HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

TOWARDS PRIVACY BY DESIGN:
REVIEW OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

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

Bob Zimmer, Chair

FEBRUARY 2018
42nd PARLIAMENT, FIRST SESSION

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

SPEAKER'S PERMISSION

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

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

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

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

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

TOWARDS PRIVACY BY DESIGN: REVIEW OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

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

Bob Zimmer
Chair

FEBRUARY 2018

42nd PARLIAMENT, FIRST SESSION

NOTICE TO READER

Reports from committee presented to the House of Commons

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

To assist the reader:
A glossary of terms used in this report is available on page 85

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Bob Zimmer

VICE-CHAIRS

Nathaniel Erskine-Smith

Charlie Angus

MEMBERS

Frank Baylis	Joyce Murray∗
Mona Fortier	Michel Picard
Jacques Gourde	Raj Saini
Hon. Peter Kent	Anita Vandenbeld

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Vance Badawey	Peter Fonseca	Dan Ruimy
Daniel Blaikie	Matt Jeneroux	Don Rusnak
Bob Bratina	Pat Kelly	Francis Scarpaleggia
Blaine Calkins	Alaina Lockhart	Sonia Sidhu
François Choquette	Wayne Long	Marwan Tabbara
Nathan Cullen	Alistair MacGregor	Karine Trudel
Emmanuel Dubourg	Brian Masse	Len Webber
Ali Ehsassi	Rémi Massé	Erin Weir
Neil R. Ellis	Irene Mathyssen	Salma Zahid
Pat Finnigan	Robert-Falcon Ouellette	

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

CLERK OF THE COMMITTEE

Jean-Denis Kusion

Hugues La Rue

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Michael Dewing

Chloé Forget

Marc-André Roy

Alexandra Savoie

Maxime-Olivier Thibodeau

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

TWELFTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*h*)(vi), the Committee has studied the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS

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

TOWARDS PRIVACY BY DESIGN: REVIEW OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

INTRODUCTION

On 1 November 2016, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) adopted a motion to undertake the review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[1]

The Committee began its review on 14 February 2017, and held 16 public meetings. It heard from a total of 68 witnesses and received 12 written submissions. In addition, the Committee considered the study on consent carried out by the Office of the Privacy Commissioner of Canada (OPC). The OPC's findings and recommendations are found in its 2016–17 annual report.[2] The Committee also considered a draft OPC position on online reputation released on 26 January 2018.[3] The Privacy Commissioner of Canada, Daniel Therrien, appeared at the beginning of the study, on 16 February 2017, as well as at the very end, on 1 February 2018.

In a brief submitted to the Committee on 2 December 2016, Commissioner Therrien proposed the following four areas of focus for the Committee's study of PIPEDA:[4]

1) meaningful consent;

2) reputation and respect for privacy;

3) the Commissioner's enforcement powers;

4) the adequacy of PIPEDA vis-à-vis the European Union's (EU) *General Data Protection Regulation* (GDPR), which will come into effect in May 2018.

---

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI], *Minutes of Proceedings*, 1st Session, 42nd Parliament, 1 November 2016.

2 Office of the Privacy Commissioner of Canada [OPC], *2016-17 Annual Report to Parliament*, September 2017.

3 OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

4 ETHI, Submission by the Privacy Commissioner of Canada, 2 December 2016.

This report provides an overview of PIPEDA, addresses each area of focus proposed by the Commissioner and makes recommendations to the Government of Canada. It also includes a report on the Committee's mission to Washington, D.C., from 2 to 4 October 2017.

PART 1: OVERVIEW OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

A. History of the *Personal Information Protection and Electronic Documents Act*

PIPEDA came into being following broad consultations. In an example of multiple stakeholder cooperation, a committee of consumer, business, government, labour and professional representatives developed a set of data privacy protection principles that, in 1996, were approved as a national standard by the Standards Council of Canada. These principles were titled the *Model Code for the Protection of Personal Information* (the Model Code).[5] Consultations and discussion papers arguing for the implementation of these principles through legislation followed. International developments regarding data protection, particularly those taking place in the EU, served as further impetus for the adoption of private sector privacy legislation in Canada.[6]

B. Scope of application of the *Personal Information Protection and Electronic Documents Act*

PIPEDA was passed into law in 2000 and came into force in three stages between 2001 and 2004.[7] PIPEDA applies primarily to the collection, use or disclosure of personal

5 Miguel Bernal-Castillero, *Canada's Federal Privacy Laws*, Publication no. 2007-44-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 1 October 2013.

6 In 1995, the EU passed a data protection directive to ensure the protection of personal information while allowing the movement of such information as necessary within the EU. The directive came into force in 1998. The directive required all member countries to adopt or modify existing national data protection legislation in order to comply with it. Article 25 of the directive extended its reach beyond the EU by prohibiting member countries (and businesses within them) from transferring personal information to any non-member country whose laws did not sufficiently guarantee the protection of that information. See European Parliament, Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995. The adequacy of PIPEDA is addressed later in this report.

7 On 1 January 2001, the Act applied to the federally regulated private sector (i.e., banking, telecommunications, and interprovincial transportation). On 1 January 2002, personal health information became subject to the Act and on 1 January 2004, the Act applied to the whole of the private sector, even to organizations that only collect, use or disclose information within a particular province. Organizations in the Northwest Territories, Yukon and Nunavut are considered to be federal works, undertakings or businesses under PIPEDA.

information in the course of commercial activities by a private sector organization and by federal works, undertakings and businesses. It regulates all such activity not only at the federal level and in the territories, but also in every province, unless that province has passed its own legislation requiring the private sector to provide comparable protection (referred to as "substantially similar legislation"). To date, Quebec, British Columbia, Alberta and, in matters relating to health care, Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have passed legislation deemed substantially similar to PIPEDA.[8]

More specifically, PIPEDA currently applies to the following organizations:

- private sector organizations carrying on business in Canada in the provinces or territories of Prince Edward Island, Manitoba, New Brunswick, Nova Scotia, Nunavut, Ontario, Saskatchewan, Newfoundland and Labrador, Northwest Territories or Yukon, but **not** their handling of employee information;

- private sector organizations carrying on business in Canada when the personal information they collect, use or disclose crosses provincial or national borders, but **not** their handling of employee information;

- federally regulated organizations carrying on commercial activity in Canada, such as a bank, airline, telephone or broadcasting company, etc., **including** their handling of health information and employee information.[9]

Part 1 of PIPEDA addresses the protection of personal information in the private sector.[10] The purpose of PIPEDA, as set out in section 3, recognizes the relationship between the need to protect personal information and the need to use it in a world increasingly driven by information technology:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of

8 OPC, *Provincial legislation deemed substantially similar to PIPEDA*. "While other provinces and territories have also passed their own health privacy laws, these have not been declared substantially similar to PIPEDA." (Office of the Privacy Commissioner of Canada, *Overview of privacy legislation in Canada*.)

9 OPC, *Overview of privacy legislation in Canada* [EMPHASIS IN THE ORIGINAL].

10 Part 2 of PIPEDA deals with electronic documents and is primarily focused on granting them the force of legal documents as well as specifying when they are equivalent to paper copies.

> organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[11]

Building on the work conducted by stakeholders in drafting the Model Code, PIPEDA incorporates the Model Code into the legislation by requiring that organizations subject to the Act comply with the obligations set out in it. The Model Code is included in Schedule 1 of the Act. In summary, organizations are required to adhere to the principles in Schedule 1 to PIPEDA.

C. The Privacy Commissioner of Canada

PIPEDA is enforced by the Privacy Commissioner of Canada, who can receive and investigate complaints from the public or any organization concerning violations of the Act.[12] The Commissioner generally uses mediation and conciliation to resolve complaints. While the Commissioner does not have the power to issue final orders to organizations, he can summon witnesses, administer oaths and compel the production of evidence if cooperation is not forthcoming. In cases that remain unresolved, the Commissioner may seek a court order from the Federal Court to achieve resolution.[13]

In addition, the Commissioner has the power to audit how personal information is managed by any organization governed by PIPEDA, make public any information about such practices if it is in the public interest,[14] and coordinate various activities with his provincial counterparts, including the development of model contracts for the protection of personal information in interprovincial or international transactions.[15] The Commissioner also has a public education mandate with respect to the Act.[16]

Lastly, the Commissioner has the authority to enter into a compliance agreement with an organization following a complaint investigation to ensure that the organization complies with PIPEDA.[17]

> In a compliance agreement, an organization agrees to take certain actions to bring itself into compliance with PIPEDA. The Office shall not apply to the Court for a hearing under

11 PIPEDA, s. 3.

12 PIPEDA, s. 11.

13 PIPEDA, ss. 14–17.

14 PIPEDA, s. 18.

15 PIPEDA, ss. 23 and 23.1.

16 PIPEDA, s. 24.

17 PIPEDA, s. 17.1.

> PIPEDA and shall apply to the Court for a suspension of any pending court applications made under PIPEDA.
>
> However, if an organization ultimately fails to live up to commitments in the agreement, the Office may either apply to the Court for an order requiring the organization to comply with the terms of the agreement, or follow through with a court application under PIPEDA, as appropriate.[18]

D. Parliamentary review of the *Personal Information Protection and Electronic Documents Act* and attempts to amend the Act

PIPEDA requires a parliamentary review every five years of Part 1, the portion of the statute that deals with privacy and personal information. The first parliamentary review, which contained 25 recommendations for amendments to the legislation, was tabled in the House of Commons in May 2007 by the Committee.[19] The government subsequently issued a response to the recommendations in the Committee's report in October 2007.[20]

In May 2010, the Minister of Industry introduced Bill C-29, *An Act to amend the Personal Information Protection and Electronic Documents Act*.[21] Bill C-29 would have added new exceptions to consent requirements, specified what constitutes "valid consent" and imposed mandatory breach notification obligations. Bill C-29 died on the *Order Paper* with the dissolution of the 40th Parliament (26 March 2011). On 29 September 2011, the government reintroduced the bill in the 41st Parliament as Bill C-12.[22] The bill was not debated in the House of Commons prior to prorogation on 13 September 2013, when it died on the *Order Paper*.

In addition to the government bills to reform PIPEDA, during the 1st Session of the 41st Parliament, Charmaine Borg, Member of Parliament for Terrebonne-Blainville, introduced Bill C-475, *An Act to amend the Personal Information Protection and Electronic Documents Act* (order-making power). This private member's bill to amend PIPEDA

---

18 OPC, *Privacy Toolkit for Businesses*.

19 ETHI, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, Fourth Report, 1st Session, 39th Parliament, May 2007.

20 ETHI, *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics: Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, 1st Session, 39th Parliament, October 2007.

21 Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act, 3rd Session, 40th Parliament.

22 Bill C-12, An Act to amend the Personal Information Protection and Electronic Documents Act, 1st Session, 41st Parliament.

would have also imposed breach notification obligations and would have given the Privacy Commissioner the power to make compliance orders.[23]

In 2012, the Committee conducted a study on privacy and social media. In the course of that study, it "heard wide-ranging evidence regarding Canada's legislative framework and, more particularly, PIPEDA." The study further noted:

> While the present study's focus is on social media and privacy – and not on a legislative review of PIPEDA – this evidence should serve as an important basis upon which to inform any future discussion with respect to reviewing or modifying PIPEDA.[24]

While no subsequent statutory review of PIPEDA has taken place,[25] on 23 May 2013, the OPC set out its positions on PIPEDA reform in a paper entitled *The Case for Reforming the* Personal Information Protection and Electronic Documents Act.[26]

In this document, then Commissioner Jennifer Stoddart recommended that:[27]

- the Office of the Privacy Commissioner be given stronger enforcement powers;

---

23 Bill C-475, An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power), 1st Session, 41st Parliament (this bill was carried over to the 2nd Session, 41st Parliament and defeated at second reading, 29 January 2014). While Bill C-475 would have also imposed mandatory breach notification obligations, it would have done so using a different standard and approach than that found in Bill C-29.

24 ETHI, *Privacy and Social Media in the Age of Big Data*, Fifth Report, 1st Session, 41st Parliament, April 2013, p. 34. A number of witnesses who appeared during the study also commented on Bill C-12.

For example, Tamir Israel of the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa observed that Bill C-12 "provides a workable framework for breach notification, but it requires fixes and a commitment to introduce penalties for non-compliance if it is to be effective" (p. 35).

