioner's recommendation on information-sharing agreements and therefore recommends:

RECOMMENDATION 4

That the *Privacy Act* be amended to require that all information sharing under paragraphs 8(2)(a) and (f) of the *Privacy Act* be governed by written agreements and that these agreements include specified elements.

RECOMMENDATION 5

That the *Privacy Act* be amended to create an explicit requirement that new or amended information-sharing agreements be submitted to the Office of the Privacy Commissioner of Canada for review, and that existing agreements should be reviewable by the Privacy Commissioner upon request.

RECOMMENDATION 6

a) That the *Privacy Act* be amended to create an explicit requirement that departments be transparent about the existence of any information-sharing agreements.

---

85 Ibid., 1200 (Mr. Dan Proulx, Director, Access to Information and Privacy Division, Canada Border Services Agency).

86 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1110 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

b) That the *Privacy Act* be amended to require, except in appropriate circumstances, the publication of the content of information-sharing agreements between departments or with other governments.

2.3 Safeguarding personal information

The Privacy Commissioner recommends creating a legal obligation for government institutions to safeguard personal information (see Recommendation 2 in Appendix A). In his initial appearance before the Committee, Commissioner Therrien said, "In the digital world, it is infinitely easier to collect, store, analyze, and share huge amounts of personal information, making it far more challenging to safeguard all of that data and raising new risks for privacy."[87] Regarding the safeguarding of information, he noted that "[c]urrently, that is the subject of government policy, not legal obligations per se."[88]

In a brief submitted to the Committee, BC FIPA said,

> We agree with the Commissioner that administrative direction from the Treasury Board Secretariat (TBS) is not sufficient, and that the *Privacy Act* should be brought in line with other legislation (including the BC's FIPPA [*Freedom of Information and Protection of Privacy Act*] and PIPEDA) by expressly including this requirement. There should not be a lower standard of protection in the public sector than the standard the federal government has imposed on the private sector through PIPEDA.[89]

In its brief, the Privacy and Access Law Section of the CBA also agreed with the need for including safeguards in the legislation, pointing out that while the TBS and other government institutions have created policies on safeguarding information "[t]hose efforts have been inadequate to signal to public servants and the public the serious risk of loss, theft or misuse of personal information in digital form."[90] The brief also noted, "A feature common to many other Canadian privacy laws, both public sector and private sector, is to require the organization to create reasonable safeguards to protect personal information including administrative, technical and physical safeguards."[91]

Mr. Israel of the CIPPIC[92] and Ms. McPhail of the CCLA[93] both endorsed the idea of creating a legal obligation to safeguard personal information. In her testimony,

---

87 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

88 Ibid., 0945.

89 BC Freedom of Information and Privacy Association, *Reform of the* Privacy Act:*Past Time for Action*, 20 October 2016, pp. 4-5.

90 Canadian Bar Association, Privacy and Access Law Section, Privacy Act *Amendments*, September 2016, p. 7.

91 Ibid.

92 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1145 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

93 Ibid., 1110 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

Ms. Austin pointed out that, "there are serious Charter issues in not safeguarding that information properly that the courts are starting to really pay attention to."[94]

Some witnesses discussed the need for sanctions when there are violations of the Act. Mr. Fraser said, "Many more modern privacy laws … have an offence provision that if an individual or even an institution, unlawfully and usually with knowledge, is in violation of the statute, they can be charged under that."[95] Mr. Gogolek of BC FIPA said, "There should be a broader scope and a broader availability of sanctions, including damages, under the *Privacy Act*."[96]

One of the safeguarding measures that was suggested is to require that data be stored in Canada. This is referred to as domestic data storage or data localization. Mr. Gogolek testified,

> in British Columbia our public sector act has a domestic data storage requirement, something that does not exist at the federal level. Again, this requirement was recently supported by the committee reviewing our Act earlier this year, and also by the Government of British Columbia. We would commend this to you as something you may want to look at….[97]

Other witnesses had reservations about this approach. In referring to the concerns about storing information in the United States, which has a different approach to the privacy of information, Ms. Austin said,

> Data localization is one response to that dynamic. I think it's an unrealistic response to think that this is a solution in the long term. Another response … is to negotiate a bilateral agreement with allies like the U.S. to say that when Canadian data is in the United States, you protect us to the same extent that you protect your own citizens.[98]

Mr. Fraser said that the location of data is only one of many factors to be considered. He said there needs to be "nuanced risk analysis" and referred to the TBS policy,

> which is, if any government department is going to make any decision about the location of data in connection with outsourcing … location is going to be a factor, but there are other things as well. Who is going to be the service provider? Who are they beholden to? What national ties do they have?[99]

---

94 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0940 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, as an individual).

95 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1100 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

96 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1115 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

97 Ibid.

98 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0945 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, as an individual).

99 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1200 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

Similarly, Assistant Commissioner Oliver of the RCMP also called for a risk-based approach to safeguarding information:

> I say that because some of the security control measures. If they were consistently applied, and if the measures that are put in place by my colleagues at CSIS were then applied to other government information, the costs would be huge. We need to take a measured approach for risk-based safeguards, based on the type of information being held and based on the threats that exit against that information. Then we must put in place measured security controls that will be cost-effective, but also meet the objective of protecting the information.[100]

Other government officials described the measures for safeguarding information that are already in place.[101]

The Committee agrees with the Commissioner's recommendation on creating a legal obligation for government institutions to safeguard personal information and therefore recommends:

RECOMMENDATION 7

That the *Privacy Act* be amended to create an explicit requirement for institutions to safeguard personal information with appropriate physical, organizational and technological measures commensurate with the level of sensitivity of the data.

RECOMMANDATION 8

That the *Privacy Act* be amended to set out clear consequences for failing to safeguard personal information.

2.4 Reporting breaches of personal information

The Privacy Commissioner recommends requiring government institutions to report material privacy breaches to the OPC and, where appropriate, to notify affected individuals (see Recommendation 3 in Appendix A). In his initial appearance, Commissioner Therrien said,

> The fact that government departments collect and use ever-greater amounts of personal information has also increased the stakes when it comes to privacy breaches. Over the years, we have seen massive government breaches affecting tens, even hundreds, of thousands of citizens.

---

100 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1235 (Assistant Commissioner Joe Oliver, Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police).

101 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1220 (Mrs. Marie-Claude Juneau, Director, Access to Information and Privacy, Canada Revenue Agency) and ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1140-1145 (Mr. Robert Mundie, Director General, Corporate Secretariat, and Mr. Dan Proulx, Director, Access to Information and Privacy Division, Canada Border Services Agency; Mr. Michael Peirce, Assistant Director Intelligence, Canadian Security Intelligence Service; Ms. Stefanie Beck, Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration).

> We recommend creating an explicit requirement for institutions to safeguard personal information under their control as well as a legal requirement to report breaches to my office.[102]

While witnesses were generally supportive of this recommendation, some had comments about it. For example, Ms. Scassa said:

> Parliament has recently amended PIPEDA to include such a requirement. Once these provisions take effect, the private sector will be held to a higher standard than the public sector unless the *Privacy Act* is also amended.
>
> Any amendments to the federal *Privacy Act* to address data security breach reporting would have to take into account the need for the commissioner and for affected individuals to be notified when there has been a breach that meets a certain threshold for potential harm, as will be the case under PIPEDA.
>
> The PIPEDA amendments will also require organizations to keep records of all breaches of security safeguards, regardless of whether they meet the harm threshold that triggers a formal reporting requirement. Parliament should impose a requirement on those bodies governed by the *Privacy Act* to keep and to submit records of this kind to the OPC. Such records would be helpful in identifying patterns or trends….[103]

Other witnesses also called for the *Privacy Act* to include similar notification obligations as will be included in PIPEDA, including Ms. McPhail of the CCLA,[104] Mr. Israel of the CIPPIC,[105] the Privacy and Access Law Section of the CBA,[106] Mr. Fraser,[107] Mr. McArthur[108] and Ms. Bernier.[109]

Mr. Bennett noted that, as well as being included in PIPEDA, "[m]andatory privacy data breach notification is now a feature of modern data protection law."[110] He went on to say that it is crucial

> to combine the stick of mandatory data breach reporting with a carrot that says that if you've taken proper technical measures and safeguards to protect that data through

---

102 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

103 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0900 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, as an individual).

104 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1110 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

105 Ibid., 1230 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

106 Canadian Bar Association, Privacy and Access Law Section, Privacy Act *Amendments*, September 2016, p. 7.

107 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1105 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

108 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1135 (Mr. Drew McArthur, Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia).

109 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1200 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

110 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1100 (Professor Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

> encryption, then it's not that you get out of jail free, but you just have to do less in terms of reporting.[111]

Some witnesses pointed out that there can be risks in notifying individuals. Mr. Molloy, the Information and Privacy Commissioner of Newfoundland and Labrador, noted that

> we've experienced situations where the unnecessary notification of individuals that their privacy has been breached can cause a lot of damage, as well. Once you've been notified it's hard to put the genie back in the bottle. People have a hard job being convinced that the breach didn't have any impact on them.[112]

In his final appearance, Commissioner Therrien responded to a question about ensuring that reporting a breach does not compound the damages to an affected party by saying,

> [Y]ou're right in that creating this obligation, whether by policy or by law, may create the risk for further increases in damages. We were consulted by the innovation department [Innovation, Science and Economic Development Canada] on the same policy in the private sector, and we actually made certain comments there on how to mitigate that risk. I recognize there is a risk, but it's possible to mitigate that risk.[113]

Most of the government officials who testified said they did not expect that a requirement to report material privacy breaches would be problematic.[114]

While the Committee has concerns about the damage that breach reporting could cause affected individuals, it agrees with the Commissioner's recommendation on reporting material breaches and therefore recommends:

RECOMMENDATION 9

That the *Privacy Act* be amended to create an explicit requirement for government institutions to report material breaches of personal information to the Office of the Privacy Commissioner of Canada in a timely manner.

RECOMMENDATION 10

That the *Privacy Act* be amended to create an explicit requirement for government institutions to notify affected individuals of material breaches of personal information, except in appropriate cases,

---

111 Ibid.

112 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1135 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

113 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1155 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

114 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1225 (Mr. Dan Proulx, Director, Access to Information and Privacy Division, Canada Border Services Agency; Mr. Michael Peirce, Assistant Director Intelligence, Canadian Security Intelligence Service; Ms. Stefanie Beck, Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration).

provided that the notification does not compound the damage to the individuals.

CHAPTER 3: LEGISLATIVE MODERNIZATION

3.1 Criteria for the collection, disclosure, use and retention of personal information

3.1.1 The Privacy Commissioner's recommendation

Commissioner Therrien recommended establishing "an explicit necessity requirement for collection," by amending "section 4 of the *Privacy Act* to create a more explicit necessity requirement for the collection of personal information, consistent with other privacy laws in Canada and abroad."[115]

Section 4 of the *Privacy Act* reads as follows: "No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."[116]

The Commissioner indicated that he currently interprets section 4 to mean that "the collection of information must be necessary for the operating program or activity,"[117] and that his interpretation is consistent with that provided by the Treasury Board Secretariat in its *Directive on Privacy Practices*. The Commissioner observed, however that "this interpretation is not always applied by the government,"[118] and that "the shift from paper-based to digital format records has actually led to a dynamic of over-collection."[119]

3.1.2 Witnesses' views

Overall, while some would go further than the Commissioner's recommendation, Ms. Scassa,[120] Ms. McPhail,[121] Mr. Israel,[122] Mr. Fraser,[123] Mr. Geist,[124] Mr. Molloy,[125]

115 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

116 *Privacy Act*, s. 4.

117 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

118 Ibid.

119 Ibid.

120 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0855 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual).

121 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

122 Ibid., 1135 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

123 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1100 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

124 Ibid., 1105 (Mr. Michael Geist, Canada Research Chair in Internet and E-Commerce Law, University of Ottawa, As an Individual).

125 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1105 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

Ms. Tully,[126] Ms. Bernier,[127] Mr. Gogolek[128] and the CBA[129] agree with the addition of a necessity requirement in the *Privacy Act* for the collection of personal information.

3.1.2.1 Reduce the quantity of personal information collected

Ms. Scassa[130] and Mr. Israel[131] indicated that the existing standard for data collection is too imprecise and loose, and that the Commissioner's recommendation is intended "to curtail the practice of overrcollection of personal information."[132] Specifically, these two witnesses said that this recommendation is necessary in the age of big data where organizations are encouraged to collect a great deal of data.[133] Mr. Israel[134] and Ms. McPhail[135] suggested that reorienting thinking toward necessity encourages public servants to ask themselves about the real necessity of collecting and retaining information.

Ms. Scassa discussed the principle of data minimization, which is supported by many data protection authorities around the world, and suggested that imposing clear limits on the government with regard to data collection encourages transparency.[136] According to Ms. McPhail[137] and Ms. Scassa, the Commissioner's recommendation is consistent with the principle of data minimization because it "requires a reduction of the amount of information that is collected."[138] Furthermore, Ms. Scassa[139] and Mr. Gogolek[140] maintained that the overcollection of data creates risks for the protection of

---

126 Ibid., 1105 (Ms. Catherine Tully, Information Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

127 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1105 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

128 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1110 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

129 Canadian Bar Association, *Privacy Act* Amendments, September 2016, brief submitted to the Committee.

130 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0855 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual).

131 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1135 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

132 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0855 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual).

133 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1135 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic); ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0950 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual).

134 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1225 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

135 Ibid., 1225 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

136 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0855 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual).

137 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

138 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0950 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual).

139 Ibid., 0855.

140 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1110 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

data. Along the same lines, Mr. Karanicolas stated that "data minimization is among the most important defensive measures in protecting personal information."[141]

3.1.2.2 Criteria for collecting personal information

The Committee heard testimony regarding the criteria that should apply to the collection of personal information.

Mr. Gogolek of BC FIPA stated that British Columbia's privacy legislation includes the necessity test for collecting information and that the "concept has received considerable interpretation, judicially and quasi-judicially, so its operation is well understood."[142]

Commissioner Therrien recommended defining the concept of necessity for the collection of personal information. He called on the Committee to consider four factors based on the Supreme Court of Canada's decision in *R v. Oakes*:[143]

> Thus, personal information would be collected under the necessity test if: the information is rationally connected and demonstrably necessary to an operating program or activity; the information is likely to be effective in meeting the objectives of the program or activity; there are no other less privacy-invasive way to effectively achieve the objectives of the program or activity; and the loss of privacy is proportional to the importance of the objectives of the program or activity.[144]

The Committee considered the possibility of imposing the standard of necessity as well as proportionality on the collection of data under the *Privacy Act*. On this front, the Commissioner responded that the OPC defines the concept of necessity "in part, through proportionality. At the end of the day, both necessity and proportionality would be part of the standard."[145] Mr. Israel,[146] Ms. McPhail[147] and Mr. Fraser[148] believe it would be advisable to adopt the principle of proportionality, particularly for the collection of personal information.

On the issue of whether the government can use personal information found on social media, Ms. Bernier specified that it is also subject to the necessity test: "The point is

---

141 Ibid., 1110 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

142 Ibid., 1110 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

143 *R v. Oakes*, [1986] 1 SCR 103.