Jennifer Stoddart, then the Privacy Commissioner of Canada, expressed concern that "in its current form, Bill C-12 was not an adequate solution to the constant and growing threat of data leakage and data-related breaches of confidence" (p. 36). She suggested that one idea that could strengthen the legislation would be to establish a penalty system to encourage companies "to invest in data protection and act as a deterrent to breaches of confidence, while remaining flexible and adaptable so as not to unduly burden smaller organizations" (p. 36).

25 According to section 29 of PIPEDA, a parliamentary review would have been due in 2011–2012 (five years following the previous review).

26 OPC, *The Case for Reforming the* Personal Information Protection and Electronic Documents Act, 23 May 2013.

27 Options include statutory damages to be administered by the Federal Court, and providing the Privacy Commissioner with order-making powers and/or the power to impose administrative monetary penalties where circumstances warrant.

- organizations be required to report breaches of personal information to the Office of the Privacy Commissioner and to notify affected individuals where warranted;

- public reporting requirements be added to increase transparency on the use of an exception in PIPEDA that allows enforcement agencies and government institutions to obtain personal information from organizations without consent for various purposes, including national security and law enforcement; and

- PIPEDA be amended to enable the Commissioner to enter into "enforceable agreements" with organizations to ensure that they are meeting their commitments to comply with the Commissioner's recommendations following investigations.[28]

E. Recent amendments to the *Personal Information Protection and Electronic Documents Act*

Bill S-4, the *Digital Privacy Ac*t (short title), was introduced in the Senate and received first reading on 8 April 2014, was amended by the Standing Senate Committee on Transport and Communications and received royal assent on 18 June 2015.

The bill amended PIPEDA in order to:

- permit the disclosure of an individual's personal information without their knowledge or consent in certain circumstances;

- require organizations to take various measures in cases of data security breaches[29];

- create offences for failure to comply with obligations related to data security breaches; and

28 As stated previously, the Commissioner now has the authority to enter into a compliance agreement with an organization following a complaint investigation to ensure that the organization complies with PIPEDA. Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act amended PIPEDA by adding this authority.

29 Please note that "the new data breach requirements in PIPEDA will come into force once the Government passes regulations, which will provide greater clarity and specificity of the requirements of the Act". See Innovation, Science and Economic Development Canada, For Discussion — Data Breach Notification and Reporting Regulations, March 2016.

- enable the Privacy Commissioner, in certain circumstances, to enter into compliance agreements with organizations.[30]

Bill S-4 incorporated certain provisions of Bill C-12 and also appeared to follow up on some of the recommendations made by witnesses during the Committee's 2012 study of privacy protection and social media and by former Commissioner Stoddart in her May 2013 position paper.[31]

Canada's Anti-Spam Legislation[32] (CASL) was passed in December 2010 and came into force on 1 July 2014, with the exception of the provisions related to unsolicited installation of computer programs or software, which came into force on 15 January 2015. CASL provides, among other things, for a private right of action in court, although those provisions have not yet been proclaimed into force. CASL also provides for administrative monetary penalties and criminal penalties.[33] Among other things, CASL makes it illegal to send commercial electronic messages without consent, including messages sent to email addresses and social media accounts, and text messages to cell phones.

In addition, CASL modified PIPEDA. According to the new provisions, the Commissioner shares responsibilities enforcing CASL with the Canadian Radio-television and Telecommunications Commission (CRTC) and the federal Competition Bureau.

> The CRTC is responsible for investigating the sending of unsolicited commercial electronic messages, the alteration of transmission data and the installation of software without consent.
>
> The Competition Bureau addresses false or misleading representations and deceptive marketing practices in the electronic marketplace.
>
> The OPC, meanwhile, focuses on two types of violations:
>
> - the harvesting of electronic addresses, in which bulk lists of email addresses are compiled through mechanisms that include the use of

30 Dara Lithwick, *Legislative Summary of Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*, Publication no. 41-2-S4-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 11 June 2014.

31 Ibid.

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

33 Government of Canada, *Canada's Anti-Spam Legislation, Fast Facts*.

computer programs to automatically mine the Internet for addresses; and,

- the collection of personal information through illicit access to other people's computer systems, primarily through means such as spyware.[34]

F. Constitutional issues

The protection of personal information involves elements that fall under the jurisdiction of both federal and provincial governments, but it is not explicitly addressed in the sections of the *Constitution Act, 1867*[35] dealing with the distribution of powers. At the federal level, PIPEDA was adopted by the Parliament of Canada in accordance with its authority to regulate inter-provincial trade pursuant to section 91(2) of the *Constitution Act, 1867*. At the time, the federal government's position was that personal information was a commodity that could be bought and sold and that its protection was a transborder issue requiring a federal legislative framework.[36]

The provinces are also able to legislate in order to protect personal information as they have authority over property and civil rights pursuant to section 92(13) of the *Constitution Act, 1867*. This is a fairly broad authority and it allows provincial legislatures to legislate on private inter-provincial matters, including trade, contracts, relationships between persons, and so forth. This jurisdiction allows provinces to pass privacy legislation similar to PIPEDA.

The constitutionality of PIPEDA has been challenged a number of times since its enactment. Some argue that this federal act governs an exclusively provincial area of jurisdiction, and federal legislation is neither necessary nor permitted.[37] The Government of Quebec filed a reference before the Quebec Court of Appeal in 2003 in order to determine whether PIPEDA is unconstitutional and encroaches on provincial jurisdiction. The case is still pending. In another case before the Federal Court, a party challenged the constitutional validity of PIPEDA. However, the Court ultimately refused

34 OPC, *The OPC's responsibilities under CASL*.

35 *Constitution Act, 1867,* 30 & 31 Victoria, c. 3.

36 House of Commons, *Hansard*, 2nd Session, 36th Parliament, Number 9 (22 October, 1999), p. 537.

37 For a complete analysis of the constitutional validity of PIPEDA, see Michel Bastarache, *The Constitutionality of PIPEDA: A Re-consideration in the Wake of the Supreme Court of Canada's Reference re Securities Act*, June 2012. The following articles argue that PIPEDA is constitutional, but they were published before the Supreme Court of Canada released its advisory opinion in the *Reference re Securities Act*, [2011] 3 SCR 837, 2011 SCC 66: Mahmud Jamal, "Is PIPEDA Constitutional?", 43 Can. Bus. L.J. 434 (2006); Josh Nisker, "PIPEDA: A Constitutional Analysis", 85 Can. B. Rev. 317 (2006).

to rule on the issue.[38] The courts have yet to decide on the constitutional validity of PIPEDA in terms of the division of powers.

PART 2: MEANINGFUL CONSENT UNDER THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* REGIME

A. The general principle of consent as set out in the *Personal Information Protection and Electronic Documents Act*

The current model of privacy protection and disclosure and sharing of personal information is based primarily on the principle that users trade their personal information for services. It is essentially a contract based, in theory, on the informed consent of individuals who agree to disclose their personal information. As indicated by Michael Karanicolas of the Centre for Law and Democracy (CLD):

> The core dynamic that underlies this model and that drives much of the digital economy is that users may choose to trade their personal information for services. There are undeniable benefits to this model, which has assisted in the rapid spread of the Internet by lowering costs of entry. However, this dynamic relies on meaningful consent, which in turn requires at least a nominal understanding by the contracting party of what they're signing on to.[39]

The premise of the consent model is that the best protection for personal information is to ensure that individuals are free to use their personal information as they wish, including exchanging it for services.[40]

The following elements summarize the rules for consent under PIPEDA:

- **Basic principle**: Principle 3 in Schedule 1 to PIPEDA specifies the rules for collecting, using or disclosing personal information. All organizations must comply with these obligations.[41] The basic principle concerning consent states as follows: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information,

38 *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 F.C. 736.

39 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1530 (Michael Karanicolas, Senior Legal Officer, Centre for Law and Democracy).

40 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1610 (Éloïse Gratton, Partner and National Co-Leader, Privacy and Data Protection Practice Group, Borden Ladner Gervais).

41 PIPEDA, s. 5(1).

except where inappropriate."[42] It is important to note that PIPEDA contains a number of exceptions where an organization could collect, use or disclose individuals' personal information without their knowledge and consent. For example, it may be impossible or unrealistic to obtain a person's consent for legal or medical reasons.[43]

- **When consent is obtained**: As stated in PIPEDA, "Consent is required for the collection of personal information and the subsequent use or disclosure of this information." Consent can be obtained at the time the information is collected. Consent must also be obtained when an organization plans to use the collected information for a new purpose.

- **Meaningful consent**: In order for consent to be meaningful, "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."[44]

- **Restriction on the amount of personal information required**: "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes."[45]

- **Type of consent and how it is obtained**: The type of consent given and the way in which it is obtained can vary depending on the circumstances and the information involved. Organizations must consider the sensitivity of the information. In addition, in "obtaining consent, the reasonable expectations of the individual are also relevant."[46] The individual "may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal."[47]

42 PIPEDA, Schedule 1, "Principle 3 – Consent", cl. 4.3.

43 Ibid.

44 Ibid., cl. 4.3.2.

45 Ibid., cl. 4.3.3.

46 Ibid., cl. 4.3.5.

47 Ibid., cl. 4.3.8.

B. The future of consent as the core principle of the *Personal Information Protection and Electronic Documents Act*

According to the Privacy Commissioner, recent innovations in information technologies have added significant complexity to online interactions and resulted in more ways to use personal information:

> When PIPEDA was adopted, the interactions with businesses were generally predictable, transparent and bidirectional. Consumers understood why the company that they were dealing with needed certain personal information. It is no longer entirely clear who is processing our data and for what purposes.[48]

Several witnesses told the Committee that the amount of personal information exchanged and the frequency of interactions with organizations that collect personal information make it impossible for individuals to take the time needed to properly inform themselves of the conditions of use for each service and to provide informed consent. According to Teresa Scassa, Professor of Law at the University of Ottawa:

> [M]ore and more of the devices that we have on our person and in our homes are collecting and transmitting information. They may even do so without our awareness, and they often do so on a continuous basis. The result is that there are fewer clear and well-defined points or moments at which data collection takes place, making it difficult to say that notice was provided and that consent was obtained in any meaningful way.[49]

For Vincent Gogolek of the B.C. Freedom of Information and Privacy Association, the user's consent is illusory because the conditions of use are almost always in the form of lengthy and vague legal texts offered on a "take it or leave it" basis.[50] Organizations can readily obtain the consent they seek and then do whatever they want with the information collected. According to Vincent Gautrais, Director of the Centre de recherche en droit public, at the University of Montréal's Faculty of Law, consent has been transformed from a tool to protect the individual to "a way to protect the

48 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1530 (Daniel Therrien, Privacy Commissioner of Canada).

49 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1540 (Teresa Scassa, Full Professor, University of Ottawa, Canada Research Chair in Information Law).

50 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1640 (Vincent Gogolek, Executive Director, B.C. Freedom of Information and Privacy Association).

companies that use the data. Companies can now completely free themselves of any contract by burying their obligations and methods in page after page."[51]

Industry representatives who develop information technologies also told the Committee that the consent model is problematic. For example, Robert Watson from the Information Technology Association of Canada (ITAC) believes that the requirement for consent can slow innovation and deprive consumers of interesting opportunities for the use of data. He stated that "slowing the transfer of information to complete transactions to garner express consent is a practice that has significant limitations for both customers and businesses."[52] Furthermore, "[t]here are also situations where unanticipated use of data could be of great benefit to users, but where it may be difficult, if not impossible, to obtain renewed expressions of consent."[53]

Wally Hill of the Canadian Marketing Association (CMA) made similar comments, stating that "With business models becoming increasingly focused on innovation, and greater customization of products and services, which is all in response to consumer expectations, the strains on a consent-based regime must be recognized."[54]

Although most witnesses who appeared before the Committee believe that consent, in one form or another, should remain an important element of PIPEDA, many of them suggested that the shortcomings of the current model could be addressed by enhancing implicit consent. With this approach, individuals are deemed to have given implied consent to the collection, use and disclosure of data when the risk of harm is low or non-existent.[55] Consent would be required only when there is a risk of harm to the individual.[56] Éloïse Gratton, a partner at Borden Ladner Gervais, touched on this approach:

> For instance, express consent would be required when using personal information to make an eligibility decision impacting the individual, a disclosure that would involve

---

51 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1640 (Vincent Gautrais, Director, Centre de recherche en droit public, Faculty of Law, University of Montréal); also ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1540 (Teresa Scassa Law).