144 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

145 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1130 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

146 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1140 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

147 Ibid., 1210 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

148 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1235 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

that the government cannot use that, because the government cannot use your personal information unless it demonstrates necessity."[149]

3.1.2.3 The necessity test and the *Canadian Charter of Rights and Freedoms*

On the one hand, Ms. Bernier supports the Commissioner's recommendation, but recommends that the Act "tie the requirement of necessity not to the program or activity, but to the *Canadian Charter of Rights and Freedoms*."[150] She explained that establishing a direct link with the Charter "rather than embed it in a justification of the program"[151] would provide greater protection.

Ms. Bernier indicated that the necessity test is found in the first section of the Charter, and that the *Oakes* decision interpreted this section as being based on four criteria: "necessity; proportionality of the intrusion to that necessity; effectiveness of that intrusion, in that you have to prove that it actually works; and the absence of a less intrusive alternative."[152]

Mr. Gogolek of BC FIPA, on the other hand, believes that "including the necessity in the Act itself works along the same lines as the *Oakes* test for proportionality. It has that aspect to it, because that's the way we generally interpret things."[153]

The Committee took great interest in the debate, but considers that tying the necessity test to an operating program or activity of a federal institution provides appropriate protection of Canadians' privacy rights.

3.1.2.4 The addition of criteria for the sharing, use and retention of personal information

The Committee heard testimony about the necessity test or other criteria, such as proportionality, should also be applied to the sharing, use and retention of personal information.

The following is a brief overview of the witnesses' opinions:

- Ms. McPhail believes that the necessity test should also apply to the retention and sharing of personal information.[154]

149 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1135 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

150 Ibid., 1105.

151 Ibid.

152 Ibid., 1135.

153 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1225 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

154 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

- Mr. Israel of CIPPIC maintained that the necessity test would also be appropriate for assessing whether data should be used or shared.[155]

- Mr. Fraser indicated that it would be better to subject the collection and secondary use of personal information to a principle of proportionality: "Is the benefit to government operation or the country as a whole proportional to any trade-off in privacy? I think those are questions that should be asked on a regular basis."[156]

- Mr. Israel recommended "the adoption of an overarching proportionality obligation that would apply to all collection, retention, use and disclosure of personal information by government agencies into the *Privacy Act.*"[157] He added that "an overarching proportionality or reasonableness obligation modelled on subsection 5(3) of PIPEDA would provide an avenue for assessing Charter considerations across all data practices."[158] Mr. Israel explained that his recommendation would allow for tempering the application of the exceptions provided for in section 8(2) of the *Privacy Act*.[159] Ms. McPhail supported Mr. Israel's recommendation.[160]

- Ms. Austin recommended that "the use or disclosure of personal information for law enforcement investigative or national security purposes should be subject to a review that reflects the protection of an individual's Charter rights under sections 7 and 8, and not simply be reviewed on a necessity standard."[161]

- Ms. Tully believes that the use of data should be guided by consistent use, which has sometimes been interpreted by the courts as incorporating the elements of necessity and proportionality.[162] Nevertheless, Ms. Tully favours adding a consideration of proportionality for the disclosure of information.[163] In her view, disclosure is often based on discretionary power, and it would be appropriate to provide guidance on this front.[164]

---

155 Ibid., 1135 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

156 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1235 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

157 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1140 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

158 Ibid.

159 Ibid., 1210.

160 Ibid., 1210 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

161 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0920 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual).

162 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1120 (Ms. Catherine Tully, Information Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

163 Ibid.

164 Ibid.

- Commissioner Therrien stressed that the *Privacy Act* already sets out certain standards for sharing personal information.[165] He specified that there was no need to impose the necessity test for sharing information for the following reason:

  > In an information-sharing context, there are two parties. There is a sending institution and there is a recipient institution. For the recipient institution, the information-sharing transaction is actually a collection exercise, so necessity may not apply to the sending institution, but it applies to the recipient institution.[166]

- The *Privacy Act* currently has very few criteria regarding the retention of personal information that has been legitimately collected by federal institutions. Mr. Israel explained that the absence of rules on how long data may be retained "can mean that that data is kept well beyond the point where its utility has expired, exponentially increasing the risk of data breach and of inappropriate uses. The lack of an explicit retention limitation requirement can even lead to the indefinite retention of data that has only a very short window of utility, greatly undermining the proportionality of a particular activity."[167] Mr. Israel added that "[i]ncluding an explicit retention limitation provision would not only mandate state agencies to adopt clear retention policies, but would also allow the Commissioner to address unreasonable retention in a principled manner."[168]

- The Commissioner indicated that necessity should be a criterion for the retention of personal information.[169]

3.1.2.5 Obligation for accuracy

Ms. Austin recommended that "subsection 6(2) of the Act be amended to impose an obligation to ensure the accuracy of any personal information that is used or disclosed by the institution for all purposes,"[170] and that the obligation for accuracy should also apply to methods of information processing because they are not all equally accurate. Ms. Austin indicated that inaccurate information can have grave consequences on fundamental rights and freedoms.

Ms. Austin explained that subsection 6(2) of the *Privacy Act,* which states that "[a] government institution shall take all reasonable steps to ensure that personal

---

165 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1130 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

166 Ibid., 1135.

167 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1140 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

168 Ibid.

169 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1135 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

170 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0920 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual).

information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible,"[171] "should apply to the disclosure of information, not just uses."[172] Furthermore it is "currently confined to administrative purposes, and it should be broadened to all the purposes that it's used for."[173]

3.1.2.6 The views of federal institutions

Several representatives of federal institutions raised concerns regarding the implementation of the Commissioner's recommendation to add a necessity test to the *Privacy Act* for the collection of personal information.

First, Mr. Proulx of the Canada Border Services Agency said that in his opinion, "the principle is already embedded in what we do every day."[174] Nevertheless, he did underscore the importance of approaching the necessity test from a practical angle, and said he is concerned from an operational perspective:

> A necessity test, in theory, seems to be a good idea; in practice, I'm not sure how you would apply it, especially with the vast amount of information that we all collect to fulfill our mandates.
>
> Whatever the test, if ever it were embedded in legislation, would have to be operationally feasible, because you have to be able to collect information in real time. I don't know how that would also affect past collection, when the legislation is introduced. Would you have to go back and do a necessity test, or prove that you do indeed have a need to collect that information, or would it start when the new legislation is implemented?[175]

As for implementation of the necessity test, RCMP Assistant Commissioner Joe Oliver emphasized that his institution's collection activities are mainly judicially authorized: "We've presented cases to a judge indicating a compelling reason for us to pursue very specific targeted and focused information under warrant or under production order."[176] From that perspective, Mr. Oliver raised concerns regarding the addition of a necessity test to the *Privacy Act*:

> [It] would have to be carefully carried out so as not to interfere with evidence gathering if that recommendation is accepted. When it comes to evidence gathering, we pursue evidence where it exists…. Limiting law enforcement to collect only certain pieces of information could restrict our ability to deliver our public safety mandate.[177]

---

171 *Privacy Act*, s. 6(2).

172 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 0920 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual).

173 Ibid.

174 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1205 (Mr. Dan Proulx, Director, Access to Information and Privacy Division, Canada Border Services Agency).

175 Ibid.

176 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1205 (Mr. Joe Oliver, Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police).

177 Ibid., 1145.

Mr. Peirce of CSIS mentioned that section 12 of the *Canadian Security Intelligence Service Act* already provides a necessity test for the collection of information.[178]

Finally, in terms of information sharing, Mr. Oliver emphasized "the importance of the right time for information to be shared quickly and efficiently,"[179] and stressed that "sharing your information is never taken lightly. It's always considered in the context of the relevancy, the accuracy, the need to know, the right to know, and all of those things."[180] Likewise, Mr. Peirce commented that information sharing is an essential part of their mandate, and that they "strive to share information in a proportionate way,"[181] but that it is sometimes very complex, and many factors come into play.

3.1.3 The Committee's recommendation

In light of the testimony, the Committee supports the Commissioner's recommendation and recognizes the importance of adding the necessity test to the *Privacy Act* for the collection of personal information. While the testimony suggested that the interpretation given to the necessity test does include an element of proportionality, it would nevertheless be important to explicitly add a proportionality test to the *Privacy Act*, along with necessity. Indeed, the witnesses convinced the Committee that the principle of proportionality is essential for determining whether it is necessary to collect personal information.

Furthermore, in light of the testimony, the Committee is of the opinion that the necessity and proportionality tests should also apply:

- to the retention of personal information;
- when personal information is being shared, i.e., to the collection of personal information when a recipient federal institution receives information through communications with another federal institution.

The Committee therefore recommends:

RECOMMENDATION 11

That section 4 of the *Privacy Act* be amended to explicitly require compliance with the criteria of necessity and proportionality in the context of any collection of personal information, consistent with other privacy laws in effect in Canada and abroad.

---

178 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1210 (Mr. Michael Peirce (Assistant Director, Intelligence, Canadian Security Intelligence Service).

179 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1245 (Mr. Joe Oliver, Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police).

180 Ibid.

181 Ibid., 1245 (Mr. Michael Peirce (Assistant Director, Intelligence, Canadian Security Intelligence Service).

RECOMMENDATION 12

That the *Privacy Act* be amended to clarify that a recipient federal institution that receives personal information through information sharing with another federal institution is collecting personal information within the meaning of section 4 of the *Privacy Act*, and must meet the criteria of necessity and proportionality that apply to the collection of personal information.

RECOMMENDATION 13

That section 6 of the *Privacy Act* be amended so as to explicitly require compliance with the criteria of necessity and proportionality in the context of any retention of personal information.

RECOMMENDATION 14

That the *Privacy Act* be amended to set clear rules governing the collection and protection of personal information that is collected on the internet and through social media.

3.2 The various overview models

The OPC is currently based on the ombudsman model. The Commissioner may investigate complaints pertaining to the rights and protections set out in the *Privacy Act*.[182] Following an investigation, if he finds that the complaint is well-founded, the Commissioner can only make non-binding recommendations to the government.[183] The Commissioner is of the opinion that the *Privacy Act* should be amended to adopt a more effective overview model.

3.2.1 Overview models in the provinces and territories

There are currently a variety of overview models for information and privacy commissioners in the provinces and territories.

The information and privacy commissioners of Alberta, British Columbia, Ontario, Prince Edward Island and Quebec have order-making powers.[184] "Eight provinces and territories do not."[185]

In 2015, the Province of Newfoundland and Labrador adopted a new overview model: the hybrid model. This involves an improved ombudsman model in which the Newfoundland and Labrador Information and Privacy Commissioner has the power to make binding recommendations to the government. However, if the government institution

182 *Privacy Act*, s. 29(1).

183 *Privacy Act*, s. 35(1)(a).

184 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

185 Ibid.

decides not to comply in whole or in part with the provincial commissioner's recommendation, it must apply to the court within 10 days of receipt of the recommendation for a declaration that it is not required to comply.[186]

3.2.2 The Privacy Commissioner's view

In the brief he presented to the Committee and during his testimony, the Commissioner emphasized that while most institutions eventually accept his recommendations, "there can be lengthy delays in reaching a satisfactory conclusion."[187] In particular, federal institutions do not necessarily have to provide the OPC with complete documents at the outset. "It's possible for them to make their real case before the Federal Court."[188] The Commissioner indicated that the delays in the process "may be in part because all we can do is to recommend, and there is no sanction for government not to act promptly in responding to our investigation."[189] In the Commissioner's view, "[t]his is inconsistent with the objective of the ombudsman model, which is to provide a quick and low-cost recourse to ensure that the privacy rights of individuals are respected."[190]

In March 2016, the Commissioner recommended to the Committee adoption of the Newfoundland and Labrador hybrid model.[191] In September 2016, however, the Commissioner informed the Committee that he was amending his recommendation and that after further review, he was now recommending the adoption of a model that would give him order-making powers.[192]

3.2.2.1 The Privacy Commissioner's initial recommendation

In March 2016, the Commissioner recommended adoption of a hybrid model. He felt this model would bring more rigour and speed to the process "while maintaining the informality of the ombudsman model"[193] and avoiding "the costs of a more formal

---

186 Newfoundland and Labrador, *Access to Information and Protection of Privacy* Act, 2015, Chapter A-1.2, 2016 c6 s2, ss. 50 and 79.

187 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016; ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

188 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1115 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

189 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0920 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

190 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

191 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

192 Office of the Privacy Commissioner of Canada, Advice to Parliament, Study of the *Privacy Act*, Letter to the Standing Committee on Access to Information, Privacy and Ethics about the study of the *Privacy Act*, 13 September 2016.

193 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

adjudicative process."[194] The Commissioner based his recommendation on two key considerations: the effectiveness of each model and the risks associated with each.

First, while order-making powers would create an incentive for federal institutions, he believed that the Newfoundland and Labrador model attains the same result: "I'm just suggesting a different way to get to the same place.…"[195]

Second, according to the Commissioner, there are fewer risks associated with the adoption of a hybrid model than with an order-making model. In particular, the Commissioner pointed out that an overview model with order-making powers means "a more formal process"[196] that "has the potential to be costlier"[197] and "involve more in terms of procedural rights."[198] The Commissioner added that "[s]uch a system could reduce the risk that some may perceive a conflict between the Commissioner's roles as impartial tribunal and privacy champion:"[199]

> Another factor is that if there are order-making powers in a body that also has a responsibility, which I'm recommending here, to promote privacy rights, can you have in the same place a body that promotes privacy and the same body adjudicating impartially on the rights of Canadians vis-à-vis a government institution? I'm not saying it's incompatible. It's possible perhaps in terms of structure to build Chinese walls and to make these distinctions.[200]

3.2.2.2 The Privacy Commissioner's modified recommendation

In September 2016, the Commissioner recommended that "the Act be amended by replacing the ombudsman model with one where the Privacy Commissioner would be granted order-making powers."[201] In support of his new recommendation, the Commissioner sent a letter to the Committee in which he stated that he had further explored the matter from the perspective of administrative law, notably with regard to procedural fairness and conflicts of interest, to determine whether granting the Commissioner order-making powers would be incompatible with his various promotion functions. The Commissioner reached the following conclusion:

> After careful review, last summer in particular, we have concluded that there are indeed legal risks with one body having both adjudicative and promotion functions. Based on our review, however, these risks are likely the same under the hybrid model in Newfoundland and Labrador.

---

194 Ibid., 0850.

195 Ibid., 0920 and 0925.

196 Ibid., 0925.

197 Ibid.

198 Ibid.

199 Ibid., 0845.

200 Ibid., 0920.

201 Office of the Privacy Commissioner of Canada, Advice to Parliament, Study of the *Privacy Act*, Letter to the Standing Committee on Access to Information, Privacy and Ethics about the study of the *Privacy Act*, 13 September 2016.

> Importantly, crucially in fact, our review also led us to conclude that these risks can be largely mitigated through a clearer separation of adjudicative and promotion functions within the OPC. This kind of structure, as you know, exists in many provinces. It is important to understand that such a separation would entail certain costs, but we have not yet quantified these. Since the legal risks and mitigation measures are the same under the hybrid model in Newfoundland and Labrador, the order-making model is in my opinion preferable as it provides a more direct route to timely, final decisions for complainants.[202]

As for the costs that would be incurred if there were a change of model, the Commissioner affirmed that it would be necessary to separate certain functions, but that his office had not yet "quantified these."[203] However, in a letter to the Committee on 17 November 2016, Commissioner Therrien mentioned that the costs will depend on the model chosen and that many variables come into play. The Commissioner anticipates that "roughly 10% of complaints that typically go on to investigations (excluding early resolved cases) could be referred to adjudication under the *Privacy Act* (representing about 80% cases per year)."[204] Overall, the Commissioner said he would "tentatively estimate costs to be in the range of $0.75-1.25M annually once an adjudicative function became fully functional."[205] Based on the testimony, it is unclear what the costs of moving to a hybrid model would be.