52 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1550 (Robert Watson, President and Chief Executive Officer, Information Technology Association of Canada).

53 Ibid.

54 ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1545 (Wally Hill, Vice-President, Government and Consumer Affairs, Canadian Marketing Association).

55 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1610 (Éloïse Gratton).

56 Ibid.

> sensitive or potentially embarrassing information, or a practice that would go against the expectation of the individual.
>
> A risk-based approach may allow organizations to streamline their communications with individuals, reducing the burden and confusion on individual consumers, since they would receive fewer requests for consent. These requests would be meaningful in the sense that they would focus on what matters to them.[57]

Implicit consent is not entirely outside the scope of the current regime. For example, Chantal Bernier, a lawyer with Dentons Canada and former Acting Privacy Commissioner and Assistant Privacy Commissioner of Canada, pointed out to the Committee that clause 4.3.6 of PIPEDA's Schedule 1 indicates that implicit consent may be adequate when the information is less sensitive.[58]

According to Mr. Hill of the CMA, this model would transfer more responsibility for protecting personal information to the organizations that collect it in exchange for greater freedom: "Organizations should have imposed on them the requirement to evaluate the risk that is involved in the use of any information and to make appropriate decisions based on that."[59] This would allow them to focus more on innovation and customization of products and services. In his opinion, an implicit consent model based on the level of risk is compatible with the notion of consent and would benefit consumers.[60]

However, some witnesses cautioned the Committee about establishing a risk-based consent model. Ms. Scassa was concerned that it would be difficult to evaluate the risks beforehand:

> What worries me about that, of course, is the threshold that there be no risk or no harm. I think that in the big data environment, we're still trying to figure out exactly what the risks and the harms are. It's not always obvious at the outset what the implications of the collection of certain types of data are going to be, depending on what is then subsequently collected by someone else and put together.[61]

Tamir Israel, Staff Lawyer with the Canadian Internet Policy and Public Interest Clinic (CIPPIC), believes that a risk-based approach could result in an "open season on

---

57 Ibid.; ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1625 (Wally Hill).

58 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1545 (Chantal Bernier, Counsel, Global Privacy and cybersecurity Group, Dentons Canada).

59 ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1625 (Wally Hill).

60 Ibid., 1620.

61 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1540 (Teresa Scassa).

individual data."[62] He also indicated that this would greatly undermine consumers' confidence, which depends on their ability to give consent.[63]

Many witnesses indicated that they would prefer to maintain consent as the basis for the PIPEDA regime and to implement measures to ensure that consent is meaningful.[64] They believe that the principle of consent currently entrenched in PIPEDA is sufficiently rigorous and flexible to adapt to challenges posed by innovations in information technology and the use of personal information. Ms. Bernier quoted section 6.1 of PIPEDA, which states that consent is valid only "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."[65] She believes this provision supports the idea that the principle of consent as set out in PIPEDA "truly allows for the complexity of the Internet, without specifying the modalities, thereby making it possible to adapt the principle to any application that emerges."[66] This view is supported by Suzanne Morin of the Canadian Bar Association (CBA), who indicated that the current model "continues to be both robust in its protection of the privacy of Canadians … and flexible for business in the face of rapidly evolving technologies, business models, and evolving customer privacy expectations."[67]

Adam Kardash of the Interactive Advertising Bureau of Canada (IAB) gave an example of the current regime's flexibility. He explained to the Committee how the online behavioural advertising industry uses the current consent model. The flexibility of the existing legal framework has allowed this industry to create AdChoices, a "Canadian self-regulatory program for online behavioural advertising," which dozens of stakeholders in this field have signed up for.[68] Mr. Kardash also pointed out that PIPEDA also sets out

---

62 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1630 (Tamir Israel, Staff Lawyer, Canadian Internet Policy and Public Interest Clinic).

63 Ibid.

64 See in particular ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1600 (John Lawford, Executive Director and General Counsel, Public Interest Advocacy Centre); and ETHI, *Evidence*, 1st session, 42nd Parliament, 30 May 2017, 1535 (Frank Zinatelli, Vice-President and General Counsel, Canadian Life and Health Insurance Association).

65 See ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1545 (Chantal Bernier).

66 Ibid.

67 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1640 (Suzanne Morin, Vice-President, Privacy and Access Law Section, Canadian Bar Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1610 (David Young, Principal, David Young Law, As an Individual).

68 ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1600 (Adam Kardash, Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP, Interactive Advertising Bureau of Canada).

useful rules applicable to the analysis and processing of big data for research and development purposes.[69]

In summary, a number of witnesses believe that the current privacy regime under PIPEDA is based on solid principles that can adapt to technological change. Rather than overhauling the consent model, it would be best to make minor adjustments and let the stakeholders – the OPC, businesses, government, etc. – adapt their practices in order to maintain and enhance meaningful consent.

The Committee is of the opinion that consent should remain the core element of the privacy protection model set out in PIPEDA. In fact, the Committee believes that respect for personal autonomy requires that individuals be generally free to decide for themselves what to do with their personal information. Although the increase in interactions between individuals and companies that collect and share their personal information has made it more difficult to obtain real and explicit consent, the Committee is of the opinion that freedom of choice is a factor that promotes consumer confidence. Therefore, instead of abandoning the consent model, the Committee is of the opinion that the Government of Canada should seek to enhance and clarify consent, as required.

Therefore, the Committee recommends:

Recommendation 1 on the principle of consent:

That consent remain the core element of the privacy regime, but that it be enhanced and clarified by additional means, when possible or necessary.

C. Enhancing the consent model

As indicated by the Privacy Commissioner in his 2016–2017 annual report, "Consent remains central to personal autonomy, but in order to protect privacy more effectively, it needs to be supported by other mechanisms."[70] Over the course of its study, the Committee heard many proposals to strengthen and clarify consent.

69 Ibid. However, Mr. Kardash told the Committee that for the purposes of clarification it would be useful for par. 7(2)(*c*) of PIPEDA to specifically state that the *analysis* of data for these purposes is permitted (and not just the *use* of data).

70 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 17.

1. Privacy policies

Many witnesses believe it is possible to make consent much more meaningful by enhancing privacy policies, which are "the foundation for the current contractual notice-and-consent model," according to the OPC.[71] Ms. Bernier believes that better privacy policies would easily make consent more meaningful:

> [E]nhancing consent involves privacy policies, which must meet three specific criteria, in my view. First, they must be written in accessible language. Second, they must be adapted to the organization. Third, they must be structured for easy consultation.[72]

Similarly, Mr. Karanicolas of the CLD believes that companies that collect personal information could publish a summary or guide explaining their privacy agreements in simple terms; agreements which are often lengthy and written in legal jargon that is difficult to understand. He also thinks that a clear notification should be sent to users when changes are made.[73] The Privacy Commissioner also believes that improving privacy policies would be very beneficial and offered guidelines in the study on consent published in his 2016–2017 annual report:[74] Furthermore, the Commissioner stated that the following elements should be included in these policies in order to obtain meaningful consent:

- what personal information is being collected;
- who it is being shared with, including an enumeration of third parties;
- for what purposes is information collected, used, or shared, including an explanation of purposes that are not integral to the service; and,
- what is the risk of harm to the individual, if any.[75]

However, the Committee notes that the OPC, as a regulatory body, does not consider that it has a role to play in drafting templates for privacy policies.[76]

---

71 Ibid., p. 20.

72 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1545 (Chantal Bernier).

73 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1530 (Michael Karanicolas).

74 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 20.

75 Ibid.

76 Ibid.

2. Opt-in consent

Other witnesses stated that the best way to address the shortcomings of the current model is to implement an opt-in consent system as the default, which would mean that the conditions of use of a service are initially set in such a way as to provide the best protection for personal information.[77] Users would explicitly choose to disclose their personal information. Mr. Israel of CIPPIC stated that, "recognizing an explicit 'privacy by default' approach will further underscore the need to obtain user input in relation to privacy practices, helping to narrow the gap between individual expectations and actual practice."[78] This view is shared by Ian Kerr, a professor at the University of Ottawa, who stated that "all default settings should default towards privacy."[79]

However, David Fraser, a partner at McInnes Cooper, had reservations about the practical implications of a default opt-in system. In his testimony, he talked about signing up for a Twitter account, a platform that promotes public expression. As he explained, if the default setting for a Twitter account offered the highest degree of privacy this "would have meant that on day one when you signed up on Twitter, all of your tweets would have been protected. Those first users would have been yelling in an empty room."[80]

Paige Backman, a partner at Aird and Berlis LLP, recommended distinguishing between information handling for non-secondary purposes, in order to provide the service requested by the user, and for secondary purposes, such as the transfer to third parties for marketing purposes. Ms. Backman stated that "an opt-out from such secondary purposes should be clearly stated and readily available to the individual."[81] Implementing this practice would enhance the consent model by reducing the preponderance of an "all or nothing 'acceptance'." Mr. Fraser made a similar distinction:

> If I go to Chapters-Indigo and order a book, do I have to opt in for them to use my address that I've just given them to ship me the book? It's completely obvious in that transaction, and you should be able to imply that consent, but secondary use, for

77 See, for example, ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1615 (Michael Geist, Canada Research Chair in Internet and E-commerce Law, Professor of Law, University of Ottawa, As an Individual); ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1640 (Vincent Gogolek).

78 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1630 (Tamir Israel).

79 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1720 (Ian Kerr, Professor and Canada Research Chair in Ethics, Law and Technology, University of Ottawa, As an Individual).

80 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1630 (David Fraser, Partner, McInnes Cooper, As an Individual).

81 ETHI, Submission by Paige Backman and Aaron Baer, April 2017.

> example, using my name and address for marketing purposes for some other purpose, seems to be a sensible opt-in.[82]

The Committee is of the opinion that making opt-in consent the default is a promising mechanism for enhancing the consent model, even though it may need to be adapted for the service provided. At a minimum, the Committee is of the opinion that any consent for the use of personal information for secondary purposes should, by default, require consent.

Therefore, the Committee recommends:

Recommendation 2 on opt-in consent by default:

That the Government of Canada propose amendments to the *Personal Information Protection and Electronic Documents Act* to explicitly provide for opt-in consent as the default for any use of personal information for secondary purposes, and with a view to implementing a default opt-in system regardless of purpose.

3. Improving algorithmic transparency

In order to obtain meaningful consent, it is vital that individuals be sufficiently informed about how the information is used by the organizations that collect it, especially in the era of big data and cross-border data transfers.[83] Today, personal information is often processed with complex algorithms, which seek to increase the quality of the user's experience, but also to assess risks and make important decisions that may affect the user's interests.[84] "These [artificial intelligence programs] are designed in ways that raise unique privacy challenges."[85] In fact, users have little information about how they work, the data they collect and how they are used.

One of the concerns raised about algorithms is the risk that their use of personal information will perpetuate prejudices or discriminatory practices that exist in our society. Valerie Steeves, full professor in the Department of Criminology at the University of Ottawa, gave the Committee an example about an intelligence system that supposedly identifies young criminals in England. According to Ms. Steeves, "The

82 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1710 (David Fraser).

83 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1620 (Michael Geist).

84 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1720 (Ian Kerr).

85 Ibid.

youngest potential criminal they identified was three years of age, and he was identified because he was racialized, he was impoverished, and he lived in a particular area."[86]

In addition to the risks related to potential discriminatory practices, Mr. Kerr argued that the use of algorithms to process personal information is not transparent and can undermine human rights:

> Machine learning, knowledge discovery in databases, and other AI techniques produce decision-making models differing so radically from the way that human decisions are made that they resist our ability to make sense of them. Ironically, [artificial intelligence programs] display great accuracy, but those who use them and even their programmers often don't know exactly how or why.
>
> Permitting such decisions without an ability to understand them can have the effect of eliminating challenges that are essential to the rule of law. When an institution uses your personal information and data about you to decide that you don't get a loan, your neighbourhood's going to be the one under more police surveillance, you don't get to go to university, you don't get the job, or you don't get out of jail, and those decisions can't be explained by anyone in a meaningful way, such uses of your data interfere with your privacy rights.[87]

In response to these concerns, some experts want practices implemented that foster greater transparency on the part of organizations that develop and use algorithms. Michael Geist believes that we must require "search engines and social media companies to disclose how information is used to determine the content displayed to each user."[88] Similarly, Ms. Steeves stated that the current legislative regime already includes some requirements for algorithmic transparency:

> In a lot of ways, it's already in our legislation.… It's just that so often it's been buried in the algorithm in ways that make it even less transparent, so certainly a number of us within the civil society sector are quite concerned about this and think that it's worth pursuing as a provision in its own right.
>
> A lot of it, too, requires that corporations be much more responsible for the outcomes. Yes, I do think there should be penalties attached when there are discriminatory outcomes in particular, and I think that would create a situation in which people would

86 See ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1635 (Valerie Steeves, Full Professor, Department of Criminology, University of Ottawa, As an Individual).

87 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1635 (Ian Kerr).

88 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1620 (Michael Geist).

> be much more careful when they are running algorithms that really significantly change people's life outcomes.[89]

The Committee is of the opinion that informed consent requires the implementation of measures to improve algorithmic transparency. The Committee would like to see greater transparency on the part of organizations that use algorithms to process Canadians' personal information, which can be achieved either by amending PIPEDA or implementing other measures.

Therefore, the Committee recommends:

Recommendation 3 on algorithmic transparency:

That the Government of Canada consider implementing measures to improve algorithmic transparency.

4. Revocation of consent

A key element of meaningful and informed consent to the collection, use and disclosure of personal information is the ability of individuals to effectively revoke their consent.[90] PIPEDA states that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.[91] Quite often there are "a myriad of circumstances right now in which providing a revocability for a consent process is very difficult in practice."[92] The following is a good example of how withdrawing personal information from social media can be problematic:

> I would think that in a situation where someone had posted something themselves and wanted it removed, and there was no other valid contractual or legal reason an organization should keep or post it, in many cases PIPEDA would now require that it be removed.
>
> I think a lot of social networks actually do operate this way. If you post something to a lot of social networks, you can remove it after you've posted it. It doesn't change the fact that people have seen it, and in some cases might not change the fact that others

89 See ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1715 (Valerie Steeves); PIPEDA, Schedule 1, cls. 4.8 and 4.9.

90 ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1705 (Adam Kardash).

91 PIPEDA, Schedule 1, cl. 4.3.8.

92 ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1705 (Adam Kardash).

> have copied it and distributed it in other ways, but you can pull it off the actual network it's on.[93]

In short, organizations that have collected, used or disclosed personal information generally give effect to the revocation of consent by deleting the information. In the case of simple transactions between individuals and these organizations, it is possible to give effect to a revocation by deleting the personal information at issue. However, in the case of multiple interactions – as on social media – it may not necessarily be possible for the organization to fully implement the revocation of consent, because the individual's personal information may have been copied and distributed to others.

The Committee is cognizant of the fact that the revocation of consent plays a key role in maintaining a viable consent-based privacy model. The Committee also recognizes the difficulties inherent in implementing revocation, difficulties that are closely linked to another issue in this report – the protection of online privacy and reputation. The government must study this issue in order to introduce mechanisms that will clarify how consent can be revoked and the practical and legal consequences of revocation.

Therefore, the Committee recommends:

Recommendation 4 on the revocation of consent:

That the Government of Canada study the issue of revocation of consent in order to clarify the form of revocation required and its legal and practical implications.

D. Exceptions to the general rule of consent

During the study, the Committee heard from many witnesses regarding existing and recommended exemptions to the general rule of consent. This section addresses some of the exemptions that attracted the Committee's attention.

1. "Publicly available information"

Under PIPEDA, it is not necessary to obtain the consent of an individual to collect, use or disclose that individual's personal information, if the information is publicly available and is specified by the regulations.[94] The *Regulations Specifying Publicly Available Information*, which came into force in 2001, set out the types of information and

93 ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1615 (David Elder, Special Digital Privacy Counsel, Canadian Marketing Association).

94 PIPEDA, ss. 7(1)(*d*), (2)(*c*.1) and (3)(*h*.1).

formats that are exempt from the consent requirement. The personal information that is exempt under the Regulations is the following:

> a) personal information consisting of the name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory;
>
> b) personal information including the name, title, address and telephone number of an individual that appears in a professional or business directory, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the directory, listing or notice;
>
> c) personal information that appears in a registry collected under a statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;
>
> d) personal information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document; and
>
> e) personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.[95]

A number of witnesses considered this definition to be obsolete. Linda Routledge, Director, Consumer Affairs, Canadian Bankers Association, described it as out of date because "[t]he current regulations reference the dominant technologies of the early 2000s."[96] Anny Duval, counsel for the Canadian Life and Health Insurance Association (CLHIA), indicated that "[t]he current definition in the *Regulations Specifying Publicly Available Information* no longer reflects reality or the expectations of the individuals it is intended to protect."[97] Ms. Duval suggested that the definition be expanded to cover all

95 *Regulations Specifying Publicly Available Information*, SOR/2001-7.

96 ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1540 (Linda Routledge, Director, Consumer Affairs, Canadian Bankers Association).

97 ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1535 (Anny Duval, Counsel, Canadian Life and Health Insurance Association).

situations where individuals decide to post personal information on a public website.[98] Mr. Watson of ITAC suggested changing the definition to make it technology-neutral, like PIPEDA, so that it can better adapt to technological changes.[99]

The OPC also believes that the Regulations need to be updated, but it expressed the following reservations:

> However, we caution against the common misconception that simply because personal information happens to be generally accessible online, there is no privacy interest attached to it.
>
> The issue of deciding how to protect the privacy interest of people whose information is accessible to the public is extremely complex.… Ultimately, however, given the importance of this issue, it would not suffice to merely tweak the existing Regulations by the Governor-in-Council. Rather, the matter merits the further attention of and deliberation by Parliament as these issues will require a careful reflection and balancing of fundamental individual and societal rights.[100]

The Committee agrees that the regulatory definition of publicly available information is obsolete and must be updated. The Committee also believes that the Regulations must be technologically-neutral, like PIPEDA.

Therefore, the Committee recommends:

Recommendation 5 on the *Regulations Specifying Publicly Available Information*:

That the Government of Canada modernize the *Regulations Specifying Publicly Available Information* in order to take into account situations in which individuals post personal information on a public website and in order to make the *Regulations* technology-neutral.

2. Legitimate business interests

A number of witnesses who appeared before the Committee talked about the terms under which personal information can be used to satisfy legitimate business interests. At present, subject to limited and specific exemptions, PIPEDA provides that organizations cannot require an individual to consent to the collection, use, or disclosure of personal information "beyond that required to fulfil the explicitly specified, and legitimate

98 Ibid.

99 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1550 (Robert Watson); ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1610 (Adam Kardash).

100 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 27.

purposes"[101] and that organizations can collect, use, or disclose personal information only "for purposes that a reasonable person would consider are appropriate in the circumstances."[102] However, as the OPC indicated, it is often difficult to seek and obtain express consent in certain situations, for example in the use of search engines, in the context of big data, and when new possibilities for use arise after the initial collection of the data.[103]

In light of this situation, some witnesses called for a new exemption to the rule of consent for legitimate business interests based on the European model, which allows businesses to use personal information without consent if the processing of that data is necessary for the purposes of their legitimate interests.[104] Ms. Routledge from the Canadian Bankers Association described the proposed exemption as follows:

> We suggest that one way to address this concern may be to streamline privacy notices so that consent is not required for uses that the individual would expect and consider reasonable. In particular, we support the concept that express consent should not be required for legitimate business purposes. Some examples of such purposes might include the purposes for which personal information was collected, fulfilling a service, understanding or delivering products or services to customers to meet their needs, and customer service training.[105]

According to Ms. Routledge, this exemption to the rule of consent would be beneficial for consumers in that it would greatly simplify privacy notices and thereby facilitate a more informed consent process.[106] She said that this would allow consumers to "focus on the information that is most important to them and on which they can take action."[107]

However, the OPC does not believe such an exemption is a good idea. In its 2016–2017 annual report, the OPC gave two reasons why it disagreed with creating a general "legitimate interest" exception. First, the OPC felt that the concept of legitimate interests is too broad since it could include circumstances where "an exception to

---

101 PIPEDA, Schedule 1, s. 4.3.3.

102 PIPEDA, s. 5(3).

103 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 15.

104 ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1535 (Frank Zinatelli); ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1600 (Adam Kardash).

105 ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1540 (Linda Routledge).

106 Ibid.

107 Ibid.

consent is not necessary."[108] Second, the OPC believes that the risk that organizations might abuse the new concept of "legitimate interest" is too great precisely because the concept is too broad.[109] However, the OPC did say that several members of the industry who participated in its study on consent indicated that it might be appropriate to apply the concept of implicit consent to these situations.[110] The OPC stated that there were also "arguments in favour of a broad description of purposes (such as 'improving customer service') which would authorize organizations to use the information for purposes not known at the time of collection."[111]

The Committee is of the opinion that measures must be taken to respond to existing concerns regarding the acceptable use of personal information to satisfy legitimate business interests. However, the Committee shares the concerns expressed by a number of witnesses regarding the implementation of a new exemption to the rule of consent for legitimate business interests.

Therefore, the Committee recommends:

Recommendation 6 on legitimate business interests:

That the Government of Canada consider amending the *Personal Information Protection and Electronic Documents Act* in order to clarify the terms under which personal information can be used to satisfy legitimate business interests.

3. Depersonalization

The Committee also considered the collection, use and disclosure of depersonalized data (also known as "anonymous" or "de-identified" data), in other words, data that has been aggregated and presented in such a way that it is impossible to identify the owner. When it comes to privacy protection, the OPC believes that there are advantages and disadvantages to depersonalization:

> On the one hand, the process of de-identification can be used to strike a balance between protecting personal information and the organizations' desire to use personal information in new and innovative ways. On the other hand, there were concerns that it

108 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 28.

109 Ibid.

110 Ibid., p. 18; ETHI, Brief submitted by the Canadian Marketing Association, May 2017.

111 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 15.

> may simply not be possible to render personal information fully non-identifiable without any residual risk of re-identification.[112]

There is some debate over whether depersonalized data should be considered personal information under PIPEDA. Ms. Bernier is of the opinion that, like Europe, Canada should specify in its legislation that "anonymization is a way to exclude personal information from application of the act."[113] Others believe that, although this data may be subject to the Act, it should be exempt from the consent requirement.[114]

In its 2016–2017 annual report, the OPC stated that this is a complex issue and that it intended to publish a document offering guidance on the de-identification of data.[115] Moreover, the OPC encouraged Parliament "to examine this emerging issue, which has the potential to provide the flexibility needed to achieve a better balance between privacy protection and economic value of data."[116] That being said, the OPC believes that depersonalization "can be a viable solution provided it is managed appropriately."[117]

The Committee is aware of the importance of protecting depersonalized data and implementing measures to minimize the risk of re-identification. Creating an exception to the rule of consent regarding depersonalized data is one possibility, but the Committee believes that it would be premature to recommend such an approach at this time.

Therefore, the Committee recommends:

Recommendation 7 on depersonalized data:

That the Government of Canada examine the best ways of protecting depersonalized data.

---

112 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 14. With regard to the risk of re-identification, see also ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2017, 1530 (Mr. Drew McArthur, Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia).

113 ETHI, *Evidence*, 1st Session, 42nd Parliament, February 14, 2017, 1545 (Ms. Chantal Bernier, Counsel, Global Privacy and Cybersecurity Group, Dentons Canada).

114 See, in particular, ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1550 (Mr. Randy Bundus, Senior Vice-President, Legal and General Counsel, Insurance Bureau of Canada); ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1600 (Mr. Adam Kardash, Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP, Interactive Advertising Bureau of Canada).