He also indicated that given that order making would only be required in a small number of cases, mediation or other solutions would be preferred: "It's important to have the tool in the tool box, but in managing the volume of work and the volume of complaints, I don't think that order making would be used in very many cases."[206]

The Commissioner explained in his letter the advantages of avoiding *de novo* hearings, which start anew with evidence being introduced afresh before the court:

> Individuals would not need to seek recourse from the Federal Court via a *de novo* hearing as they would be able to obtain a remedy directly from my Office. Further, orders would be subject to judicial review under s. 18.1 of the *Federal Courts Act*. Departments seeking to challenge my orders would have to initiate these proceedings, carry the burden of proof and be limited in the evidence they could rely on. This would encourage departments to be more forthcoming and timely with their submissions to my office up front during the process knowing that they would be generally committed to this evidentiary basis should the matter be judicially reviewed before the courts.[207]

---

202 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1er November 2016, 1100 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

203 Ibid., 1205.

204 Office of the Privacy Commissioner of Canada, Letter to the Committee, 17 November 2016.

205 Ibid.

206 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1er November 2016, 1125 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

207 Office of the Privacy Commissioner of Canada, Advice to Parliament, Study of the *Privacy Act*, Letter to the Standing Committee on Access to Information, Privacy and Ethics about the study of the *Privacy Act*, 13 September 2016.

3.2.3 Witnesses' views

During its study, the Committee heard a number of points of view regarding the best overview model to adopt. There was consensus on one point, however: the current ombudsman model with powers of recommendation is not effective. This section presents the views of the witnesses who advocate the order-making model, and those who advocate the hybrid model. It should be noted that some witnesses did not have a fixed position, and presented arguments in favour of both models.

3.2.3.1 Witnesses advocating for the order-making model

Ms. Austin,[208] Ms. McPhail,[209] Thomas Keenan of the University of Calgary,[210] Mr. Rubin,[211] Mr. Bennett,[212] Mr. Geist,[213] Mr. Gogolek,[214] Ms. Tully[215] and Mr. McArthur[216] advocate adopting the order-making model. While Mr. Dickson[217] of the CBA advocates the hybrid model, he presented arguments in favour of both systems. The summary below includes his arguments for the order-making model.

Appendix B of this report presents the testimony regarding the order-making model. The key ideas that emerged from the testimony are as follows:

- Order-making power creates an incentive for federal institutions to cooperate, which makes this model more effective.
    - A commissioner with order-making powers can more easily guide the parties toward informal resolution processes, such as mediation, which are faster.
    - Complaints are resolved more quickly and seriously.

---

208 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 1000 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual).

209 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1110 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

210 Ibid., 1120 (Mr. Thomas Keenan, Professor, University of Calgary, As an Individual).

211 Ibid., 1130 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

212 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1105 and 1200 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

213 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1200 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

214 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1115 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

215 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1115 and 1210 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

216 Ibid., 1125 (Mr. Drew McArthur (Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia).

217 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1120 and 1125 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

- The Commissioner can obtain responses more quickly in the context of an investigation.

- The right to privacy is protected by the *Canadian Charter of Rights and Freedoms* and a quasi-constitutional statute, the *Privacy Act.* The Commissioner's powers should be proportional to the importance of that right and the significant damage that can be caused by a violation of privacy.

- When an agency uses order-making powers, the procedures are more formal, notably due to procedural fairness.

  - Respect for procedural fairness serves to lengthen the time to handle complaints.

  - The process is less accessible and flexible.

  - The parties are often represented by lawyers.

  - The Commissioner's decisions must be exhaustive, explanatory and judicial in nature.

- The order-making model is consistent with international practices in terms of agencies that are mandated to protect data.

- The change from the ombudsman model to the order-making model would be costly.

  - Within the OPC, it would be necessary to separate the groups that promote privacy, the groups that handle complaints through mediation, and the groups that handle complaints as an administrative tribunal.

3.2.3.2 Witnesses advocating for the hybrid model

Clyde Wells,[218] Member of the Independent Statutory Review Committee, Mr. Dickson,[219] Mr. Fraser,[220] Mr. Molloy[221] and Mr. Drapeau[222] advocated the hybrid model. Mr. Karanicolas did not take a position. He raised several questions,

---

218 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 May 2016, 0915 and 0945 (Mr. Clyde Wells, Member, Independent Statutory Review Committee).

219 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1120, 1125, 1155, 1200 and 1220 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

220 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1105 and 125 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

221 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1150 and 1210 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

222 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1120 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Law, As an Individual).

however, including why the order-making model would be considered more effective than the hybrid model.[223]

Appendix C of this report presents the testimony regarding the hybrid model. The key ideas that emerged from the testimony are as follows:

- The hybrid model was developed in order to address the problem of delays in handling complaints within the Office of the Information and Privacy Commissioner of Newfoundland and Labrador, and to propose solutions to make the investigative process faster and more efficient.
    - To shorten the time for handling complaints, the Newfoundland and Labrador Act imposes strict time limits. This serves as an important incentive for agencies.
    - The time limits set out in the Act ensure that the Commissioner can obtain responses from agencies faster, while maintaining his role as ombudsman.
    - The hybrid model proposes a less confrontational approach than the order-making model because the Commissioner has the power to move the discussions forward, but not the power to oblige an agency to take action.
    - The Commissioner can participate in hearings in order to provide his viewpoint.
- Given that it is still based on the ombudsman model, the hybrid model is more accessible, more user friendly, less structured, less formal and more flexible than the order-making model. The accessibility of the process is consistent with the quasi-constitutional status of privacy accorded to Canadians in the *Privacy Act*.
    - For an investigation under the hybrid model, procedural fairness does not have to be as rigid. The time limits imposed by the Commissioner can be shorter than those imposed through the order-making model, while still respecting procedural fairness.
- With the hybrid model, the burden shifts from the requester to the public agency that does not want to comply with the Commissioner's recommendations.
- While the hybrid model has been established in a jurisdiction that receives relatively few complaints, that does not mean that it is not appropriate for a jurisdiction that receives a high volume of complaints. Nevertheless, in

223 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

jurisdictions with very few employees, the hybrid model is preferable to the order-making model given that it would be impossible to create a wall separating the groups with order-making and mediation functions.

- It would be easier to transition the OPC from the ombudsman model to the hybrid model than to the order-making model.

- The hybrid model is not yet proven given that it has been in place for less than a year. For the time being, however, it does appear to be working well.

3.2.4 The view of federal institutions

Monique McCulloch of Shared Services Canada indicated that if the Commissioner is accorded order-making powers, she does not believe there will be much of an impact on her organization given that there would be very few situations requiring orders to be issued.[224] Along the same lines, Maxime Guénette of the Canada Revenue Agency (CRA) commented that he would prefer to attempt to resolve the situation before an order was issued.[225] He also said that it is difficult to predict the implications of adopting an order-making model, but that "with a place like CRA, with the volume that we're dealing with, depending on how this gets rolled out, there may be an impact in terms of our processes and our resources."[226] Finally, Ms. Beck from Immigration, Refugees and Citizenship Canada underscored that her department "would want to make sure that, notwithstanding new powers given to the Commissioner, we could still protect our national security issues."[227]

3.2.5 The powers of the Privacy Commissioner and Information Commissioner

In February 2016, the Committee began a study of the *Access to Information Act.* During that study, the Committee heard from a number of witnesses in support of the Information Commissioner's recommendation to strengthen "oversight of the right of access by adopting an order-making model."[228] On 31 March 2016, the President of the Treasury Board, the Honourable Scott Brison, announced that in the context of the reform of access to information in Canada, the government would be implementing several commitments, including giving the Commissioner the power to order the release of

---

224 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1230 (Ms. Monique McCulloch, Director, Access to Information and Privacy, Shared Services Canada).

225 Ibid., 1230 (Mr. Maxime Guénette, Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch, Canada Revenue Agency).

226 Ibid.

227 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 October 2016, 1150 (Ms. Stefanie Beck (Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration).

228 Office of the Information Commissioner of Canada, Striking the Right Balance for Transparency–Recommendations to Modernize the *Access to Information Act*, March 2015; ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 February 2016, 0855 (Ms. Suzanne Legault, Information Commissioner of Canada, Office of the Information Commissioner of Canada).

government information.[229] In June 2016, the Committee tabled its report entitled *Review of the Access to Information Act*, in which it recommended: "That the government strengthen the oversight of the right of access by adopting an order-making model with clear and rigorously defined parameters."[230]

As Commissioner Therrien stated to the Committee on a number of occasions, the Supreme Court of Canada has recognized that the *Privacy Act* and the *Access to Information Act* are a seamless code.[231] The Commissioner explained this concept as follows:

> Certainly, both statutes provide a right of access…. In both statutes, there are provisions that call for certain exceptions or exemptions to that right, to protect certain interests: law enforcement, international relations, etc. The right of access and the exceptions to the right of access are extremely similar in the two pieces of legislation, and I think that is the core of what the Supreme Court is referring to when it says the two acts constitute a seamless code. I think that, if you change coverage in one act, you should at least consider whether to amend coverage in the other act.[232]

In this context, several witnesses addressed the following question: if the overview model for the Privacy Commissioner and the Information Commissioner is amended, should these two Officers of Parliament have the same powers?

Commissioner Therrien commented that "it is not obvious to me that if one Commissioner has order-making powers, the other Commissioner needs to have the same powers exactly,"[233] and that "[i]t might be desirable to let the acts work in the same way, but it might not be necessary. Certainly, for right of access and exceptions, and most likely for coverage.... On other issues, there might be room for separate decisions on the two pieces of legislation."[234] Mr. Karanicolas mentioned that there are important differences between the Privacy Commissioner and the Information Commissioner, and they do not necessarily require similar powers.[235] Specifically, Mr. Karanicolas stated that there should be a determination of whether the Privacy Commissioner should have order-making powers for both the public sector and the private sector, given that there are differences in the role played by the Commissioner in these two sectors.[236]

---

229 The Honourable Scott Brison, President of the Treasury Board, *Speaking notes for the Honourable Scott Brison, President of the Treasury Board to the Canadian Open Dialogue Forum 2016*, Ottawa, 31 March 2016.

230 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Review of the Access to Information Act*, Second report, 1st Session, 42nd Parliament, June 2016.

231 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016; Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police), [2003] 1 S.C.R. 66, at para 22.

232 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0855 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

233 Ibid., 0850.

234 Ibid.

235 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

236 Ibid., 1135.

Mr. Bennett[237] and Ms. Tully[238] believe that the two Commissioners should have the same powers. Mr. Bennett explained it as follows: "Canada is probably the only country in the world where the issues of access to information and privacy are seen as two sides of the same coin."[239]

3.2.6 The Committee's recommendation

The Committee recommends:

RECOMMENDATION 15

a) That the Government of Canada strengthen the oversight of privacy rights by adopting an order-making model with clear and rigorously defined parameters.

b) That, in order to ensure the most effective use of resources, the Government of Canada explore ways of finding efficiencies, by, among other things, combining the adjudicative functions of the Office of the Privacy Commissioner of Canada and the Office of the Information Commissioner of Canada.

3.3 Expand judicial recourse and remedies

The Commissioner initially recommended that "section 41 of the Act be broadened to allow complainants, or the Privacy Commissioner, to apply for review by the Federal Court concerning all matters that may be the subject of a complaint, including collection, use and disclosure matters,"[240] and that "the Court be able to award a full array of remedies including damages as currently exists under the *Personal Information Protection and Electronic Documents Act* (PIPEDA)."[241] Indeed, at the present time, the *Privacy Act* provides for a review by the Federal Court only where an individual has been refused access to personal information and has made a complaint to the Privacy Commissioner.[242] The *Privacy Act* does not, however, provide for legal remedies in the majority of situations in which there has been a violation of the rights it guarantees.

The Commissioner explained that this recommendation would probably no longer be necessary if he were given full order-making powers, because "individuals would not

---

237 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1245 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

238 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1210 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

239 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1245 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

240 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

241 Ibid.

242 *Privacy Act*, s. 41.

need to seek recourse from the Federal Court via a *de novo* hearing as they would be able to obtain a remedy directly from my Office."[243]

Despite this sentiment, several witnesses discussed the various remedies possible, and recommended a number of measures.

Ms. Austin,[244] Mr. Rubin,[245] Mr. Gogolek[246] and the CBA[247] supported the Commissioner's recommendation.

Mr. Rubin indicated that it would be helpful "if individuals and groups bringing such privacy violation cases to court were given resources to sue the government."[248] Ms. Scassa stressed that opening up new remedies under the *Privacy Act* exposes the government of Canada to fines.[249] Mr. Drapeau, meanwhile, commented that "one of the most important remedies that can be provided to a complainant is to handle his or her complaint in a reasonable amount of time,"[250] and that he would like a time limit to be imposed on the Commissioner for reporting and making recommendations.

Mr. Fraser[251] and Mr. Gogolek[252] mentioned that it would be important to add an element of personal accountability to the *Privacy Act*, such as an offence under which charges can be brought against a person or institution that violates the statute.

Ms. Bernier stressed that in Europe, privacy commissioners have the power to impose fines even on government institutions.[253] Likewise, Mr. Keenan mentioned that under the European Union's new general data protection regulations, the fines "are

---

243 Office of the Privacy Commissioner of Canada, Advice to Parliament, Study of the *Privacy Act*, Letter to the Standing Committee on Access to Information, Privacy and Ethics about the study of the *Privacy Act*, 13 September 2016.

244 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 1000 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual).

245 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1130 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

246 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1110 and 1115 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

247 Canadian Bar Association, *Privacy Act* Amendments, September 2016, Submission to the Committee.

248 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1130 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

249 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 1020 (Ms. Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual).

250 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1115 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Common Law, As an Individual).

251 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1100 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

252 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1215 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

253 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 October 2016, 1135 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

astronomical, something like 4% of the annual turnover of a business,"[254] and that this has a deterrent effect.

Patricia Kosseim of the Office of the Privacy Commissioner indicated that the remedies provided for in PIPEDA could make sense in the context of the *Privacy Act*, saying it:

> provides a good model of the array of remedies a court could order in the event of contravention of the act – in that case PIPEDA, but there is no reason that it wouldn't apply in the case of the *Privacy Act* as well – by way of an order to do something, an order to stop doing something, an order for damages, or an order for a publication of a notice of any action taken or proposed to be taken to correct practices. All of those are applicable in the public sector as well.[255]

Mr. Israel of the CIPPIC said he would go further than what is provided for in PIPEDA:

> The current damages mechanism in PIPEDA is closer to a fine, basically. It's hard to actually implement, because you need to meet very high standards of proof before you can show that someone intentionally violated privacy, whereas an administrative monetary penalty regime would be more appropriate to these types of regulatory regimes. We specifically suggested in our comments, but very briefly, consideration of a private right of action. There is an issue, of course, where you're opening the government up to fines. …[256]

Mr. Keenan[257] and Mr. Israel[258] said they were in favour of administrative penalties subject to judicial review by the Federal Court. Mr. Keenan added that "education would be a wonderful use of any monies collected."[259]

Finally, Mr. Israel stated that he would also be in favour of creating a private right of action independent of and parallel to the filing of a complaint with the Commissioner's office.[260]

The Committee welcomes the testimony heard on this matter, but did not consider that it had sufficient information to make a decision regarding sanctions. Accordingly, the Committee recommends:

---

254 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1205 (Mr. Thomas Keenan, Professor, University of Calgary, As an Individual).