115 OPC, *2016-17 Annual Report to Parliament*, September 2017, p. 26.

116 Ibid., p. 27.

117 Ibid., p. 26.

4. Financial crime

Following an amendment to PIPEDA in 2015, organizations may now disclose personal information without consent to another organization in certain circumstances, such as cases related to an investigation or fraud.[118] In committee, Ms. Routledge of the Canadian Bankers Association stated that fraud is not the only financial crime that financial institutions have to deal with and for which information sharing is important. She said that fraud "does not include other types of criminal activity such as theft of data or personal information, money laundering, terrorist financing, cybercrime, and even bank robbing."[119]

In order to address this gap in PIPEDA, Ms. Routledge recommended replacing the word "fraud" with "financial crime" and that this term be defined in the legislation in such a way as to include the following:

> first, fraud; second, criminal activity and any predicate offence related to money laundering and the financing of terrorism; third, other criminal offences committed against financial institutions, their customers, and their employees; and fourth, contravention of laws of foreign jurisdictions including those relating to money laundering and terrorist financing.[120]

According to Ms. Routledge, such a change would help banks to better combat financial crime.[121] The Committee agrees and it therefore recommends:

Recommendation 8 on financial crimes:

a) That paragraph 7(3)(d.2) of the *Personal Information Protection and Electronic Documents Act* be amended to replace the term "fraud" with "financial crime."

b) That the definition of "financial crime" in the Act include:

- **fraud;**
- **criminal activity and any predicate offence related to money laundering and terrorist financing;**

118 PIPEDA, par. 7(3)(*d*.2).

119 ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1545 (Linda Routledge).

120 Ibid.

121 Ibid.

- **all criminal offences committed against financial service providers, their customers or their employees;**

- **the contravention of laws of foreign jurisdictions, including those relating to money laundering and terrorist financing.**

E. Consent and the protection of minors

Applying the consent-based model for protecting personal information poses a unique challenge in the case of minors. Many witnesses shared their concerns about young people's awareness of the issues related to the protection of personal information and their ability to consent to the collection, use and disclosure of that information.

During a study conducted in the fall of 2016, Ms. Steeves noted that none of the 13- to 16-year-olds she met with knew about fair information practices or remembered consenting to the collection of their information when they signed up for various social media platforms or posted information on them.[122] She stated that these young people believe privacy policies "have been purposely written to obfuscate and confuse them, so they won't know what's happening, and so they will feel powerless."[123] Ms. Steeves also told the Committee that there is a large gap between young people's expectations and reality:

> In 2015 we surveyed 5,500 kids between the ages of 10 and 17 across the country. We asked them, 'Who should be able to see what you post online?' and 83% of them said that the corporations that own the platforms where they're posting the information should not have access to it.… And 95% said that marketers should not be able to see what they post.…
>
> I think this brief snapshot really strongly suggests that there is a disconnect between the regulatory model and the lived experiences of the people who play, shop, go to school, and hang out on these platforms.[124]

There are also concerns regarding the age at which adolescents are considered mature enough to give their consent for the collection, use or disclosure of their personal information.[125]

---

122 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1630 (Valerie Steeves).

123 Ibid.

124 Ibid.

125 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1655 (John Lawford).

In response to these concerns, many witnesses proposed introducing a minimum age at which an individual can give valid consent to disclose personal information. A number of witnesses suggested a minimum age of 16,[126] which is generally consistent with the European regulations. For anyone under the age of 16, consent would have to be given by the parents, and that parental consent would have to be verifiable:

> Any method to obtain verifiable consent should be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent or legal guardian. While the age of 16 is not a magic number, it is consistent with domestic laws as well as international laws, such as the GDPR. In relation to the approach to obtain the consent of the parent or guardian, our recommendations are consistent with the U.S. FTC's children online protection rule as well as the GDPR requiring organizations to make reasonable efforts to obtain verifiable parental consent, taking into consideration the available technologies.[127]

Owen Charters, President and Chief Executive Officer, Boys and Girls Clubs of Canada (BGCC), proposed prohibiting the collection, use and disclosure of personal information from children under the age of 13. He believes that they are simply "too young to understand the implications of data collection and use."[128] Mr. Charters also noted that the United States has a law that deals specifically with privacy protection for minors, the *Children's Online Privacy Protection Act*, which requires parental consent for collecting personal information from children under the age of 13. Moreover, in Europe, the GDPR requires parental or guardian consent to access online services for children under the age of 16, or a younger age provided that it is not below 13.[129] According to Dennis Hogarth of the Consumers Council of Canada, "Without some form of reliable registry system to verify age, controls will be hard to implement without generating new privacy concerns."[130]

---

126 See for example Ibid.; ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1555 (Dennis Hogarth, Vice-President, Consumers Council of Canada); ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1635 (Paige Backman, Partner, Aird and Berlis LLP, As an Individual); ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1535 (Owen Charters, President and Chief Executive Officer, Boys and Girls Clubs of Canada).

127 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1635 (Paige Backman).

128 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1535 (Owen Charters).

129 Ibid., 1655.

130 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1555 (Dennis Hogarth).

However, Mr. Karanicolas of the CLD noted that it is currently possible to spoof age verification systems, which makes it somewhat meaningless to introduce a minimum age of consent.[131]

Finally, former commissioner Stoddart expressed some reservations regarding the introduction of regulations specifically targeting minors, because such matters may fall under provincial jurisdiction. According to Ms. Stoddart, in order to avoid jurisdictional disputes, it would be better to address the issue of minors "from the angle of strengthening the principle of consent" rather than introducing a specific age for consent.[132]

Given how much young people use information technologies and given that they are a particularly vulnerable group when it comes to privacy protection, the Committee is of the opinion that special measures should be introduced to govern their ability to provide valid consent. Measures should also be put in place to limit the ability of organizations to collect, use and disclose the personal information of minors.

Therefore, the Committee recommends:

Recommendation 9 on specific rules of consent for minors:

That the Government of Canada consider implementing specific rules of consent for minors, as well as regulations governing the collection, use and disclosure of minors' personal information.

F. Data portability

As stated earlier, the principle of consent is based largely on the idea that individuals must remain as free as possible to use their personal information as they wish. However, this freedom should not be limited to the ability to consent to the collection, use and disclosure of their personal information or to withdraw that consent. The Committee believes that it is just as important for individuals to be able to transfer their personal information between service providers so it can be reused.

This right to "data portability" is recognized in the EU by article 20 of the GDPR, which provides a number of situations where

131 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1635 (Michael Karanicolas).

132 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1710 (Jennifer Stoddart, As an Individual).

> [t]he subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.[133]

The right to data portability implies that service providers must ensure that their processes for collecting and storing personal information are sufficiently compatible with their competitors' processes so that users can request and ensure the transfer of their information from one provider to another.

The Committee is of the opinion that such a right should be explicitly recognized in PIPEDA.

Therefore, the Committee recommends:

Recommendation 10 on data portability:

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* to provide for a right to data portability.

PART 3: ONLINE REPUTATION AND RESPECT FOR PRIVACY

Protection of online reputation and respect for privacy are major issues when it comes to protecting personal information. The permanence of information posted online can have a major impact on reputation and raises questions about whether Canadians' privacy is truly protected under PIPEDA. In this report, the Committee addresses two issues regarding the protection of online reputation and respect for privacy. First, it will look at data permanence and the right to be forgotten. Second, the Committee will consider the concept of privacy by design.

At this time, it is worth pointing out that PIPEDA does not operate in a vacuum when it comes to the protection of online reputation. As Ms. Bernier said, a number of federal and provincial laws come into play.[134] Online reputational damage that occurs within the framework of personal relationships rather than commercial transactions does not fall under PIPEDA, but generally under provincial legislation governing tort and civil

133 General Data Protection Regulation, Reg 2016/679 (EU), art. 20.

134 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1550 (Chantal Bernier).

liability.[135] What is more, at the federal level, the *Criminal Code* provides for a number of applicable offences, including the publication of intimate images without consent, which is addressed in section 162.1.[136] As a result, this section of the report will focus mainly on protecting privacy and online reputation in the context of commercial transactions.

A. The right to be forgotten

The advent of new information technologies has a significant impact on the protection of reputation and privacy given how easy it is to search for and access information, and given the permanence of personal information online. This situation can have a major impact on online reputation, particularly when it comes to minors. As the OPC explained, "The permanence of online information means that time does not erase past misdeeds and poor decisions."[137]

This issue gave rise to the right to be forgotten, which originated primarily in Europe and involves measures to prevent information that could be harmful to a person's reputation from haunting them indefinitely. Although "the right to be forgotten" is a popular term, it is unclear and usually refers to one of the following two concepts:

- the *right to erasure*, namely, the right to have information removed from a website; or

- the *right to de-indexing* (some witnesses also referred to this as the right to "dereferencing" or the right to "delisting"), namely, the right to have a website containing personal information removed from the results of search engines such as Google.

1. The right to erasure

PIPEDA currently contains very limited provisions regarding the deletion, correction or accuracy of personal information.

Regarding information disclosed to service providers by individuals themselves, PIPEDA provides individuals with the option to withdraw their consent and to have their

135 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1550 (Chantal Bernier). Ms. Bernier noted that British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador passed laws under which the violation of privacy can be an actionable tort. In Quebec, a judge can prescribe measures to stop harm to online reputation.

136 *Criminal Code*, R.S.C. 1985, c. C-46, s. 162.1.

137 OPC, Online Reputation: What are they saying about me?, January 2016; ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1545 (Robert Watson).

personal information deleted except in certain situations, such as when there are contractual provisions to the contrary.[138] When someone wishes to remove personal information they posted on social media, for example, that person has the absolute right to do so.[139] The legislation also provides that "[p]ersonal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous."[140]

The situation becomes more complex when it comes to the removal of personal information about an individual when it was disclosed to a service provider by someone else. An example of such a situation would be a photo or message posted by a third party on social media or an independent publication containing personal information. In these situations, PIPEDA provides very few tools permitting an individual to have information that was published without their initial consent deleted.[141] Clause 4.9.5 of PIPEDA's Schedule 1 provides that organizations must correct inaccurate, incomplete or out-of-date information, and section 5(3) provides that organizations may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. According to the OPC, these two provisions could be used in order to have certain personal information published by a third party deleted in circumstances limited by these two provisions.[142] Otherwise, PIPEDA does not provide the right to have information deleted that was published by a third party, who is protected by the freedom of expression guaranteed by subsection 2(*b*) of the *Canadian Charter of Rights and Freedoms*.

The Committee also noted that there is at least one Canadian court decision in which the court ordered the removal of data published on the Internet because it violated PIPEDA, and that is the recent decision of the Federal Court in *A.T. v. Globe24h.com*.[143] In that case, the Federal Court ordered that a Romanian-based commercial website remove all Canadian court and tribunal decisions containing personal information since it found that the information was not being used for appropriate purposes under

138 PIPEDA, Schedule 1, cl. 4.3.8; OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

139 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0930 (Daniel Therrien).

140 PIPEDA, Schedule 1, cl. 4.5.3; OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

141 Ibid.

142 OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

143 *A.T. v. Globe24h.com*, 2017 FC 114.

section 5(3) of PIPEDA.[144] The Committee is, however, aware that this is an isolated decision and that the respondent did not participate in the proceedings.[145]

Although PIPEDA provides some tools for the removal of personal information, it is far from a comprehensive regime and does not allow for redress in cases where truthful yet potentially harmful information is posted online by third parties.[146] This could include things such as embarrassing acts or photos, but also certain acts of cyberbullying or revenge porn. The presence of such information on the Internet could have serious consequences for those affected, particularly if they are minors. Ms. Backman raised this issue in her testimony:

> There are significant benefits to children and youth engaging in online resources through social media. However, an error in judgment of a minor, or judgment of another that involves the information of a minor, can have significant short-term and long-term consequences for both the minor and society. More frequently, we are seeing that an online footprint, whether placed there by the individual, the minor or child themself, or someone else, can be central to online bullying. Such bullying can significantly impact the physical and mental health of the child and can lead to long-term consequences for both the minor and society.[147]

Given the gaps in PIPEDA, many witnesses recommended that Canadian law recognize a right to erasure similar to that recognized in the EU under the GDPR, which will come into force in May 2018.[148] The GDPR gives individuals the right to the erasure of their personal data, including:

- when that data is no longer necessary;
- when the data subject withdraws consent and there is no legal basis preventing removal;
- when the data subject objects to the processing and there are "no overriding legitimate grounds" for the data to be kept; and

144 Section 5(3) of PIPEDA provides that an organization "may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

145 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1625 (David Fraser).

146 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2017, 1530 (Drew McArthur).

147 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1635 (Paige Backman).