255 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 0945 (Ms. Patricia Kosseim (Senior General Counsel and Director General, Legal Services, Policy, Research and Technology Analysis Branch, Office of the Privacy Commissioner of Canada).

256 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1215 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

257 Ibid., 1220 (Mr. Thomas Keenan, Professor, University of Calgary, As an Individual).

258 Ibid., 1220 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

259 Ibid., 1220 (Mr. Thomas Keenan, Professor, University of Calgary, As an Individual).

260 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1220 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

RECOMMENDATION 16

That the Government of Canada further examine the possibility of expanding judicial recourse and remedies under the *Privacy Act*.

3.4 Statutory mechanism for independently reviewing complaints

During his last appearance before the Committee, the Commissioner recommended that the government "consider creating a statutory mechanism to independently review privacy complaints against the OPC [Office of the Privacy Commissioner]."[261] The Commissioner explained that since his previous appearance,

> [T]he Federal Court recently considered the Privacy Commissioner ad hoc mechanism that my office created to provide for an independent review of complaints against my own office. This mechanism was needed when the OPC itself became subject to the *Privacy Act* with the adoption of the *Federal Accountability Act* in 2007. In assessing the independence of this mechanism, the court noted this was a question [in particular if there should be a statutory basis for this mechanism][262] more appropriately addressed by Parliament.[263]

The Committee did not hear any testimony on this subject.

3.5 Privacy impact assessments

3.5.1 The Privacy Commissioner's view

Commissioner Therrien made a recommendation to "require government institutions to conduct privacy impact assessments (PIAs) for new or significantly amended programs and submit them to OPC prior to implementation."[264] Because PIAs have a preventative goal, assessments should generally be done "prior to the adoption of new or substantially modified programs, in all but exceptional cases."[265] In addition, the Commissioner pointed out that PIAs are invaluable in "identifying and mitigating privacy risks prior to project implementation."[266]

In his brief, the Commissioner noted that privacy laws in numerous jurisdictions, both provincial and international, require PIAs to be conducted in many circumstances.[267]

The Treasury Board Secretariat's *Directive on Privacy Impact Assessment* requires "institutions planning on undertaking projects which involve personal information to

---

261 Office of the Privacy Commissioner, Brief, 1 November 2016.

262 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1135 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

263 Ibid., 1105.

264 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

265 Ibid.

266 Ibid.

267 Ibid.

conduct a Privacy Impact Assessment and submit a copy to [the OPC]."[268] Nonetheless, according to the Commissioner, it is important that the *Privacy Act* include a requirement to conduct PIAs for new or significantly amended programs and submit them to the OPC prior to implementation, as

> [t]he use of PIAs by institutions, as well as their timeliness and quality, have sometimes been uneven. A legal requirement would ensure PIAs are conducted in a thorough manner and completed before new programs are launched or when information management rules of existing programs are substantially modified.[269]

The Commissioner underscored the importance that the OPC be involved from the outset in order to reduce privacy risks: "[I]t is preferable to identify, reduce, and mitigate privacy risks before they occur, as opposed to finding remedies after the risk has materialized. It is important to have remedial powers, but it is just as important, and probably more important, to identify risks as programs are developed, and to mitigate these risks from the get-go."[270]

Lastly, the Commissioner said that including a legal requirement to conduct PIAs in the *Privacy Act* could increase costs for federal institutions whose practices do not include PIAs.[271]

3.5.2 Witnesses' views

Several witnesses, including Ms. McPhail,[272] Mr. Israel,[273] Mr. Bennett,[274] Mr. Geist,[275] Mr. Fraser,[276] BC FIPA[277] and the CBA,[278] supported the Commissioner's recommendation.

Ms. McPhail[279] and Mr. Bennett[280] said that, to achieve the preventative goal of PIAs, it is important to start the process and involve the Commissioner at the design stage

---

268 Ibid.

269 ETHI, Evidence, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

270 ETHI, Evidence, 1st Session, 42nd Parliament, 1 November 2016, 1110 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

271 Ibid., 1145).

272 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

273 Ibid.6, 1145 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

274 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1105 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

275 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1200 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

276 Ibid., 1200 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual)

277 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

278 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

to identify and mitigate privacy risks in a timely manner and build in protections. Mr. Israel recommended introducing "an avenue for facilitating public input into the process so that discussions of privacy-invasive programs can occur with public input at the formative stages.[281] Similarly, Ms. McPhail added that PIA summaries should be made public "so that citizens can see that this process has happened."[282]

Mr. Bennett said that, to be effective, PIAs must not just be a statutory checklist but "a recurrent process, an ongoing process."[283] He argued that they are "far more useful when the implications for privacy are considered in a broader context beyond the law and when agency officials are invested in the process of doing that analysis in a recurring way."[284]

Many witnesses highlighted the importance of including a requirement to conduct a PIA in the *Privacy Act*. Mr. Bennett said that, unless a requirement to conduct a PIA is formalized in the *Privacy Act*, "experience is going to vary and quality is going to vary."[285] Mr. Fraser added that "[i]f you do not do a privacy impact assessment, and you're legally required to under the Act, you've broken the law, which is more than slightly different from just avoiding a policy, skipping a policy, or a procedural step."[286] Along the same lines, Mr. Geist explained that privacy "too often becomes an afterthought on legislation that has a significant privacy impact"[287] and that the inclusion in the *Privacy Act* of a requirement to conduct a PIA prior to introducing a bill or at least prior to its implementation would ensure a recognition that considering the privacy implications of legislation is "essentially part of the legislative-making process."[288]

Sean Murray from the Office of the Information and Privacy Commissioner of Newfoundland and Labrador pointed out that Newfoundland and Labrador's legislation includes a PIA requirement and that it is a "useful process in order for public bodies to get a good handle on the risks to privacy and to be able to address or mitigate those risks."[289]

---

279 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

280 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1225 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

281 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1145 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

282 Ibid., 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

283 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1105 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

284 Ibid., 1225 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

285 Ibid., 1230.

286 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1200 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual)

287 Ibid., 1200 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

288 Ibid.

289 ETHI, Evidence, 1st Session, 42nd Parliament, 4 October 2016, 1115 (Mr. Sean Murray, Executive Director, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

Similarly, the CRA,[290] CSIS,[291] IRCC,[292] the RCMP[293] and the CBSA[294] said they have conducted PIAs, which they found to be an invaluable process, and that their dealings with the OPC were constructive and collaborative. For example, the IRCC said that PIAs allow them to identify and address issues, especially because of the help and perspective the OPC provides.[295] The CBSA said it tries to involve the Commissioner from the beginning.[296] However, the IRCC[297] and the RCMP[298] said they do not necessarily consult the Commissioner at the outset but when they best see fit. The IRCC[299] and the CBSA[300] said that the process is complex and time-consuming and requires a lot of resources, especially because of the expertise required.

3.5.3 The Committee's recommendation

In light of the testimony heard, the Committee recognizes the importance and usefulness of conducting PIAs as a way to reduce privacy risks. The Committee supports the Commissioner's recommendation and therefore recommends:

RECOMMENDATION 17

That the *Privacy Act* be amended to include a requirement for government institutions to conduct privacy impact assessments for new or significantly amended programs and submit them to the Office of the Privacy Commissioner of Canada in a timely manner.

290 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1120 (Mr. Maxime Guénette, Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch, Canada Revenue Agency).

291 ETHI, Evidence, 1st Session, 42nd Parliament, 25 October 2016, 1210 (Ms. Stefanie Beck (Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration).

292 Ibid., 1210 (Mr. Michael Peirce, Assistant Director Intelligence, Canadian Security Intelligence Service).

293 Ibid., 1240 (Ms. Rennie Marcoux, Chief Strategic Policy and Planning Officer, Royal Canadian Mounted Police).

294 Ibid., 1235 (Mr. Dan Proulx, Director, Access to Information and Privacy Division, Canada Border Services Agency).

295 Ibid., 1210 (Mr. Michael Peirce, Assistant Director Intelligence, Canadian Security Intelligence Service).

296 Ibid., 1140 (Mr. Dan Proulx, Director, Access to Information and Privacy Division, Canada Border Services Agency).

297 Ibid., 1240 (Mr. Michael Peirce, Assistant Director Intelligence, Canadian Security Intelligence Service).

298 Ibid., 1240 (Ms. Rennie Marcoux, Chief Strategic Policy and Planning Officer, Royal Canadian Mounted Police).

299 Ibid., 1210 (Ms. Stefanie Beck (Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration).

300 Ibid., 1205 (Mr. Dan Proulx, Director, Access to Information and Privacy Division, Canada Border Services Agency).

3.6 Consultation on draft legislation and regulations

3.6.1 The Privacy Commissioner's view

Commissioner Therrien made a recommendation to "require government institutions to consult with the OPC on draft legislation and regulations with privacy implications before they are tabled."[301]

In his brief, the Commissioner noted that "[s]everal provincial and international laws now set out an explicit requirement for government institutions to consult their data protection authority as they prepare new legislation."[302] In Newfoundland and Labrador, for example, the legislation states that:

> a Minister shall consult with the Commissioner on a proposed bill that could have implications for access to information or protection of privacy, as soon as possible before, and not later than, the date on which notice to introduce the bill in the House of Assembly is given. The Commissioner must advise the Minister as to whether the proposed bill has implications for access to information or protection of privacy, and can comment publically on a draft bill any time after it has been made public.[303]

The Commissioner added that a new provision in the EU *General Data Protection Regulation* requires that:

> Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to the processing of personal data (Article 34, Recital 7).[304]

In his testimony, the Commissioner said that the purpose of this recommendation is to "[prevent] privacy violations"[305] by requiring parliamentarians to consult the OPC when drafting legislation.[306] He also mentioned that the recommendation applies to both government and private members' legislation.[307] He noted that this new role would be in addition to his advisory role during a committee's legislative review process. Lastly, the Commissioner said that his recommendations further to such consultations should be made public:

---

301 ETHI, Evidence, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada); Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

302 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

303 Ibid.

304 Ibid.

305 ETHI, Evidence, 1st Session, 42nd Parliament, 10 March 2016, 0940 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

306 Ibid.

307 Ibid.

> Such a system must not […] create the impression that the OPC is advising the party in power in one way and advising the other political parties differently. In exercising this responsibility, it is extremely important for us to be seen as acting impartially.[308]

3.6.2 Witnesses' views

On the one hand, Ms. McPhail,[309] Mr. Israel,[310] Ms. Bernier[311] and the BC FIPA[312] supported the Commissioner's recommendation. For example, Ms. McPhail said that consultation should take place before a bill is tabled and that having this process in place where privacy interests are taken into consideration "gives privacy rights the appropriate weight and is consistent with international trends."[313] Mr. Israel[314] and Ms. McPhail said that consultation with the Commissioner should be done for both government and international legal agreements:

> Whether it's a multilateral treaty, a trade agreement, a new piece of legislation, or a new data processing system, there should always be at some appropriate level consideration of what the risks are going to be to people's privacy, and of course, a number of other factors.[315]

Based on the Commissioner's role as an Officer of Parliament and the fundamental nature of the right to privacy, Ms. Bernier supported the Commissioner's recommendation: "Because of this status, and the fact that privacy has been entrusted to an institution with this status, it is completely logical that the Commissioner be consulted about legislation or regulations prior to their being tabled, to ensure they are privacy-compliant."[316]

From a practical perspective, Mr. Murray pointed out the effectiveness of Newfoundland and Labrador's new provision requiring government institutions to consult the Commissioner before tabling draft legislation:

> We have been consulted a number of times since June 2015, when the ATIP of 2015 came in. We have provided input on draft bills and had an impact on the bill that was eventually tabled in the House of Assembly for debate.

---

308 ETHI, Evidence, 1st Session, 42nd Parliament, 1 November 2016, 1200 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

309 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1110 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

310 Ibid., 1205 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

311 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1105 1205 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

312 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

313 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1110 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

314 Ibid., 1205 (Mr. Tamir Israel, Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

315 Ibid., 1210 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

316 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1105 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

> Prior to that, there was an ad hoc occasional practice of consulting the commissioner's office. It was unsatisfactory because there were times when bills went before the House that we had not had notice of and were not aware of and that had a significant impact on privacy and access to information. There was a lost opportunity, then, to have that input.[317]

On the other hand, Mr. Dickson supports the "practice of advance consultation but questions whether it is appropriate to be a statutory requirement."[318] He noted that Treasury Board's *Policy on Privacy Protection* includes the following requirement:

> 6.2.12 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.[319]

Mr. Dickson noted that the Commissioner's recommendation could pose some problems:

> We absolutely agree with the importance of early consultation, but we question whether it's realistic to make it a condition precedent to a bill's first reading. My experience as a House leader in the official opposition of a provincial legislature is that from time to time bills have to be introduced on short notice. It may be the end of a session or it may be that bills need to be introduced quickly, not to shorten and abridge the period for consideration but in fact to allow for ample consultation. In most cases it would be absolutely appropriate to have prior notice, but I can imagine cases in which it might not be useful or realistic to have a statutory requirement for prior notice.[320]

3.6.3 The Committee's recommendation

The Committee recommends:

RECOMMENDATION 18

That the *Privacy Act* be amended to require federal government institutions to consult with Office of the Privacy Commissioner of Canada on draft legislation and regulations with privacy implications before they are implemented.

---

317 ETHI, Evidence, 1st Session, 42nd Parliament, 4 October 2016, 1115 (Mr. Sean Murray, Executive Director, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

318 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

319 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1125 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

320 Ibid.

3.7 Provide the Office of the Privacy Commissioner with an explicit public education and research mandate

3.7.1 The Privacy Commissioner's view

The Commissioner made a recommendation to the Committee that "the Commissioner be given express authority under the *Privacy Act* to conduct, on his own initiative, research and studies on issues of public importance"[321] and that the *Privacy Act* "should expressly authorise the Commissioner to engage in public education and awareness activities."[322]

The Commissioner noted that the *Privacy Act* does not provide him with an explicit public education and research mandate: "As a consequence, the Office lacks an explicit legislative authority to work proactively on outreach and education efforts tied to public sector issues."[323] However, the Commissioner has such a mandate under the PIPEDA and has carried out research and education for over a decade.[324] According to the Commissioner, adopting this recommendation "would align his mandate with respect to research and education with his current mandate under PIPEDA and otherwise advance the purposes of the *Privacy Act*."[325]

3.7.2 Witnesses' views

Mr. Drapeau disagreed with the Commissioner's recommendation. He does not believe that public education is necessary given that the *Privacy Act* is not a complex piece of legislation and that its breadth and reach are limited.[326] Mr. Drapeau noted that adding an education mandate to the *Privacy Act* "would lead to a substantial increase to an already large bureaucracy at the OPC."[327] Lastly, Mr. Drapeau argued that "the role of public education and research, if required, should be left to the universities and research organizations or bar associations."[328]

However, many witnesses, including Mr. Rubin,[329] Mr. Fraser,[330] Mr. Israel,[331] Mr.Bennett,[332] Mr. Geist,[333] Mr. Karanicolas,[334] Ms. Tully,[335] Mr. Molloy,[336] BC FIPA[337]

---

321 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

322 Ibid.

323 Ibid.

324 Ibid.

325 Ibid.

326 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1115 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Common Law, As an Individual).