148 General Data Protection Regulation, Reg 2016/679 (EU).

- when the data has been unlawfully processed.[149]

The GDPR does, however, provide for some exceptions to that right, namely, to allow organizations to comply with their legal obligations and prevent infringement of the right to freedom of expression, freedom of the press, and the right to information.[150]

Those in favour of incorporating a right to erasure into PIPEDA believe that, like the strengthening of consent, it is an effective way of giving individuals more control over their personal information. As Alysia Lau, Legal Counsel, Public Interest Advocacy Centre (PIAC), said, "Canadians must have choice and control over the ways their personal data is used, including through consent, rectification of information, and especially the removal or erasure of their information."[151] Ms. Scassa agreed. She believes that data erasure is important when a person no longer wants to do business with a private-sector organization, for example, a networking site.[152] Kristjan Backman of the National Association for Information Destruction–Canada (NAID) stated that a clear legislative framework for the destruction of information that is no longer needed would be an effective way of ensuring that "private, personal, and business information is not used for purposes other than for which it was originally intended."[153]

The right to erasure is considered important in preventing minors' errors in judgment – for example posting inappropriate photos online – from having serious short- and long-term consequences. This concern was raised in particular by Mr. Charters of the BGCC, who supports a right to erasure for minors when they reach the age of majority:

> [T]he choices [children] ma[k]e while under the age of majority are not reflective of the identity and choices they will make once they have reached the age of majority. While we know there are also many out there who would like their online life to be erasable and forgotten, children should actually be able to benefit from this right.[154]

149 Ibid., art. 17(1); ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1605 (Alysia Lau, Legal Counsel, Public Interest Advocacy Centre).

150 General Data Protection Regulation, Reg 2016/679 (EU), art. 17(3); ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1615 (Florian Martin-Bariteau, Assistant Professor, Common Law Section, Faculty of Law, and Director, Centre for Law, Technology and Society, University of Ottawa, As an Individual).

151 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1605 (Alysia Lau).

152 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1610 (Teresa Scassa) and 1615 (Florian Martin-Bariteau).

153 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1545 (Kristjan Backman, Chair, National Association for Information Destruction - Canada).

154 Ibid. (Owen Charters).

Ms. Backman, who is in favour of recognizing a limited right to erasure for minors, also believes that this would be a good way to mitigate the risks associated with minors' use of websites that collect their personal information.[155]

Some witnesses expressed doubts about the ability to strike a balance between a right to erasure and the right to freedom of expression guaranteed under the *Canadian Charter of Rights and Freedoms*,[156] since any measure that would restrict the ability to publish information on the Internet could be considered to infringe on freedom of expression. This raised the question as to whether it is possible to create a right of erasure that would protect privacy without infringing on freedom of expression, or that would at least constitute a reasonable limit on that right under section 1 of the Charter. Robert Dickson, Former Saskatchewan Information and Privacy Commissioner, told the Committee that he believed a right to erasure would not survive a Charter challenge.[157]

However, other witnesses, including Ms. Bernier, believe that it is possible to formulate a right to erasure that is consistent with the Charter:

> I believe the right to erasure … can be framed in such a manner that it would protect privacy without infringing upon freedom of expression, as, in fact, in my view, the Protecting Canadians from Online Crime Act does as well. In the latter act, we criminalize an expression, if you can say so—for example, putting someone's intimate images without consent on the web. So far, it has not been challenged or not been declared unconstitutional, because the privacy violation is so egregious as not to warrant freedom of expression at large.[158]

During his appearance before the Committee, Commissioner Therrien drew a useful distinction between the removal of factual information – which can at least be held to a certain standard of accuracy – and the suppression of opinions – an issue that falls more clearly under freedom of expression.[159] In his view, erasure should apply to the publication of facts and could be a quicker and more effective solution than other traditional remedies, such as suing for defamation before the courts.[160] However, as

---

155 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1635 (Paige Backman); ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1725 (Valerie Steeves).

156 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0850 (Daniel Therrien).

157 See ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Robert Dickson, Consultant, Former Saskatchewan Information and Privacy Commissioner, As an Individual).

158 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1705 (Chantal Bernier).

159 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0950 (Daniel Therrien).

160 Ibid.

stated by Commissioner Therrien, any taking down of information must consider the interests of third parties who published it and their right to freedom of expression.[161]

A right to erasure would nevertheless have to be carefully framed in order to strike an appropriate balance between freedom of expression and protection of privacy. For example, Ms. Bernier suggested avoiding giving the platforms the discretionary power to determine when to remove information and to instead leave it up to the courts to decide whether a display of personal information constitutes a violation of privacy and should therefore be removed.[162] While he did not comment specifically on the relevance of a right to erasure, Mr. Karanicolas of the CLD also shared with the Committee the importance of due process as carried out by a court or a quasi-judicial authority.[163]

Furthermore, in order not to infringe on freedom of expression, a limited right to erasure must focus mainly on the information referred to in PIPEDA, namely, personal information that is collected, used and disclosed in the course of commercial activities. The purpose of a right to erasure is not to give people absolute control over their online reputations.[164] As Florian Martin-Bariteau, Assistant Professor, Faculty of Law, University of Ottawa, stated, recognition of a right to erasure should not allow individuals to require newspapers to delete articles or information in their archives: "I don't see why today, because it's facilitated by technology, we would allow actions like that, which would erase the memory."[165] The Association of Canadian Archivists (ACA) agrees. Greg Kozak, who testified on behalf of the ACA, believes that it is essential that a right to erasure not unduly interfere with preserving the integrity and authenticity of public documents and that "the test to determine reputational harm must be clear, and the bar should be set high enough to remove frivolous or inconsequential requests."[166]

After considering all of the testimony heard throughout the study, the Committee is of the view that it is important to include a more robust data erasure regime in PIPEDA in order to protect Canadians' privacy. The Committee believes that, in general, individuals should have the right to have their personal information removed when they end a business relationship with a service provider or when the information was collected, used or disclosed contrary to PIPEDA. The Committee also notes that the right to erasure

161 Ibid., 0935.

162 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1550 (Chantal Bernier).

163 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1535 (Michael Karanicolas).

164 Ibid.

165 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1655 (Florian Martin-Bariteau).

166 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 June 2017, 1545 (Greg Kozak, Representative, Ethics Committee, Association of Canadian Archivists).

is not a concept that is foreign to PIPEDA, but that it must be clarified and strengthened. While the Committee is aware that there could be conflict between the recognition of this right and freedom of expression, the Committee also believes that it is possible to somewhat expand the right to erasure by using the GDPR as a model in order to better protect Canadians' privacy while respecting the Charter. Specifically, the Committee believes that, in the case of young people, balancing freedom of expression and privacy should focus on establishing a more robust right to erasure, to have personal information posted online either by themselves or through an organization taken down.

Therefore, the Committee recommends:

Recommendation 11 on the right to erasure:

That the Government of Canada consider including in the *Personal Information Protection and Electronic Documents Act* a framework for a right to erasure based on the model developed by the European Union that would, at a minimum, include a right for young people to have information posted online either by themselves or through an organization taken down.

2. The right to data de-indexing

In addition to the right to erasure, the other concept associated with the right to be forgotten is the right to de-index websites containing personal information. Unlike the right to erasure, de-indexing is not a matter of deleting the information in question. Rather, it involves ensuring that the information no longer appears in the results of search engines such as Google, thus making it harder to find. As Donna Bourne-Tyson, President, Canadian Association of Research Libraries (CARL), explained:

> In effect, delisting removes information from the public view obtained through a simple keyword search, but does not actually remove it from the reach of the more skilled and persistent researcher, who may also search for repositories that are not indexed by search engines.[167]

Like the right to erasure, the right to de-indexing can allow individuals to dissociate themselves from past errors in judgment or from publications reporting false accusations or other potentially damaging information. In such cases, de-indexing makes it more difficult for people to access certain legitimately published third-party websites. For example, an individual who was pardoned for a crime could ask that any newspaper articles referring to that episode in his life be de-indexed so that typing his name into a

167 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 June 2017, 1535 (Donna Bourne-Tyson, President, Canadian Association of Research Libraries).

search engine would no longer bring up the articles. They would still be available on the Internet and accessible through other means, and any court decision on the case would continue to be accessible in case law databases, which are not indexed on Internet search engines. This is an effective way to counter data permanence, while allowing the de-indexed information to remain in the public domain. Jane Bailey, a professor in the Faculty of Law at the University of Ottawa, said that "practically speaking, most people are not going to go to more trouble than a Google search. If that link is no longer something that pops up in a Google search, you get effective, practical obscurity from that kind of measure, without the downside."[168]

As Ms. Steeves indicated, it is about striking a balance between the individual's interest in moving on from past mistakes and the public's interest in having access to certain information:

> I think that the right to be forgotten, as it's been articulated in Europe, is really about ease of access, especially if there's a public benefit to having that ease of access. Then that's part of the balancing. But even if you look at court records, court records have to be public because justice has to be public. It has to be seen as having been done. But when they started putting up matrimonial matters, and neighbours were looking up neighbour to see how much somebody made, it created all sorts of problems, so they took that off the Internet. It's still public; it's still available. That ease of access is what was causing the problem.[169]

In 2014, the Court of Justice of the European Union (CJEU) ruled on the issue of de-indexing in *Google Spain v. AEPD and Mario Costeja González (Google Spain)*.[170] In that case, the Court found that search engines, such as Google, must consider requests made by individuals to remove certain websites from the search results that appear when their name is searched. In interpreting Directive 95/46/EC on the protection of personal information (soon to be replaced by the GDPR), the Court found the following:

> [E]ven initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.[171]

---

168 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1605 (Jane Bailey, Professor, Faculty of Law, University of Ottawa, As an Individual).

169 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1700 (Valerie Steeves).

170 *Google Spain v. AEPD and Mario Costeja González*, ECLI:EU:C:2014:317.

171 Ibid., para. 93.

In regard to that decision, Mr. Karanicolas told the Committee that Google had received approximately 348,000 requests to remove links and that between 150,000 and 170,000 websites had been removed from search results.[172] If a person's request for removal is denied, they can seek recourse through the courts.

Canada does not have an explicit de-indexing regime like the EU. In its draft position, the OPC recommended an interpretation of PIPEDA that would require search engines to remove links in certain circumstances.[173] In answer to a question from the Committee, Commissioner Therrien agreed however that this interpretation does have its critics and that it would be worth clarifying PIPEDA in this respect.[174]

However, as Ms. Stoddart explained, something similar to de-indexing does exist in Canadian law. For example, she told the Committee that when individuals are pardoned of a crime, those records become less accessible.[175] Moreover, in 2017, the Supreme Court found in *Google Inc. v. Equustek Solutions Inc.* that it was possible for a Canadian court to grant a worldwide interlocutory injunction against a search engine in order to have it delist websites.[176] It is important to note, however, that this court proceeding was not initiated under PIPEDA or another privacy regime; rather, the application for an interlocutory injunction was presented as part of trade litigation related to the unlawful acquisition of confidential information and trade secrets.

The Committee heard from many witnesses on the possible recognition of a right to de-indexing in PIPEDA. With regard to minors, Ms. Steeves told the Committee that the right to delink information was "absolutely crucial."[177] She believes it is very important for young people who are saying, "'Oh, something I did when I was 16 is going to sink me, and I will never be able to get over it'."[178] Ms. Bourne-Tyson of CARL thinks that a limited right to de-indexing could be appropriate. She said that "[t]he removal of links to references to a minor juvenile crime or to sexually explicit photographs of a private citizen are examples of a proper application of the right to be forgotten," but that there are some grey areas that must be taken into account, such as information regarding a

172 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1600 and 1610 (Michael Karanicolas).

173 OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

174 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0900 (Daniel Therrien).

175 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1650 (Jennifer Stoddart).

176 *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34.

177 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1635 (Valerie Steeves).