327 Ibid.

328 Ibid.

329 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1230 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

330 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1100 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual)

and the CBA[338] supported the Commissioner's recommendation and stressed the importance of an education, awareness and research mandate for the Commissioner. Mr. Karanicolas noted:

> It's about a gap in understanding among Canadians about what privacy is and about the changes that have occurred as a result of digitization, which have dramatically changed people's relationship with personal information. It's about giving the Privacy Commissioner a stronger role in promoting privacy.[339]

Mr. Lyon said there is a need for education, especially in the area of national security and domestic life, and that "this too could be coordinated by the Privacy Commissioner with an expanded brief."[340] Mr. Bennett said the Commissioner's recommendation is not controversial and would formalize the practice:

> The Privacy Commissioner has a very effective contributions program and gives out money for research, which is very valuable in terms of finding out about new technologies and new practices. That is done for public and for private sector issues, so it's very much a question of formalizing what has become the practice of the office over the last 10, 15 years.[341]

With regard to research, Mr. Keenan said there is a need for research in the privacy sector: "I'll say fund more research. The Privacy Commissioner does some already, but could a lot more."[342]

---

331 Ibid., 1230 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

332 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1235 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

333 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1105 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

334 ETHI, Evidence, 1st Session, 42nd Parliament, 20 October 2016, 1140 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

335 ETHI, Evidence, 1st Session, 42nd Parliament, 4 October 2016, 1145 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

336 Ibid., 1105 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

337 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

338 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

339 ETHI, Evidence, 1st Session, 42nd Parliament, 20 October 2016, 1140 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

340 ETHI, Evidence, 1st Session, 42nd Parliament, 14 June 2016, 0910 (Mr. David Lyon, Professor, Queen's University, As an Individual).

341 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1235 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

342 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1200 (Mr. Thomas Keenan, Professor, University of Calgary, As an Individual).

3.7.3 The Committee's recommendation

The Committee believes that, because of constantly changing technology, public education and awareness activities and research are essential to achieve the *Privacy Act*'s purpose. The Committee supports the Commissioner's recommendation and therefore recommends:

RECOMMENDATION 19

That the *Privacy Act* be amended to explicitly confer the Privacy Commissioner with:

a) the authority to conduct, on his own initiative, research and studies on issues of public importance, and

b) a mandate to undertake public education and awareness activities.

3.8 Require an ongoing five-year review of the *Privacy Act*

The Commissioner recommended that "the *Privacy Act* be amended to require a mandatory parliamentary review every five years."[343] He stressed that this recommendation is important to ensure that the *Privacy Act* never again becomes "a badly out-of-date law in the future."[344]

Mr. Keenan,[345] Mr. Dickson,[346] Mr. Karanicolas[347] and BC FIPA[348] supported the Commissioner's recommendation.

Mr. Drapeau believes, however, that a five-year review of the *Privacy Act* is too frequent, and recommends reviewing it every 10 years instead.[349] On the other hand, Mr. Dickson believes that a five-year review is the best option:

> I think five years is appropriate, though, because it not only lines up with a number of Canadian provinces that provide for that statutory review but also ensures that this kind of material doesn't get forgotten. If you rely on a department of justice, or some other department, doing an internal review, it just doesn't attract that kind of attention.…

343 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

344 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 March 2016, 0845 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

345 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1120 (Mr. Thomas Keenan, Professor, University of Calgary, As an Individual).

346 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1215 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

347 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1130 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

348 BC Freedom of Information and Privacy Association, Reform of the *Privacy Act*: Past Time for Action, October 2016, brief submitted to the Committee.

349 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1115 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Common Law, As an Individual).

> We certainly value the notion of more public reviews done on a regular basis. If there hasn't been a lot of change, then there may be no need for huge amendment. However, it ensures that in a world where technology is changing and so many new risks to privacy keep on developing and appearing, there is an attempt to stay current.[350]

According to BC FIPA, "[i]f a five year mandatory review had been included in the original *Privacy Act*, it is extremely doubtful that it would have been allowed to deteriorate to the extent it has."[351]

Mr. Dickson pointed out, however, that a parliamentary review does not guarantee that the recommendations of the parliamentarians responsible for reviewing the Act will be implemented.[352]

Given that technology is constantly evolving and that it may pose risks for the protection of privacy, the Committee is of the opinion that amending the *Privacy Act* to require a five-year review is important for ensuring that the Act remains up to date and able to effectively protect Canadians' privacy. The Committee supports the Commissioner's recommendation and therefore recommends:

RECOMMENDATION 20

That the *Privacy Act* be amended to require an ongoing five-year parliamentary review.

CHAPTER 4: ENHANCE TRANSPARENCY

4.1 Grant the Privacy Commissioner discretion to publicly report on government privacy issues when in the public interest

4.1.1 The Privacy Commissioner's view

The Commissioner made a recommendation that "section 64 [of the *Privacy Act*] be amended to create an exemption from confidentiality requirements to provide the Privacy Commissioner with the discretionary authority to report proactively on government privacy issues where he considers it in the public interest to do so."[353]

Currently, sections 63 through 65 of the *Privacy Act* set out confidentiality requirements "prohibiting the Commissioner from publicly disclosing information related to

---

350 Ibid., 1215 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

351 BC Freedom of Information and Privacy Association, Reform of the *Privacy Act*: Past Time for Action, October 2016, brief submitted to the Committee.

352 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1215 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

353 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016; ETHI, Evidence, 1st Session, 42nd Parliament, 10 March 2016, 0845 and 1005 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

investigations and reviews, other than in our annual or special reports to Parliament."[354] While the Commissioner, as an ombudsman, recognizes the importance of confidential investigations, he believes in some cases "it would be in the public interest for the Commissioner to make his findings public."[355] The Commissioner notes that "there should be some allowance made for limited exceptions, on grounds of public interest, as in PIPEDA."[356]

The goal of the Commissioner's recommendation is to "inform parliamentary debate and public discussions in a timely way"[357] and allow the Commissioner to "make [findings] public in a less formal way"[358] than through special reports. Moreover, this discretionary authority "would allow for more timely and relevant disclosure rather than having to wait until the end of the reporting year when the information may have become moot, stale or largely irrelevant."[359]

In his appearance, the Commissioner said that if his recommendation were implemented by government, he would exercise this authority in the same way he does under the PIPEDA:

> We have experience with this under PIPEDA, […] I have discretion to make public findings and recommendations outside of the context of an annual report. […] We issue case reports, give documents to practitioners, to experts, which is helpful to them and helpful to companies in changing their behaviour or adapting to what we say. I think that if we had similar authority to do that for the public sector, outside of the context of annual reports, this would be helpful to departments as well as providing guidance during the year.[360]

Lastly, as to when he would use this authority and the potential impact of disclosing his findings in an election period, the Commissioner said that his office acts independently but responsibly: "We would certainly have regard, from the timing perspective, for the impact of our release of findings so as not to advantage any one party or the other, but on the contrary, to ensure that the publication of the finding does not influence what would otherwise be the considerations, say, in an election period."[361]

---

354 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

355 Ibid.

356 Ibid.

357 Ibid.

358 ETHI, Evidence, 1st Session, 42nd Parliament, 1 November 2016, 1200 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

359 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

360 ETHI, Evidence, 1st Session, 42nd Parliament, 1 November 2016, 1200 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

361 Ibid.

4.1.2 Witnesses' views

Mr. Fraser,[362] Mr. Geist,[363] Ms. Bernier,[364] BC FIPA[365] and the CBA[366] supported the Commissioner's recommendation and believe it would promote government transparency in its use of personal information.

Ms. Bernier, former Interim Privacy Commissioner, said that the constraint of having to publish findings having a significant impact on Canadians in annual or special reports only is a "hindrance to transparency, for no use."[367] She illustrated her concerns with the following example from her time as interim Commissioner:

> I was confronted with this when we finished the investigation of, as it was then, Employment and Social Development Canada. You will recall that it lost a hard drive of 583,000 Canadians' financial information. It was just too big, I felt, to leave it to the annual report. I thought that the Canadian public deserved a quicker result of our investigation, and therefore, proceeded by tabling a special report.
>
> But it is quite stilted and onerous. It is demonstrating a lack of flexibility. I was wanting to serve the Canadian public well by stating the results of our investigation, but I could only do it through the special report procedure.[368]

According to Mr. Geist, the Commissioner's recommendation makes sense in order to keep pace with technology:

> In our current 24-hour, social-media-driven news cycle, restrictions on the ability to disseminate information, particularly information that can touch on the privacy of millions of Canadians, can't be permitted to remain outside of the public eye and left for annual reports when they are tabled. Where the commissioner deems doing so to be in the public interest, the office must surely have the power to disclose in a timely manner.[369]

Mr. Fraser said that summaries of some notable cases in the Commissioner's annual reports are insufficient to educate the public and that in adopting this recommendation, "[t]ransparency [...] would be significantly served."[370] BC FIPA said that a new provision giving the Commissioner discretionary authority "would mirror the

---

362 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1100 and 1105 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

363 Ibid., 1105 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

364 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1240 and 1245 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

365 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

366 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

367 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1245 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

368 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1240 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

369 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1105 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

370 Ibid., 1100 and 1105 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

proposed creation of a general public interest override in the [*Access to Information Act*], and it would allow the Commissioner to better serve the public interest."[371] Lastly, while the CBA supports the Commissioner's recommendation, it believes that this new authority is likely to have limited impact given that the "current reporting obligations for federal institutions leave much to be desired, particularly where a federal institution has experienced a privacy breach and personal information has been inadvertently or improperly disclosed."[372]

In his appearance before the Committee, RCMP Assistant Commissioner Oliver expressed some concerns about adopting this recommendation:

> I hope that if that recommendation is adopted, it won't weaken section 62 [of the *Privacy Act*], which relates to the security requirements, or section 65 [of the *Privacy Act*], which relates to the protection of sensitive capabilities, such as investigative techniques, and those types of things.
>
> These are some areas, possibly impeding our ability to deliver our mandate, in which disclosure of certain information could compromise the identity of human sources or the identity of people in witness protection. It could compromise sensitive investigative techniques that we try to protect so that criminal organizations or terrorists do not modify their behaviours to avoid detection or put in place countermeasures to avoid those things. We'd be looking to maintain the protection of that type of information.[373]

4.1.3 The Committee's recommendation

In light of the testimony heard, the Committee believes that the Commissioner's recommendation would strengthen transparency and therefore recommends:

RECOMMENDATION 21

That section 64 of the *Privacy Act* be amended to create an exemption from confidentiality requirements to provide the Privacy Commissioner with the discretionary authority to report proactively on government privacy issues where he considers it in the public interest to do so.

4.2 Share information with the Privacy Commissioner's counterparts domestically and internationally

4.2.1 The Privacy Commissioner's view

The Commissioner recommended, "expanding the ability of the OPC to collaborate with other data protection authorities and review bodies on audits and investigations of

---

371 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

372 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

373 ETHI, Evidence, 1st Session, 42nd Parliament, 25 October 2016, 1145 (Assistant Commissioner Joe Oliver, Technical Operations, Royal Canadian Mounted Police).

shared concern in connection with *Privacy Act* issues."[374] The Commissioner said he was given this authority in connection with investigations and public education work under PIPEDA: "Our enforcement actions abroad have become much more timely and effective owing to this new ability to work cooperatively with other authorities."[375]

4.2.2 Witnesses' views

BC FIPA,[376] the CBA[377] and Mr. Karanicolas[378] supported the Commissioner's recommendation. Mr. Dickson from the CBA said that the Commissioner's recommendation is "frankly all about trying to coordinate enforcement to address the problems with data flowing outside the territorial borders of Canada."[379] Mr. Dickson added that the recommendation protects Canadians by "ensuring that data protection authorities can look at joint investigations."[380] Mr. Karanicolas demonstrated the importance of this recommendation:

> The Internet poses a significant challenge to traditional understandings of borders and jurisdiction, which makes it difficult to safeguard rights online. When a guy in Saudi Arabia, a country where adultery is a criminal offence, has his Ashley Madison profile leaked due to negligent safeguards by that company, where does his remedy lie?
>
> […] There are very serious international consequences to these kinds of leaks. The Internet is a borderless place, and any agency that seeks to protect the rights of Canadians online needs to coordinate internationally.[381]

4.2.3 The Committee's recommendation

The Committee believes that the Commissioner's recommendation protects the privacy of Canadians and supports his recommendation. The Committee therefore recommends:

RECOMMENDATION 22

That the *Privacy Act* be amended to expand the ability of the Office of the Privacy Commissioner of Canada to collaborate with other data

---

374 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

375 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016; Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, s. 23.

376 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

377 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

378 ETHI, Evidence, 1st Session, 42nd Parliament, 20 October 2016, 1100 et 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

379 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1215 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

380 Ibid.

381 ETHI, Evidence, 1st Session, 42nd Parliament, 20 October 2016, 1100 and 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

protection authorities and review bodies on audits and investigations of shared concern in connection with *Privacy Act* issues.

4.3 Discretion to discontinue or decline complaints

4.3.1 The Privacy Commissioner's view

The Commissioner recommended "amending section 32 of the *[Privacy] Act* to permit the Commissioner to exercise discretion in discontinuing or refusing complaints on specific grounds, including where a complaint is frivolous, vexatious or made in bad faith."[382] The Commissioner said his recommendation is consistent with "a context of finite resources, and where Canadians deserve efficient and effective oversight that is seized with issues of systemic interest and of the greatest significance to them."[383]

Currently, the Commissioner is required to investigate every complaint received.[384] The Commissioner pointed out in his brief that the PIPEDA as well as several provincial laws, including Alberta's, "have given their Information and Privacy Commissioners discretion to refuse to investigate or conduct an inquiry on legitimate grounds."[385]

The Commissioner said he used the expression "including where a complaint is frivolous, vexatious or made in bad faith" in his recommendation because the PIPEDA includes other grounds for refusal,[386] for instance where there may be another effective remedy available to the individual, where the Commissioner has before him another complaint that raises the same issue,[387] where "there's insufficient evidence to pursue the investigation,"[388] where the organization "has already provided a fair and reasonable response to the individual" or where the "matter has already been the subject of a report by the commissioner and a recurring issue has already been dealt with."[389]

Lastly, the Commissioner said that judicial review would be an appropriate remedy if a complainant is dissatisfied with the Commissioner's decision to discontinue or decline a complaint filed under the *Privacy Act*.[390]

---

382 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

383 Ibid.

384 *Privacy Act,* s.29.

385 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

386 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, s. 12.2.

387 ETHI, Evidence, 1st Session, 42nd Parliament, 1 November 2016, 1140 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

388 Ibid., 1140 (Ms. Patricia Kosseim (Senior General Counsel and Director General, Legal Services, Policy, Research and Technology Analysis Branch, Office of the Privacy Commissioner of Canada).