178 Ibid.; ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1620 (Jennifer Stoddart).

company's bankruptcy.[179] Mr. Kozak of the ACA believes that de-indexing could be a worthwhile alternative to the erasure of information since it would allow the information in question to remain part of the public record while limiting the harm done to individuals. He also believes that de-indexing would make it possible for information with archival value to become more accessible once some time has passed and the risk of harm has diminished:

> In cases where the harm to reputation diminishes over time, and certainly with deceased individuals, would we want to completely destroy listings or records? De-indexing might be a solid way of achieving that middle ground, of concealing it during a period of sensitivity, with mindfulness that this information is part of the public record and might eventually come back into the public record in a more accessible format.[180]

The concerns that were raised in committee regarding Europe's right to de-indexing model mainly had to do with the fact that the private sector is responsible for administering it. Colin McKay of Google Canada told the Committee that the decision in *Google Spain* forced Google into a "position of staffing up and running an office that then makes a decision about whether or not a request to delist a URL from search results is in fact appropriate, based on the laws of 21 different jurisdictions."[181]
Mr. McKay also expressed doubts about the ability of a private stakeholder to strike an acceptable balance between the interests in question when deciding on requests for de-indexing:

> [T]here are people who have childhood criminal records or were indiscreet in university, and then there are people who have explicit corruption convictions or other violent crimes, or more simply, who have a history of poorly stated and poorly thought out political or personal beliefs. It's a difficult role for the private sector to be the adjudicator on that.[182]

Mr. Karanicolas agreed. He believes that private sector companies, such as Google, are not equipped to take into account the public interest, including freedom of expression, which could result in "a tendency to remove information whenever there's a complaint."[183]

---

179 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 June 2017, 1535 (Donna Bourne-Tyson).

180 Ibid., 1630 (Greg Kozak).

181 Ibid., 1610 (Colin McKay, Head, Public Policy and Government Relations, Google Canada).

182 Ibid.; ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1540 (Robert Ghiz, President and Chief Executive Officer, Canadian Wireless Telecommunications Association).

183 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1600 and 1610 (Michael Karanicolas).

While Commissioner Therrien fully acknowledges that there are legitimate concerns about having the private sector administer a right to de-indexing, he urged the Committee not to underestimate the practical benefits of this solution.[184] He pointed out that these organizations already have obligations under PIPEDA requiring them to exercise judgment and balance a variety of interests, particularly copyright.[185] He added, "[f]rankly, I don't see why the compliance with the federal private sector privacy law would be any different than an infringement of copyright or other laws."[186] The OPC considers it "appropriate to have search engines providing the first level of review of a de-indexing request."[187]

One way of addressing concerns about the role of the private sector is to adopt a solid legislative framework and have an objective third party with the proper expertise implement it. For example, Ms. Bourne-Tyson and Mr. Karanicolas proposed placing the administration of the right to de-indexing in the hands of a tribunal.[188] Mr. Karanicolas, who did not support recognition of a right to de-indexing, nevertheless believes that the process should be transparent, which includes "making available detailed information about how decision-making processes work and how they have been applied."[189] In order to leverage the practical benefit of the private sector having a role as mentioned by Commissioner Therrien and to reduce the volume of requests, such a tribunal could hear appeals of decisions made by search engines.

Ms. Bailey also believes that the process to create a right to de-indexing should be transparent. However, she thinks that such a right could be administered by service providers if accountability mechanisms are put in place:

> I think the idea of a right to be forgotten that's a practical measure for delinking is actually an interesting practical response, provided that we have some understanding and accountability about how service providers are making these decisions when requested to make these decisions. We need accountability, transparency, and disclosure from them about how many requests they are getting, what the bases of their decision-making are, how many they agree with, how many they dismiss, and

184 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0905 (Daniel Therrien).

185 Ibid., 0920.

186 Ibid.

187 OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

188 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 June 2017, 1535 (Donna Bourne-Tyson); ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1635 (Michael Karanicolas).

189 Ibid.

> those sorts of things. I think that's a practical kind of a right to be forgotten that can give a certain amount of relief.[190]

In its draft position, the OPC presented a non-exhaustive list of factors that could be relevant to assessing a de-indexing request:

- whether the individual concerned is a public figure (e.g. a public office holder, a politician, a prominent business person);
- whether the information at issue relates to a matter of public controversy or debate;
- whether the information relates to an individual's private life as opposed to, for example, their professional or working life;
- whether the information concerns a criminal offence for which the individual has been given a discharge, a pardon, or a record suspension; and
- whether the information relates to a minor….[191]

The Committee believes that implementing a legal framework that would allow individuals to request, in certain specified circumstances, the de-indexing of harmful personal information is a good way of protecting Canadians' reputation and privacy. In order to protect the public interest, as well as freedom of expression, this legal framework would have to provide for a rigorous and transparent decision-making process. In addition, the Government of Canada would have to take into account the unique situation of minors when developing the right to de-indexing.

Therefore, the Committee recommends:

Recommendation 12 on the right to de-indexing:

That the Government of Canada consider including a framework for the right to de-indexing in the *Personal Information Protection and Electronic Documents Act* and that this right be expressly recognized in the case of personal information posted online by individuals when they were minors.

190 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1605 (Jane Bailey).

191 OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

B. Destruction of personal information

Another privacy protection concern raised in the study is PIPEDA's lack of clarity regarding how information – whether on paper or electronic – should be destroyed.

According to Mr. Backman of NAID, this aspect of privacy protection is often overlooked:

> [F]ar too often little attention is paid to the end of a document's life cycle. We see evidence of this on almost a daily basis in the media, with reports of information being left intact and publicly accessible in dumpsters, recycling bins, and discarded electronic devices sent for reuse and recycling.[192]

The presence of personal information on recycled devices and any other improper handling of personal information to be destroyed jeopardizes the privacy of Canadians:

> With destruction more generally, we've had many cases in Canada of sensitive personal files, including those related to youth, being breached through a failure to destroy personal information. This has included medical records and client files from the Children's Aid Society. Again such breaches are potentially devastating for all ages, but more so for youth.[193]

Mr. Martin-Bariteau also stated that "the erasure of data should be compulsory – and not simply recommended – once it is no longer necessary or accurate through stricter controls of the retention of data over time."[194]

In light of this problem, NAID has recommended that PIPEDA be amended to make destruction mandatory and provide a clear definition of the term. In its brief, NAID suggests that the word "destruction" be defined as "the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information (or parts thereof) is not practical."[195] The NAID brief also recommends several other amendments to PIPEDA to clarify the obligation to destroy, including requiring organizations to have a personal information destruction policy as part of their broader privacy policy and imposing an explicit requirement for organizations to destroy information that is no longer needed.[196]

---

192 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1545 (Kristjan Backman).

193 Ibid.

194 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1550 (Florian Martin-Bariteau).

195 ETHI, NAID brief, 8 February 2017, p. 5.

196 Ibid.

The Committee believes that Canadians' privacy can be further protected by strengthening PIPEDA's provisions for destroying personal information that has been collected by businesses and is no longer needed or should otherwise be destroyed. In this regard, the Committee supports the recommendation made by NAID to enhance the PIPEDA provisions pertaining to the destruction of personal information.

Therefore, the Committee recommends:

Recommendation 13 on the destruction of personal information:

That the Government of Canada consider amending the *Personal Information Protection and Electronic Documents Act* to strengthen and clarify organizations' obligations with respect to the destruction of personal information.

C. Privacy by design

One way to improve PIPEDA's privacy mechanisms is to focus on privacy protection right from the design stage of services and systems. "Privacy by design" is meant to ensure that privacy considerations are taken into account at all stages of development, including the design, marketing and retirement of a product. The concept was developed in Canada in the 1990s by Ann Cavoukian, then Information and Privacy Commissioner of Ontario.[197]

Privacy by design seeks to protect personal information by implementing measures proactively and preventively. The approach is based on seven foundational principles:

1) Proactive not Reactive; Preventative not Remedial: The goal of privacy by design is to take preventative action by implementing measures to reduce the risk of privacy infractions.[198]

2) Privacy as the Default Setting: The default setting for all products and services should be to protect personal information so that an individual's privacy is automatically protected without any action being required by the individual.[199]

197 Information and Privacy Commissioner of Ontario, *Privacy by Design, The 7 Foundational Principles*, January 2011; in general, see Ann Cavoukian, *Privacy by Design… Take the Challenge*. Information and Privacy Commissioner of Ontario, 2009.

198 Information and Privacy Commissioner of Ontario, *Privacy by Design, The 7 Foundational Principles*, January 2011.

199 Ibid.

3) Privacy Embedded into Design: The protection of personal information should be an integral part of information systems and business practices; it should not be an add-on.[200]

4) Full Functionality – Positive-Sum, not Zero-Sum: Privacy by design should be considered a benefit; there should be no trade-offs with other features to achieve this goal.[201]

5) End-to-End Security – Full Lifecycle Protection: The protection of personal information must extend throughout the system's entire life cycle.[202]

6) Visibility and Transparency – Keep it Open: Transparency is important to ensure that systems and practices are truly able to protect user privacy; independent verification must always be possible.[203]

7) Respect for User Privacy – Keep it User-Centric: Above all, privacy by design entails putting individuals' interests first.[204]

In the EU, the principles of data protection by design have been written into Article 25 of the GDPR.[205] Giovanni Buttarelli, the European Data Protection Supervisor, explained as follows:

> Privacy by design and privacy by default are no longer recommendations. They are now legal grounds and clear obligations for every controller. It means that systems are to be designed with a user-friendly and less invasive approach. There are obligations addressed to controllers, but there is a system to make designers, producers, and developers engaged in practice.[206]

The Committee believes that privacy by design is an effective way to protect the privacy and reputation of Canadians. This proactive, integrated approach should be at the heart of any PIPEDA review.

---

200 Ibid.

201 Ibid.

202 Ibid.

203 Ibid.

204 Ibid.

205 *General Data Protection Regulation*, Reg (EU) 2016/679, article 25; see also paragraph 78 of the preamble.

206 ETHI, *Evidence*, 1st Session, 42nd Parliament, 13 June 2017, 1240 (Giovanni Buttarelli, Supervisor, European Data Control Supervisor).

Therefore, the Committee recommends:

Recommendation 14 on privacy by design:

That the *Personal Information Protection and Electronic Documents Act* be amended to make privacy by design a central principle and to include the seven foundational principles of this concept, where possible.

PART 4: ENFORCEMENT POWERS OF THE PRIVACY COMMISSIONER

A. Recall of the Committee's recommendation regarding the *Privacy Act*'s enforcement

During its study of the *Privacy Act* in 2016, the Committee examined various overview models that the Office of the Privacy Commissioner could consider for enforcement of the Act. The Committee made the following recommendations:

> 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.[207]

While the *Privacy Act* and PIPEDA establish different obligations for different spheres of activity – one public and the other private – they are both part of the same federal privacy regime administered by the OPC. That is why the Committee believes the recommendations it made in its study of the *Privacy Act* must be taken into account when recommending possible changes to the OPC's overview models for enforcing PIPEDA.

B. Position of the Office of the Privacy Commissioner of Canada

In his brief to the Committee from 2 December 2016, the Privacy Commissioner discussed the appropriateness of the ombudsman model under PIPEDA and possible amendments to the legislation to add further compliance incentives, such as

207 ETHI, *Protecting the Privacy of Canadians : Review of the Privacy Act*, Fourth Report, 1st Session, 42nd Parliament, December 2016, recommendation 15, p. 35.

> statutory damages, order-making powers and/or the power to impose administrative monetary penalties (or some combination thereof), in order to ensure the Commissioner's continued ability to protect individuals' privacy rights in a globalized economy where threats to privacy proliferate.[208]

In 2013, Ms. Stoddart, the former privacy commissioner, made a recommendation to "[s]trengthen enforcement and encourage greater compliance."[209] In her brief, she explained how statutory damages, order-making powers and administrative monetary penalties would apply to PIPEDA.

More recently, the reinforcement of the Commissioner's powers was part of the OPC's consultations on potential enhancements to the consent model under PIPEDA. As well, the Draft OPC Position on Online Reputation states that the rationale and conclusions presented in the OPC consent paper – calling for order-making and fining powers, as well as more formalized powers to act proactively – apply equally to online reputations.[210]

C. Evidence

1. Should the Privacy Commissioner be given new powers?

Appearing on behalf of the Canadian Radio-television and Telecommunications Commission, Steven Harroun said he was convinced that administrative monetary penalties, when used with other enforcement methods, were a deterrent to non-compliance.[211] He advised the Committee that "enforcement agencies need a broad range of tools in their arsenal that they can tailor to the circumstances of each case."[212]

Krista Campbell of Innovation, Science and Economic Development Canada believes that the next statutory review of PIPEDA will focus on choosing between an ombudsman model with powers similar to those currently possessed by the Commissioner and a different type of model.[213]

---

208 ETHI, Brief by the Privacy Commissioner of Canada, 2 December 2016.

209 OPC, *The Case for Reforming the* Personal Information Protection and Electronic Documents Act, May 2013; *Schrems v. Data Protection Commissioner*, C-362/14, 6 October 2015.