389 Ibid.

390 Ibid., 1140 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

4.3.2 Witnesses' views

Mr. Bennett[391], Mr. Fraser,[392] Mr. Gogolek[393] and the CBA[394] supported the Commissioner's recommendation.

The CBA reiterated its recommendation of 2012 to the federal government to give the Commissioner "discretion to decline complaints or discontinue investigations based on certain criteria, for example those that are trivial, frivolous, vexatious, made in bad faith, supported by insufficient evidence, have been dealt with already by the Commissioner or are better resolved in a different forum."[395] Moreover, Mr. Gogolek said that this recommendation was understandable and "necessary for the economy of public resources in cases where there is a request or a demand for review that is frivolous, vexatious, or done in bad faith,"[396] but stressed "it should be restricted to those narrow points."[397]

Mr. Fraser highlighted the importance of the Commissioner's recommendation but said one "would want to institute it with the appropriate checks and balances and possible judicial review, because cutting somebody off from redress under the *Privacy Act* is a pretty significant step given its quasi-constitutional status in Canada."[398] Mr. Gogolek also emphasized that individuals should be able to appeal the Commissioner's decision not to investigate.[399] Mr. Bennett said that British Columbia, in order to deal with frivolous and vexatious complaints, allows any one person to have only three active complaints at one time.[400]

Mr. Fraser, however, said that this measure was "probably too blunt an instrument since every case stands on its own."[401] He suggested there was no need to reinvent the wheel, as the "courts have developed a meaningful test for what is a vexatious litigant" and the test "always does take into account the nuances and the circumstances."[402]

---

391 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1235 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

392 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1215 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

393 ETHI, Evidence, 1st Session, 42nd Parliament, 20 October 2016, 1115 and 1210 (Mr. Vincent Gogolek, Executive Director, BC Freedom of Information and Privacy Association).

394 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

395 Ibid.

396 ETHI, Evidence, 1st Session, 42nd Parliament, 20 October 2016, 1115 and 1210 (Mr. Vincent Gogolek, Executive Director, BC Freedom of Information and Privacy Association).

397 Ibid.

398 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1215 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

399 ETHI, Evidence, 1st Session, 42nd Parliament, 20 October 2016, 1210 (Mr. Vincent Gogolek, Executive Director, BC Freedom of Information and Privacy Association).

400 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1235 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

401 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1215 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

402 Ibid.

For his part, Mr. Drapeau opposed the Commissioner's recommendation because of the quasi-constitutional nature of the rights under the *Privacy Act* and because it would deprive the complainant of "any possible remedy before the court."[403]

4.3.3 The Committee's recommendation

The Committee supports the Commissioner's recommendation and therefore recommends:

RECOMMENDATION 23

That section 32 of the *Privacy Act* be amended to grant the Privacy Commissioner discretion to discontinue or decline complaints on specified grounds, including when the complaint is frivolous, vexatious or made in bad faith, and that the Commissioner's decision to discontinue or decline a complaint be subject to a right of appeal by the complainant.

4.4 Strengthen transparency reporting requirements for government institutions

4.4.1 The Privacy Commissioner's view

The Commissioner recommended that the government "[s]trengthen reporting requirements on broader privacy issues dealt with by federal organizations as well as specific transparency requirements for lawful access requests made by agencies involved in law enforcement."[404]

The Commissioner indicated that departments publish annual reports pursuant to section 72 of the *Privacy Act.* The Commissioner commented, however, that "for the lay reader, these annual transparency measures typically comprise an elaborate collage of statistics on the number of personal information requests received and processed in a year – with little or no explanation [sic] what the figures mean."[405] The Commissioner maintains that, "in order for these reports to be meaningful and useful to the public, they need to be rendered intelligible."[406]

The Commissioner's office "has recently called upon federal organizations to be open about the number, frequency and type of lawful access requests they make to internet service providers and other private sector organizations entrusted with customer

403 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1115 and 1230 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Common Law, As an Individual).

404 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

405 Ibid.

406 Ibid.

communications data."[407] According to the Commissioner, more openness is required on this front.[408]

4.4.2 Witnesses' views

Ms. McPhail,[409] Mr. Karanicolas,[410] the CBA[411] and the BC FIPA[412] support the Commissioner's recommendation. For Mr. Karanicolas, "rather than setting specific standards in the act, we would suggest leaving the specific scope of that to either the Privacy Commissioner or the Information Commissioner, to be defined through their regulations. That is in order to allow them to deal with emerging issues as they arise without having to reform the law."[413]

Ms. McPhail[414] and Mr. Geist[415] maintained that access to information pertaining to lawful access requests is extremely important for transparency.

4.4.3 The Committee's recommendation

The Committee believes that it is important to strengthen transparency reporting requirements for federal institutions. In the same vein, the public should have access to information regarding federal institutions' administration of the *Privacy Act* that is accessible and relevant. The Committee supports the Commissioner's recommendation and recommends:

RECOMMENDATION 24

That reporting requirements on broader privacy issues dealt with by federal institutions be reinforced by requiring the addition of a descriptive element so as to make the information in the reports accessible and relevant.

RECOMMENDATION 25

That there be specific transparency requirements for lawful access requests from agencies involved in law enforcement.

---

407 Ibid.

408 Ibid.

409 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

410 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

411 Canadian Bar Association, *Privacy Act* Amendments, September 2016, brief submitted to the Committee.

412 BC Freedom of Information and Privacy Association, Reform of the *Privacy Act*: Past Time for Action, October 2016, brief submitted to the Committee.

413 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

414 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1105 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

415 Ibid., 1140 (Mr. Michael Geist, Canada Research Chair in Internet and E-Commerce Law, University of Ottawa, As an Individual).

4.5 Extend coverage of the *Privacy Act*

The Commissioner made a recommendation to "[a]mend the [Privacy] Act to extend coverage to all government institutions, including Ministers' Offices and the Prime Minister's Office, and extend rights of access to foreign nationals."[416]

4.5.1 Scope of the *Privacy Act*

4.5.1.1 The Privacy Commissioner's view

Currently, the *Privacy Act* "applies exclusively to those government institutions listed in Schedule 1 of the Act or those added in the definitions section (e.g. Crown corporations)."[417] According to the Commissioner, "individuals should be able to access their personal information and challenge its accuracy regardless of where it is within government."[418]

Given that the *Access to Information Act* and the *Privacy Act* form a seamless code, the Commissioner argued: "If you amend the right of access or the exceptions in one act, normally you should do the same, or certainly you should consider whether to do the same, in both pieces of legislation. […] This would deserve some thinking and consideration, but I am inclined to think that if coverage is extended in one piece of legislation, it might not work very well if the same decision is not made for the other Act."[419]

Moreover, the Commissioner said that his recommendation aims to extend coverage of the *Privacy Act* to all government institutions and the entire executive branch, including ministers' offices and the Prime Minister's Office (PMO).[420] The Commissioner explained his recommendation as follows:

> There is personal information held in ministers' offices and the PMO that is extremely relevant to service delivery and how rights are delivered.
>
> Many statutes provide statutory responsibilities to ministers, who then delegate them in the bureaucracy. A lot of the information that relates to these questions is in the bureaucracy, and that's currently accessible. But ultimately it's the minister who's responsible to make these determinations, and in some cases the ministers personally do make these decisions. It shouldn't matter whether the information rests in the bureaucracy or in a minister's office if it's the same kind of information that can potentially be used for the same statutory purposes.[421]

---

416 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

417 Ibid.

418 Ibid.

419 ETHI, Evidence, 1st Session, 42nd Parliament, 10 March 2016, 0850 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

420 Ibid., 0910 and 0925.

421 Ibid., 0925.

4.5.1.2 Witnesses' views

Mr. Rubin,[422] Ms. McPhail,[423] Mr. Fraser,[424] Mr. Bennett,[425] Mr. Geist,[426] Ms. Bernier,[427] BC FIPA[428] and the CBA[429] supported the Commissioner's recommendation.

Ms. Bernier said that "there is personal information held or could be held in these offices that is not currently protected. When you look at the fact that the government in power, the ministers, the Prime Minister, do exercise the powers of government, they should be held to the standards of the *Privacy Act* to collect, use, or disclose that information."[430] In the same vein, Ms. McPhail said that "at all levels of government and at all levels of power Canadians have the right to know that information is being collected and held safely and well and of the concurrent right to make requests under other acts for the information."[431] Similarly, Mr. Geist explained the importance of bringing ministers' offices under the purview of the *Privacy Act*:

> [D]ecision-making and policy development now occur not just in the department. They quite clearly occur very often in the ministerial offices, so from my perspective, having an understanding of those processes and ensuring that they are subject to the same kind of transparency and openness requirements is important. That means ensuring that the *Access to Information Act* covers it, but I think it also means that the *Privacy Act* does as well.[432]

Ms. Tully[433], Mr. Molloy[434] and Mr. McArthur[435] said that their province's legislation applies to the premier's office and ministers' offices.

---

422 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1125 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

423 Ibid., 1205 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

424 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1150 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

425 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1150 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

426 Ibid., 1150 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

427 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1240 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

428 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

429 Canadian Bar Association, Privacy Act Amendments, September 2016, brief submitted to the Committee.

430 ETHI, Evidence, 1st Session, 42nd Parliament, 6 October 2016, 1240 (Ms. Chantal Bernier, Counsel, Privacy and Cybersecurity, Dentons Canada).

431 ETHI, Evidence, 1st Session, 42nd Parliament, 20 September 2016, 1205 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

432 ETHI, Evidence, 1st Session, 42nd Parliament, 29 September 2016, 1150 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

433 ETHI, Evidence, 1st Session, 42nd Parliament, 4 October 2016, 1220 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

434 Ibid., 1220 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

In addition, BC FIPA demonstrated the importance of the Commissioner's recommendation by drawing the Committee's attention to the OPC investigation of the case involving Sean Bruyea, whose personal information held by a federal institution was included in ministerial briefing notes.[436]

4.5.1.3 The Committee's recommendation

The Committee recommends:

RECOMMENDATION 26

That the Government of Canada explore extending the scope of the *Privacy Act* to all federal government institutions, including ministers' offices and the Prime Minister's Office.

4.5.2 Right of access to personal information

4.5.2.1 The Privacy Commissioner's view

The Commissioner pointed out that the *Privacy Act* currently "only affords access rights to Canadian citizens, permanent residents or persons physically present in Canada."[437] However, the Commissioner said that,

> Federal government departments hold vast amounts of personal information about non-citizens, owing both to global travel, migration and commercial activities. Foreign nationals, such as those seeking to immigrate to Canada, who want access to their personal information, often have to do so by having an agent make an *Access to Information Act* request, and consenting to the release of their personal information.[438]

In his brief, the Commissioner referred to the Information Commissioner's Special Report to Parliament, which notes:

> Among the provinces and territories, Commonwealth countries, the U.S., in model laws, and those jurisdictions with access legislation ranked in the top 10 on the Global Right to Information Rating, only Canada, New Zealand and India limit who may have access to government information. All of the other jurisdictions reviewed provide a universal right of access and none have indicated that the universal right has resulted in an unmanageable amount of requests. A broadened right of access has also been recommended on numerous occasions in Canada in the past.[439]

---

435 Ibid., 1220 (Mr. Drew McArthur (Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia).

436 BC Freedom of Information and Privacy Association, Reform of the Privacy Act: Past time for Action, October 2016, brief submitted to the Committee.

437 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016.

438 Ibid.

439 Office of the Privacy Commissioner of Canada, Advice to Parliament, Privacy Act Reform in an Era of Change and Transparency, 22 March 2016; Office of the Information Commissioner of Canada, Striking the Right Balance for Transparency–Recommendations to modernize the Access to Information Act, March 2015.

4.5.2.2 Witnesses' views

Mr. Drapeau opposed the Commissioner's recommendation given, in his opinion, the OPC's already long complaints process and the inadvisability of extending coverage of the *Privacy Act* to foreign nationals before the service for Canadians is optimal.[440] In his testimony, Minister Brison said that before extending coverage to foreign nationals, he thought the focus would be on improving response times for Canadian citizens.[441]

Moreover, the IRCC said that the Commissioner's recommendation "could have a significant operational impact"[442] on their work:

> Currently, foreign nationals and those outside of Canada can obtain access to their personal information by hiring a Canadian representative and filing a request under the *Access to Information Act*. […]
>
> The Privacy Commissioner has recommended that foreign nationals and those outside Canada should be able to submit a request for their personal information under the Act. Our concern with this proposal is that, because of IRCC's lines of business and international mandate, the proposed recommendation could lead to an enormous increase in privacy requests that would place an undue burden on our resources and create considerable operational constraints. This could seriously compromise our ability to meet the deadlines for responding to requests as set out in the Act.[443]

The RCMP,[444] CSIS[445] and the CBSA[446] said they would have similar concerns to those of the IRCC if the *Privacy Act* was extended to foreign nationals.

Sue Lajoie from the OPC said it's unclear "how many additional requests opening the *Privacy Act* to a broader audience would change"[447] in the case of the IRCC. The Commissioner said that, with respect to the IRCC, "to give foreign nationals a right of access under the *Privacy Act* wouldn't deal directly with what currently occurs indirectly when you have foreign nationals making access requests through agents under the *Access to Information Act*."[448]

---

440 ETHI, Evidence, 1st Session, 42nd Parliament, 27 September 2016, 1115 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Common Law, As an Individual).

441 ETHI, *Evidence*, 1st Session, 42nd Parliament, 24 November 2016, 1120 (Hon. Scott Brison, President of the Treasury Board).

442 ETHI, Evidence, 1st Session, 42nd Parliament, 25 October 2016, 1135 (Ms. Stefanie Beck (Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration).

443 Ibid.

444 Ibid., 1220 (Ms. Rennie Marcoux, Chief Strategic Policy and Planning Officer, Royal Canadian Mounted Police).

445 Ibid., 1220 (Mr. Michael Peirce (Assistant Director Intelligence, Canadian Security Intelligence Service).

446 Ibid., 1220 (Mr. Robert Mundie, Director General, Corporate Secretariat, Canada Border Services Agency).

447 ETHI, Evidence, 1st Session, 42nd Parliament, 1 November 2016, 1110 (Ms. Sue Lajoie, Director General, Privacy Act Investigations, Office of the Privacy Commissioner of Canada).

448 Ibid., 1110 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

4.5.2.3 The Committee's recommendation

In light of the testimony heard, the Committee recommends:

RECOMMENDATION 27

That the Government of Canada consider extending the right of access to personal information to foreign nationals.

4.6 Exemptions to personal information access requests

In his brief, the Commissioner indicated that he favours, "maximizing disclosure where an individual seeks access to their personal information."[449] For this, the Commissioner recommends "limiting exemptions to access to personal information requests, severing protected information wherever possible, and ensuring such exemptions are generally injury-based and discretionary, where appropriate."[450]

Nevertheless, the Commissioner did say that he disagrees with the recommendation of the Information Commissioner to amend the exemption for personal information provided for in section 19 of the *Access to Information Act* "to allow disclosure of personal information in circumstances in which there would be no unjustified invasion of privacy."[451] The Privacy Commissioner does not recommend that "the exemption from access concerning the personal information about another individual be narrowed."[452] He explains his recommendation as follows:

> The exemption currently applies to all personal information regardless of whether disclosure would constitute an unjustified invasion of privacy. This protects the privacy rights of third party individuals, in keeping with Canadian jurisprudence that has stressed the importance of privacy, even over access.[453] Moreover, the *Privacy Act* already permits the disclosure of personal information where, in the opinion of the head of the institution, the public interest clearly outweighs any invasion of privacy.[454] This public interest override strikes the right balance between privacy and access.[455]

The Commissioner called on the Committee to consider the *Access to Information Act* and the *Privacy Act* as seamless codes: "Changes to the way in which access and

449 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

450 Ibid.

451 Office of the Information Commissioner of Canada, Striking the Right Balance for Transparency – Recommendations to modernize the *Access to Information Act*, March 2015.

452 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

453 *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403.

454 *Privacy Act*, s. 8(2)(m).

455 Office of the Privacy Commissioner of Canada, Advice to Parliament, *Privacy Act* Reform in an Era of Change and Transparency, 22 March 2016.

privacy rights are balanced under the current legislation should be carefully thought through."[456]

Mr. Rubin[457] and Mr. Israel[458] supported the Commissioner's recommendation.

The CBA was unable to achieve a consensus position on the Commissioner's recommendation.[459]

Mr. Gogolek said he is in favour of the Information Commissioner's recommendation: "We have for a long time been in favour of exceptions to release under the ATIA [*Access to Information Act*] being harms-based, and that would include personal information. We are also not in favour of this being discretionary.[460]

Similarly, Mr. Karanicolas disagrees with the Privacy Commissioner:

> CLD [Centre for Law and Democracy] strongly supports the OIC's [Information Commissioner] position in narrowing the definition.
>
> The first reason is that there are enormous amounts of personal information whose disclosure is not sensitive – for example, where the information is already broadly publicly available – and as a consequence there would be no material harm in its disclosure. A harm test, which is what we're advocating, clarifies that information should always be disclosed in these kinds of cases. This prevents undue delays in processing requests and is a core earmark of good access to information legislation.
>
> Second, in its submission the OPC [Office of the Privacy Commissioner] has advocated for a formula that inherently tilts the scales in favour of privacy by requiring that a public interest override to have the information disclosed would only kick in if the interest in disclosure would clearly outweigh the privacy interest. This is an incorrect approach. The right to information is a human right, is broadly recognized internationally, and is also recognized as a limited and derivative constitutional right. It should be balanced against the right to privacy on equal terms.[461]

RECOMMENDATION 28

That the Government of Canada examine the possibility of limiting exemptions to access to personal information requests under the *Privacy Act*.

---

456 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2016, 1105 (Mr. Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

457 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1125 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

458 Ibid., 1140 (Mr. Tamir Israel, Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic).

459 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1125 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

460 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1115 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

461 Ibid., 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

LIST OF RECOMMENDATIONS

APPENDIX A

REVIEW OF THE *PRIVACY ACT* – REVISED RECOMMENDATIONS OF THE PRIVACY COMMISSIONER OF CANADA

THEME ONE: TECHNOLOGICAL CHANGES

1. Clarify requirements for information-sharing agreements: Require that all information sharing under paragraphs 8(2)(a) and (f) of the *Privacy Act* be governed by written agreements and that these agreements include specified elements. Further, all new or amended agreements should be submitted to the Office of the Privacy Commissioner of Canada (OPC) for review, and existing agreements should be reviewable upon request. Finally, departments should be required to be transparent about the existence of these agreements.

2. Create a legal obligation for government institutions to safeguard personal information: Create an explicit requirement for institutions to safeguard personal information with appropriate physical, organizational and technological measures commensurate with the level of sensitivity of the data;

3. Make breach reporting mandatory: Create an explicit requirement for government institutions to report material breaches of personal information to the OPC in a timely manner and to notify affected individuals in appropriate cases;

THEME TWO: LEGISLATIVE MODERNIZATION

4. Create an explicit necessity requirement for collection: Amend section 4 of the Privacy Act to create a more explicit necessity requirement for the collection of personal information, consistent with other privacy laws in Canada and abroad;

5. Replace the ombudsman model for the investigation of complaints with OPC powers to issue binding orders;

6. Consider creating a statutory mechanism to independently review privacy complaints against the OPC;

7. Require government institutions to conduct privacy impact assessments (PIAs) for new or significantly amended programs and submit them to OPC prior to implementation;

8. Require government institutions to consult with OPC on draft legislation and regulations with privacy implications before they are tabled;

9. Provide OPC with an explicit public education and research mandate: Add a provision to the *Privacy Act* explicitly conferring the Privacy Commissioner with a mandate to undertake public education and research activities in respect of public sector privacy issues;

10. Require an ongoing five year review of the Act;

THEME 3: ENHANCING TRANSPARENCY

11. Grant the Privacy Commissioner discretion to publicly report on government privacy issues when in the public interest: Amend section 64 of the Act to create an exemption from confidentiality requirements to allow the Privacy Commissioner to report publicly on government privacy issues where he considers it in the public interest to do so;

12. Expand the Commissioner's ability to share information with counterparts domestically and internationally to facilitate enforcement collaboration;

13. Provide the Privacy Commissioner with discretion to discontinue or decline complaints in specified circumstances: Amend section 32 of the Act to grant the Commissioner with discretion to decline complaints or discontinue investigations on specified grounds, including when the complaint is frivolous, vexatious or made in bad faith**;**

14. Strengthen transparency reporting requirements for government institutions: Strengthen reporting requirements on broader privacy issues dealt with by federal organizations as well as specific transparency requirements for lawful access requests made by agencies involved in law enforcement;

15. Extend coverage of the Act: Amend the Act to extend coverage to all government institutions, including Ministers' Offices and the Prime Minister's Office, and extend rights of access to foreign nationals;

16. Limit exemptions to access to personal information requests under the Act: Exemptions to personal information access requests should be limited. They should generally be injury-based and discretionary to maximize disclosure.

Source: Office of the Privacy Commissioner, "Review of the Privacy Act - Revised recommendations," 1 November 2016.

APPENDIX B

EVIDENCE REGARDING THE ORDER-MAKING MODEL

Evidence on the Order-Making Model
"I would say that I don't have a firm view on that particular debate, except that I lean heavily towards the order-making power. I would encourage you, in thinking that through, to take the perspective of the individual rights holder here in terms of privacy, and ask which is going to be better for them in terms of which of these models puts more of a burden on the individual to go to court to vindicate their rights rather than have it dealt with in this other process. We have an access to justice crisis here, and putting burdens on individuals to take it up in court when they are supposed to have these robust rights is, I think, unrealistic. […] The only other thing I would say is that in these charter contexts that I'm extremely concerned about, having a strong stick is good, because in these charter contexts, the individual is in a conflicting relationship with the state, whereas in the more administrative context, where the state's administering a social program, there's not that strong conflict."[1] Ms. Lisa Austin
"We would like to see order-making power given to the Privacy Commissioner. It was with interest that we noted he now agrees. More information sharing and collection means that more potential harm can come from excesses. There need to be consequences in proportion to the risks, which means that the commissioner needs expanded powers to make sure the fullest protection of the revised law can be brought to bear in a timely and effective manner."[2] Ms. Brenda McPhail
"Therefore, I support […] enhanced mechanisms, including order-making powers, to enable the Privacy Commissioner to preserve public confidence. I also support regular review of our privacy laws at least every five years."[3] Mr. Thomas Keenan

1 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 June 2016, 1000 (Ms. Lisa Austin, Associate Professor, University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights, As an Individual).

2 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1110 (Ms. Brenda McPhail, Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association).

3 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1120 (Mr. Thomas Keenan, Professor, University of Calgary, As an Individual).

"My sixth recommendation is for a privacy commission to have order-making power. Now Commissioner Therrien agrees at this point, but enforcement powers and stiffer penalties for privacy invasion would still be needed to help effectively restrict privacy invasions and regulate transborder data flow."[4] Mr. Ken Rubin
"the most important powers of a privacy commission are those that are proactive and general or systemic, rather than those that are reactive or individual-based. I would like to see the act reformed in such a way that some of the more proactive powers are included in the legislation. That includes order-making power. The commissioner can only make non-binding recommendations; he cannot compel a public body to take or cease any action without recourse to the courts."[5] Mr. Collin Bennett
"I think a distinction has to be made between the tribunal model in Quebec and the commission models in B.C. and Alberta. […] We should also be very careful about generalizing from the provinces to the federal government and translating models that might work in B.C. or Quebec and think they're going to work in Ottawa. However, I do favour order-making for a couple of reasons. I think it focuses the mind better. […] the former commissioner—she would say that knowing you have that power focuses the mind of the organization to mediate. Therefore, the kinds of processes that are engaged in mediation should take place more expeditiously, more seriously. I don't think simply having order-making power necessarily makes it longer. Again, it's apples and oranges, […] The other thing about order-making power is it does establish a clarity of law which you do not necessarily get through an ombudsman process."[6] Mr. Collin Bennett
"Most of my thoughts, I must admit, are within the private sector context. […] I think the experience we've had over the last number of years demonstrates that real penalties matter. […] I would also say that we now have enough experience with companies being quite willing to disregard the Privacy Commissioner's views that I think a tougher position is needed. A classic example would involve Bell—it comes up again, I suppose—in the decision involving relevant targeted advertising. […] The commissioner has made a finding, and Bell's initial position is "well, that's nice; that's your view; we disagree". It's not clear to me, given the import we place and the responsibility we place on the Privacy Commissioner, how companies can adopt that position and basically say, "See you in court, and let's litigate this for a few years

4 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 September 2016, 1130 (Mr. Ken Rubin, Investigative Researcher, Advocate, As an Individual).

5 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1105 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

6 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1200 (Mr. Colin Bennett, Professor, Department of Political Science, University of Victoria, As an Individual).

before we decide what will take place". Bell ultimately backed down, but I think the presence of order-making power would have changed that dynamic considerably."[7]

Mr. Michael Geist

"In terms of the ombudsman versus order-making power versus hybrid, we see that the Privacy Commissioner himself, last month, has come around to the view that order-making power would be preferable. This is the view we have long held and the view we have also put forward in terms of the Information Commissioner. Both of these officers of Parliament should have order-making powers."[8]

Mr. Vincent Gogolek

"With the order-making model, an advantage is that it would clearly align more closely with international models of data protection. That's what you would see in the Federal Trade Commission and the Federal Communications Commission in the U.S., as well as in the United Kingdom and Mexico. Most European data protection authorities also have that kind of an order-making tribunal model. Clearly we would see much a more timely response to the oversight office once formal investigations are started. In the experience in those provinces that have order-making, there tends to be a more positive response and a more timely response when the commissioner comes calling. Obviously there would be higher levels of compliance in cases where the government institution would otherwise not accept a recommendation from the commissioner, although you've already heard from the Information Commissioner that most recommendations are now accepted without any order-making capacity. With regard to the disadvantages, the process tends to be more formal and more attenuated when you have an administrative tribunal. The strict obligation to ensure procedural fairness typically builds in longer time periods to move a file forward. That could translate to even longer delays than those already encountered, and certainly less flexibility for the commissioner. The process will be less user friendly for your constituents and perhaps more intimidating to individuals who make complaints to the order-making commissioner. It will likely mean dividing staff and creating a separate group of intake officers and mediators, then a separate group of adjudicators or hearing officers, and then installing within the office some kind of a wall between the two groups."[9]

Mr. Gary Dickson

---

7 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1200 (Mr. Michael Geist, Canada Research Chair in Internet and E-commerce Law and Professor of Law, University of Ottawa, As an Individual).

8 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1115 (Mr. Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

9 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1120 and 1125 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

"There is no question that there is more formality in the [order-making] process. If you take Alberta or British Columbia, they have people in their office who specifically work on mediation. They have other people in the office whose sole responsibility is writing formal orders in those jurisdictions, so you have that kind of division. It brings in some additional complexity. Under the existing Privacy Act, there is a provision that the commissioner creates his own procedural rules. There is a provision that nobody is entitled, as a right, to be able to see what the other party has said. They are not entitled to sit in when other people are being interviewed or examined. I think the Canadian Bar Association's position is that the enhanced ombudsman model provides a significant advantage in terms of flexibility and accessibility."[10]

Mr. Gary Dickson

"In Alberta and British Columbia, for example, the process is clearly more formal. There are more opportunities for parties to be able to see what the other side is saying and what other parties are submitting by way of argument. That, of course, is part of procedural fairness. What happens in an information commissioner's office or a privacy commissioner's office in the ombudsman model is that there is more flexibility. If an issue comes up in the course of an investigation in Alberta or British Columbia, then it is almost like going back to the start. You have to do a bunch of notifications and so on, and start over. There are additional time periods. With the ombudsman model, if in the course of an investigation another important issue comes up, you provide a more informal notification to the public body. You give them a shorter timeline to provide any additional response. We would see that as being fair, but it is not as rigid a sense of procedural fairness as what you get with an administrative tribunal."[11]

Mr. Gary Dickson

"My experience with this was back in B.C., and it compared to what's happening in Nova Scotia with the recommendations. […] When matters reached the stage where it went to adjudication, there was a wall between the informal mediation and the adjudication. It was quite formal relative to recommendation-making. Parties tended to be represented by lawyers. They provided witness submissions. There was an exchange of submissions. The hearings generally, though, almost exclusively, were in writing before a single adjudicator, but it required the B.C. office to have a group of adjudicators separate from the rest of the staff who conducted these hearings and issued written reports."[12]

Ms. Catherine Tully

---

10 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1200 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

11 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1200 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

12 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1115 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

"From having experience with both order-making and recommendation-making, I can say without hesitation that plain recommendation-making is not a good model. […] Order-making worked really well in B.C. [...] When there's order-making, the informal resolutions go faster, the public body is taken more seriously, there's less foot-dragging, they're more willing to engage and engage quickly, and they have better submissions. When you only get to recommend at the end, there's a degree of inconsistency in terms of who's accepting and who's not, so it's hard to set a good standard across all public bodies, because some are willing to follow the recommendations and some aren't. It definitely needs more. I like the hybrid model for a small jurisdiction. I think that would really work. My office is very small. There are only seven of us. There's no way we're going to have resources to be able to have a separate adjudication unit, whereas the federal offices are large and probably much more capable of absorbing that responsibility."[13]

Ms. Catherine Tully

"Under order-making power and mediation and consultation, in British Columbia the mandate of the office includes the promotion of access and privacy rights, public education, advice to public bodies and businesses, investigation of complaints, mediation, and independent adjudication. These functions are complementary, and in my opinion, best delivered under one roof […] Combining the investigation and adjudication into one office provides clear benefits to citizens. Combining those provides one-stop shopping for citizens. This clarity and convenience is important. […] We have not found that the public education or the advisory functions of a commissioner pose a risk of undermining the adjudicative function. We do take steps to protect the integrity of the adjudication process. For example, no information about investigative files or attempts at informal resolution are ever disclosed to the adjudicators. […] Adjudication enhances our ability to resolve issues through mediation. The adjudicative function lends greater authority to our investigators by focusing the minds of the parties, and it provides an incentive to both parties to avoid formal adjudication. As a result, we resolve 90% of our complaints and reviews in mediation. […] The fact that we have public education and advisory functions, complemented by investigative powers, with the ultimate ability to order compliance through our adjudicative function, gives us a level of authority that can influence the public and the government."[14]

Mr. Drew McArthur

---

13 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1210 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

14 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1125 (Mr. Drew McArthur, Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia).

APPENDIX C

EVIDENCE REGARDING THE HYBRID MODEL

Evidence on the Hybrid Model
"It started at the outset with the commissioner complaining about the inordinate delays, of sometimes two, three, and four years, before the information was released—an incredible portion. […] We were the ones who raised, with the commissioner, an order-making model, and we were inclined to go to that model, but the commissioner kept speaking against it and expressing his view that the ombudsman model worked better. He argued that the order-making model would introduce even longer delays than were already being experienced because they would have to do a detailed assessment and write a supporting decision that would stand up to legal scrutiny on appeal of any such order. He believed it would introduce even longer delays because of the hearing processes, and so on […] As a result of the discussions, it started to come to light what was driving some of the inherent delays, and the commissioner came around and said, "Well, we could live with an order-making model. It may work all right, but we think the ombudsman model is best for Newfoundland and Labrador." When we then did the detailed assessment of what was driving it—and all that information is in the report—it was clear that the commissioner's office was the cause of 90% of the delay. The procedures and the approach being taken weren't greatly different from what they were in most other provinces […] We worked on a system that would speed it up, and the hybrid model is what we produced. […] [W]e had very strict time limits placed on the time frame. When the recommendation of the commissioner is made, if it's unacceptable to the public body, the public body has two choices: follow the recommendation and release it if it requires release, or apply to the court right away, within 10 days, for an order that you would not be required to release it. As a result, the burden shifts to the public body, not to the requester to provide it. That's effectively making it an order, but it doesn't place the commissioner in the position where he or his office feels they have to go through these processes of hearings and to write this learned, extensive "court of appeal" type of judgment on the issue that takes all of this time, and then have the appeal of it go to a court, which hears the issue *de novo*, all over again."[1] Mr. Clyde Wells

1 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 May 2016, 0915 (Mr. Clyde Wells, Member, Independent Statutory Review Committee).

"If you have a hybrid model where 700 recommendations are involved, why do you need an order model because 70,000 recommendations are involved? Why would there be a difference merely because of numbers? You'd still have perhaps an even greater burden in the order-making model with 70,000 requests than you would with an order-making model with 700 requests. I would think the burden would be greater to use an order-making model than the hybrid model. That's my guess. The commissioner would know better than I."[2]

Mr. Clyde Wells

"I have trouble understanding why the commissioner has done an about-face and is now requesting order-making powers rather than the hybrid model. Like him, I will refer to the La Forest judgment. Justice La Forest warned us that such a change would be costly, that it could further delay the investigation process and, worse still, that it could lead to closed-door hearings. I will now quote Justice La Forest's statements that are included in the Privacy Commissioner's letter.

> There is a danger that a quasi-judicial, order making-model could become too formalized, resulting in a process that is nearly as expensive and time-consuming as court proceedings. It is also arguable that the absence of an order-making power allows the conventional ombudsman to adopt a stronger posture in relation to government than a quasi-judicial decision-maker. There is also some virtue in having contentious access and privacy issues settled by the courts, where proceedings are generally open to the public."[3]

Mr. Michel Drapeau

"The CBA completely agrees with the commissioner that the current model of pure ombudsman requires reform. […] The alternative we suggest would be the newer model that's been created and then implemented in Newfoundland and Labrador's June 2015 amendments to their access and privacy law. […] The chief advantage of the enhanced ombudsman model is a less formal, more flexible process that we think will be more user-friendly for your constituents. Allowing the commissioner to hold government institutions to account and order them to provide relevant documents and responses within deadlines, which don't currently exist for the privacy commissioner under the Privacy Act, will go a long way towards expediting and accelerating the process. I remind you that this process is often prolonged and arduous, the key being how to get co-operation from government institutions in providing the documents and information you need. We think improved efficiency should flow from the new powers suggested to better control the process of an investigation. On the substantive issue of whether there has been a breach, the enhanced ombudsman model shifts the onus to government institutions. This is something we think highly appropriate. If a government institution is dissatisfied with a decision of the commissioner, it's up to the government

2 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 May 2016, 0945 (Mr. Clyde Wells, Member, Independent Statutory Review Committee).

3 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1120 (Colonel (Retired) Michel Drapeau, Professor, University of Ottawa, Faculty of Common Law, As an Individual).

institution to go to court to obtain a final determination. Finally, as we see it, it would be easier for the privacy commissioner's office to transition to the enhanced ombudsman model than to an order-making model. When I recently spoke with Newfoundland and Labrador's information and privacy commissioner's office, one of the senior officials commented that the new system, only a year old, was working in an excellent fashion. He thought it had been very successful. The disadvantage is that we only have about a year of experience here. Newfoundland embarked on this new process in June of 2015, so it's a limited time. We understand, though, that the system appears to be working well at present."[4]

Mr. Gary Dickson

"I think my response would be this. If you take the approach the CBA does—that Canadians have quasi-constitutional rights to have their privacy protected and to have access to government records and government information—then the focus needs to be on accessibility, and accessibility usually translates into a simpler process rather than a more complex one. When we look at the kinds of complaints that come from different jurisdictions, it's often about delay. It is not so much that decisions of commissioners aren't respected—most times they are complied with, and that's true right across the board, as well as federally—but the issue tends to be one of delay. I think the proposal the Newfoundland committee came up with, which is embedded in the Newfoundland legislation, points a way to an expedited process that can reduce the delay by ensuring a more informal process."[5]

Mr. Gary Dickson

"I think the Canadian Bar Association's position is that the enhanced ombudsman model provides a significant advantage in terms of flexibility and accessibility."[6]

Mr. Gary Dickson

"In Alberta and British Columbia, for example, the process is clearly more formal. There are more opportunities for parties to be able to see what the other side is saying and what other parties are submitting by way of argument. That, of course, is part of procedural fairness. What happens in an information commissioner's office or a privacy commissioner's office in the ombudsman model is that there is more flexibility. If an issue comes up in the course of an investigation in Alberta or British Columbia, then it is almost like going back to the start. You have to do a bunch of notifications and so on, and start over. There are additional time periods. With the ombudsman model, if in the course of an investigation another important issue comes up, you provide a more informal notification to the public body. You give them a shorter timeline to provide any

4 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1120 and 1125 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

5 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1155 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

6 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1200 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

additional response. We would see that as being fair, but it is not as rigid a sense of procedural fairness as what you get with an administrative tribunal."[7] Mr. Gary Dickson
"I think there are certainly strengths with the order-making model and I've worked in those jurisdictions that have it, but in terms of providing the highest measure of service to Canadians and the most successful kind of service, I think the enhanced ombudsman model best fits the bill. Beyond that, the other process is ensuring that the commissioner has a broader range of powers. Parliament has provided the commissioner with diverse powers in PIPEDA, which are appropriate, and we see them being used frequently. The Privacy Commissioner needs a similar arsenal of remedies, tools, and resources when he's dealing with matters under the federal Privacy Act.[8] Mr. Gary Dickson
"Then ultimately, there's making it effective. I'm not a fan of order-making powers. I think the ombuds model works, but I have come around to see the wisdom of the Newfoundland hybrid model, where if a government department is not going to follow a recommendation with respect to any obligation under the Privacy Act—collection, use, disclosure, or other safeguards—the department should have to stand up in front of a court and justify it and explain why it doesn't have to. In effect, that puts the onus on the government department, and we would end up with a body of case law that would be more clear."[9] Mr. David Fraser
"Not having any teeth in the legislation I think is ultimately problematic. Forcing the individual concerned to be the one who goes to court and has the onus of proving to the judge that somehow their rights have been infringed I think places too much of a burden on the individual. Also, when you simply look at the economics between the two—the government and an individual—that's a pretty daunting prospect for an individual. There is probably greater opportunity when the commissioner doesn't have the ability to compel the person to do something, but does have a lot of authority in terms of the ability to sit down and discuss it. […] It's a much less confrontational approach. The commissioner would have the ability to work with the public body in order to exercise moral suasion to convince them that "this is it and that ultimately this is the recommendation". Then, if the government institution decides that they're not going to follow that recommendation, they should be the ones to stand up in front of a judge and say that they're not legally required to do this. You can clearly have a difference of opinion. To me, it's as much not wanting to change the character of the interaction between the office and the individual, or the office and the institution, and

7 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1200 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

8 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 September 2016, 1220 (Mr. Gary Dickson, Executive Member, Privacy and Access Law Section, Canadian Bar Association).

9 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1105 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

wanting to make sure that the onus is properly on the right party, and also that the burden ultimately is on the right party. […] If the commissioner has an education mandate and an advocacy mandate and all these other sorts of things, you don't want to turn the commissioner into essentially a tribunal as well. You want to separate that as well."[10]

Mr. David Fraser

"that's not to say that we're opposed to order-making power. To me, it comes down, first of all, to whether order-making power is necessary to compel compliance with the recommendations that are being issued and, second of all, to whether it would make the OPC more effective in its oversight role. Would it create a greater impetus for organizations to follow their recommendations? Would it turn it into a stronger body, or would it further delay the process by making companies more defensive through the investigations? I don't know the answer to that question, but I think it's important to think about the issue in those terms.

It's also worth considering in the context of the statement by the OPC that most institutions do eventually agree to their recommendations, though there can be lengthy delays. Against that backdrop, obviously the delays are a legitimate concern, but if that's the major issue, I'm not entirely certain how order-making power would solve it more effectively than the hybrid model that had been previously suggested."[11]

Mr. Michael Karanicolas

"The model we have, whereby we make a recommendation that can become an order if it's not appealed to the court within 10 days, is very effective. It places the burden on the public body. It also allows us to participate in the court hearing, which is invaluable, because we get to give our own objective perspective in court. Sometimes in the case of a person who doesn't have the resources to have their own counsel, that is really the only substantive quality argument the court hears, other than the arguments that are filed on behalf of the public body."[12]

Mr. Donovan Molloy

10 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 September 2016, 1125 (Mr. David Fraser, Partner, McInnes Cooper, As an Individual).

11 ETHI, *Evidence*, 1st Session, 42nd Parliament, 20 October 2016, 1105 (Mr. Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

12 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1150 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

"A pure recommendation model is completely ineffectual. From our point of view, the fact that a recommendation can become an order in 10 days motivates the public bodies and other authorities to co-operate and to get these things concluded, because if it goes to a formal report and they're not prepared to follow the recommendation, they have to go to court and they have to justify why they didn't. I think the hybrid model is fairly powerful as well."[13]

Mr. Donovan Molloy

"I like the hybrid model for a small jurisdiction. I think that would really work. My office is very small. There are only seven of us. There's no way we're going to have resources to be able to have a separate adjudication unit, whereas the federal offices are large and probably much more capable of absorbing that responsibility."[14]

Ms. Catherine Tully

13 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1210 (Mr. Donovan Molloy, Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador).

14 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2016, 1210 (Ms. Catherine Tully, Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia).

APPENDIX D
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
Office of the Privacy Commissioner of Canada Patricia Kosseim, Senior General Counsel and Director Genera Legal Services, Policy, Research and Technology Analysis Branch Sue Lajoie, Director General Privacy Act Investigations Daniel Therrien, Privacy Commissioner of Canada	2016/03/10	5
Independent Statutory Review Committee Doug Letto, Member Jennifer Stoddart, Member Clyde Wells, Member	2016/05/31	17
As an individual Lisa Austin, Associate Professor University of Toronto, Faculty of Law, David Asper Centre for Constitutional Rights David Lyon, Professor Queen's University Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law Thomas Keenan, Professor, University of Calgary Ken Rubin, Investigative Researcher, Advocate	2016/06/14 2016/09/20	21 23
Canadian Civil Liberties Association Brenda McPhail, Director Privacy, Technology and Surveillance		
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic Tamir Israel, Staff Lawyer		
As an individual Colin J. Bennett, Professor Department of Political Science, University of Victoria Michel W. Drapeau, Professor University of Ottawa, Faculty of Common Law	2016/09/27	24
Canadian Bar Association Gary Dickson, Executive Member Privacy and Access Law Section Kellie Krake, Staff Lawyer Law Reform		

Organizations and Individuals	Date	Meeting
As an individual	2016/09/29	25
David Fraser, Partner, McInnes Cooper		
Michael Geist, Canada Research Chair in Internet and E-commerce Law Professor of Law, University of Ottawa		
Office of the Information and Privacy Commissioner of British Columbia	2016/10/04	26
Drew McArthur, Acting Commissioner		
Bradley Weldon, Senior Policy Analyst		
Office of the Information and Privacy Commissioner of Newfoundland and Labrador		
Donovan Molloy, Privacy Commissioner House of Assembly		
Sean Murray, Executive Director House of Assembly		
Office of the Information and Privacy Commissioner of Nova Scotia		
Catherine Tully, Information and Privacy Commissioner for Nova Scotia		
Canada Revenue Agency	2016/10/06	27
Maxime Guénette, Assistant Commissioner and Chief Privacy Officer Public Affairs Branch		
Marie-Claude Juneau, Director Access to Information and Privacy		
Dentons Canada		
Chantal Bernier, Counsel Privacy and Cybersecurity		
Shared Services Canada		
Monique McCulloch, Director Access to Information and Privacy		
B.C. Freedom of Information and Privacy Association	2016/10/20	29
Vincent Gogolek, Executive Director		
Centre for Law and Democracy		
Michael Karanicolas, Senior Legal Officer		
Canada Border Services Agency	2016/10/25	30
Robert Mundie, Director General Corporate Secretariat		
Dan Proulx, Director Access to Information and Privacy Division		

Organizations and Individuals	Date	Meeting
Canadian Security Intelligence Service	2016/10/25	30
Michael Peirce, Assistant Director Intelligence		
Department of Citizenship and Immigration		
Stefanie Beck, Assistant Deputy Minister Corporate Services		
Audrey White, Director Access to Information and Privacy Division		
Royal Canadian Mounted Police		
Rennie Marcoux, Chief Strategic Policy and Planning Officer		
Joe Oliver, Assistant Commissioner Technical Operations		
Office of the Privacy Commissioner of Canada	2016/11/01	32
Patricia Kosseim, Senior General Counsel and Director General Legal Services, Policy, Research and Technology Analysis Branch		
Sue Lajoie, Director General Privacy Act Investigations		
Daniel Therrien, Privacy Commissioner of Canada		
Hon. Jody Wilson-Raybould, P.C., M.P., Minister of Justice	2016/11/24	36
Hon. Scott Brison, P.C., M.P., President of the Treasury Board		
Department of Justice		
Mala Khanna, Director, General Counsel Centre for Information and Privacy Law		
Laurie Wright, Assistant Deputy Minister, Public Law and Legislative Services Sector		
Treasury Board Secretariat		
Jennifer Dawson, Deputy Chief Information Officer		

APPENDIX E
LIST OF BRIEFS

Organizations and Individuals

Austin, **Lisa**

B.C. Freedom of Information and Privacy Association

Canadian Bar Association

Keenan, **Thomas**

Office of the Privacy Commissioner 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. 5,17, 21, 23, 24, 25, 26, 27, 29, 30, 32, 36, 37, 38 and 39) is tabled.

Respectfully submitted,

Blaine Calkins
Chair