210 OPC, *Draft OPC Position on Online Reputation*, 26 January 2018.

211 ETHI, *Evidence*, 1st Session, 42nd Parliament, 9 May 2017, 1555 (Steven Harroun, Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission).

212 Ibid.

213 ETHI, *Evidence*, 1st Session, 42nd Parliament, 9 May 2017, 1605 (Krista Campbell, Director General, Digital Policy Branch, Spectrum, Information Technologies and Telecommunications Sector, Innovation, Science and Economic Development Canada).

> If you give order-making powers but still want to be able to have open conversations with business, saying, 'Come in and talk to us early on and we'll work with you on how you go about designing new products and services,' then having greater order-making power in the same organization could cause some concerns about what the core mandate priorities are. A holistic review of the Office of the Privacy Commissioner and PIPEDA would need to be undertaken before we would decide to give new powers.[214]

During his appearance on 16 February 2017, and in advance of PIPEDA's next statutory review, Commissioner Therrien explained his position on giving enforcement powers to the Privacy Commissioner. He felt the most effective approach would be a combination of order-making powers and the power to impose financial penalties, subject to certain parameters.[215] During his appearance on 1 February 2018, Commissioner Therrien repeated this position, adding that "[i]f organizations know that their interlocutor has order-making powers, I think that it would discipline the conversation."[216]

Like the Commissioner, many witnesses were in favour of changing the current ombudsman model and giving the Commissioner enforcement powers.[217] For example, John Lawford of the Public Interest Advocacy Centre recommended giving the Commissioner real enforcement powers, including the broad discretionary authority to impose administrative monetary penalties or the authority to impose fines.[218] In his view, the authority to impose fines should not be limited to specific circumstances, reserved for the courts or subject to restrictions.[219]

Mr. Dickson, the former Saskatchewan information and privacy commissioner, pointed out that an order-making model combined with the ability to impose penalties could

---

214 Ibid.

215 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1610 (Daniel Therrien).

216 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 February 2018, 0855 (Daniel Therrien).

217 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1640 (Vincent Gogolek); ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2017, 1535 (Drew McArthur); ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1605 (Micheal Vonn, Policy Director, British Columbia Civil Liberties Association); ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1620 (Michael Geist); ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1630 (Ian Kerr); ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1645 (Vincent Gautrais); Option consommateurs, Brief, *Review of the* Personal Information Protection and Electronic Documents Act: *All things come to those…*, 11 May 2017, recommendation 1(n), p. 15; ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1600 (Dennis Hogarth); ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 June 2017, 1645 (Greg Kozak).

218 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1600 (John Lawford).

219 Ibid.

increase the effectiveness of PIPEDA among small and medium-sized enterprises (SMEs) and create a body of precedents.[220]

Mr. Martin-Bariteau recommended that PIPEDA establish a maximum deterrent fine based on a percentage of the organization's worldwide turnover for the previous year and a second threshold amount, the greater of which would be applied.[221] This recommendation is consistent with the EU's GDPR, which is discussed in greater detail in the next part of the report. Mr. Martin-Bariteau specified that the fines under PIPEDA should be payable to the Receiver General and that none of the Commissioner's powers, including those to make orders and impose penalties, should be dependent on the prior receipt of a formal complaint.[222] However, he suggested that these powers be subject to a possible judicial review.[223]

Mr. Martin-Bariteau also recommended giving individuals a statutory right of action that is not subject to a prior complaint to the OPC and is supported by statutory damages, in order to enforce compliance with PIPEDA or to obtain remedies, whichever the case.[224] Mr. Israel of CIPPIC echoed this recommendation and further advised that the Commissioner be authorized to designate transparency reporting obligations for the various sectors under his responsibility.[225]

Ms. Scassa addressed the issue of damages awarded under PIPEDA:

> PIPEDA currently does not provide any guidance as to damage awards. The Federal Court has been extremely conservative in damage awards for breaches of PIPEDA, and the amounts awarded are unlikely to have any deterrent effect other than to deter individuals who struggle to defend their personal privacy. Some attention should be paid to establishing parameters for non-pecuniary damages under PIPEDA. At the very least, these will assist unrepresented litigants in understanding the limits of any recourse that's available to them.[226]

---

220 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Robert Dickson).

221 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1550 (Florian Martin-Bariteau).

222 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1555 (Chantal Bernier). Ms. Bernier made a similar recommendation, stating that the fine in question should be equal to a percentage of the organization's annual revenues

223 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1550 (Florian Martin-Bariteau).

224 Ibid.

225 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1635 (Tamir Israel).

226 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1545 (Teresa Scassa).

Ms. Scassa also recommended that the Commissioner have the authority to impose fines on organizations in cases of substantial or systemic non-compliance with privacy obligations.[227] Similarly, Mr. Israel advocated empowering the Commissioner to impose context-specific restrictions.[228] As he explained, "PIPEDA's recommendation and *de novo* enforcement model is significantly out of touch with the realities of modern data protection."[229]

Colin Bennett, Professor of Political Science at the University of Victoria, recommended that the Privacy Commissioner of Canada be given the same powers as the Information and Privacy Commissioner for British Columbia.[230] In his view, the Privacy Commissioner of Canada must have all the privacy protection tools available, including codes of practice, privacy seals, privacy standards, and privacy impact assessments. He recommended

> a more explicit recognition in section 24 of PIPEDA that the commissioner may encourage these kinds of tools and, in some cases, require the adoption of those accountability mechanisms by Canadian companies and their trade associations. In particular, there is privacy by design and privacy by default.[231]

2. A European perspective on fines

Mr. Buttarelli, the European Data Protection Supervisor, told the Committee that he feels all infringements cannot be treated in the same manner: the seriousness of the infringement must be considered so that the associated penalties are reasonable and credible.[232] As he stated, "We need to avoid a system whereby the fines are simply a

---

227 Ibid.

228 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1630 (Tamir Israel).

229 Ibid., 1635.

230 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1640 (Colin Bennett, Professor, Department of Political Science, University of Victoria).

231 Ibid. Section 24 of PIPEDA concerns promoting the purposes of Part 1 of the Act, which deals with privacy in the private sector, and states as follows:

"The Commissioner shall:

(a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part;

(b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry;

(c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and

(d) promote, by any means that the Commissioner considers appropriate, the purposes of this Part."

232 ETHI, *Evidence*, 1st Session, 42nd Parliament, 13 June 2017, 1320 (Giovanni Buttarelli).

budget line item for a big corporation. We need to increase the amount of fines where and when dispensable, but in the end we need to consider the amount of money and the energy that the controller, in the process, has spent on the case."[233]

3. The application of the law to the specific situation of children

With regard to children, the Boys and Girls Clubs of Canada recommended in its brief to the Committee that the OPC be given "the power to enforce new children's privacy regulations."[234] Speaking before the Committee on 25 September 2017, Mr. Charters of the BGCC explained that it is "not enough to just create these laws. Companies and sites must be monitored and held accountable for their compliance with these provisions."[235]

Mr. Charters gave two examples of the type of requirements he would like to see added to PIPEDA in order to explicitly include children's privacy rights: the U.S. *Children's Online Privacy Protection Act*, which requires parental consent to collect personal information from children under 13; and the GDPR, which requires the consent of a parent or guardian to access online services for children under the age of 16, or a younger age provided that it is not below 13.[236]

4. The point of view of organizations subject to the *Personal Information Protection and Electronic Documents Act*

Looking at the Privacy Commissioner's powers from the other side of the equation, a number of witnesses recommended maintaining the ombudsman model rather than introducing enforcement powers, or they supported enforcement powers with strict

233 Ibid.

234 Boys and Girls Clubs of Canada, Brief, *Protecting children's privacy online*, March 2017, recommendation 4, p. 2.

235 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1545 (Owen Charters).

236 Ibid., 1655.

limits.[237] For example, Ms. Duval of the CLHIA recommended that the ombudsman model be maintained "since it effectively balances individuals' right to privacy and the rights of organizations to use that information legitimately and reasonably in a business context."[238]

Ms. Bernier commented that a comparison of the OPC's enforcement powers with those of similar offices around the world shows that an upgrade appears to be needed, but it should be done within specific parameters.[239] She recommended that the Committee consider empowering the Commissioner to impose fines but only if there is evidence of an organization's negligence. In her view,

> the imposition of sanctions is not necessarily bad for the private sector, because it evens the playing field. You have good organizations that invest the money up front and, therefore, get good results on privacy protection, and you have negligent organizations that fail to make the upfront investments and, therefore, pay the fine at the end. A lot of good organizations will tell you, 'Thank you. You've just evened the playing field.'[240]

On the subject of the OPC's enforcement powers compared with those of other offices around the world, former commissioner Stoddard noted in her 2013 brief that the U.S. Federal Trade Commission has negotiated a number of financial settlements over privacy infractions.[241]

> The United Kingdom, Ireland, New Zealand, and Spain data protection authorities (DPAs) also have order-making power, with the United Kingdom and Spain also having the ability to fine organizations. In the United Kingdom, these stronger enforcement powers

---

237 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1630 (David Fraser); ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1640 (Paige Backman); ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1610 (Alex Cameron, Partner and Chair, Privacy and Information Protection Group, Fasken Martineau DuMoulin LLP); ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1540 (Robert Ghiz); ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1550 (Wally Hill); ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1650 (David Elder); ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1550 (Robert Watson); ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1625 (André Leduc, Vice-President, Government Relations and Policy, Information Technology Association of Canada); ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1610 (Scott Smith, Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce); ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1550 (Randy Bundus); ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1600 (Adam Kardash); ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 June 2017, 1550 (. Jason McLinton, Vice-President, Grocery Division and Regulatory Affairs, Retail Council of Canada); ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 June 2017, 1655 (Colin McKay).

238 ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1540 (Anny Duval).

239 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1555 (Chantal Bernier).

240 Ibid.

241 OPC, *The Case for Reforming the Personal Information Protection and Electronic Documents Act*, 23 May 2013, p. 6.

> have not precluded an ombudsman-like approach, where appropriate, and fines have been issued only where a softer touch has failed.[242]

Ms. Stoddart also noted that, at the time of her brief's publication, Australia had amended its *Privacy Act* to allow its commissioner to accept enforceable undertakings and apply to the federal court to impose penalties of over AUD$1 million on a company.[243]

When asked for examples of other jurisdictions that authorize fining powers and could serve as a model for Canada, Ms. Bernier mentioned the United Kingdom, which allows fines of up to £25,000, and France, which allows fines up to €300,000.[244] Mr. Hogarth argued that the order-making powers in these two countries may seem a bit extreme but they are very effective in ensuring compliance with the law.[245]

The next section of this report will address the new penalties that the EU will soon introduce under the GDPR.

Like Mr. Martin-Bariteau, Ms. Bernier recommended that fines be payable to the Receiver General to prevent any conflict of interest, and that there be a right of appeal to the Federal Court. She also felt that the fine should be a percentage of the organization's annual revenue, similar to the new European regulation, because the use of personal information contributes to an organization's profits. As Ms. Bernier explained:

> [T]he misuse of personal information should be part of financial loss. There is a logic there that I believe recognizes the monetary value of personal information. Secondly, it matches the investment that is required to be made upstream and leaves the issue of damages to the courts, where that would be more appropriately dealt with.[246]

Ms. Gratton expressed concern that statutory damages and other sanctions stifle business innovation, and recommended that "any enforcement powers, penalties, or statutory damages should come into play only once a certain practice is clearly illegal and once the organization has been advised of such and is refusing to adjust its business practices."[247]

---

242 Ibid.

243 Ibid.

244 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1725 (Chantal Bernier).

245 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1710 (Dennis Hogarth).

246 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1555 (Chantal Bernier).

247 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1620 (Éloïse Gratton).

Mr. Karanicolas supported broader investigative powers for the OPC to promote good practice in information management and security. However, he was not convinced that the Commissioner needed order-making powers.[248] He explained that these powers raise issues of procedural fairness in investigations, and that the Privacy Commissioner has previously stated that organizations comply with most of his recommendations.[249]

Ms. Morin of the ABC recommended "maintaining [the ombudsman model] unless, once again, there is evidence that a change to the OPC's enforcement powers is actually needed."[250] She also recommended amending PIPEDA to authorize the OPC "to issue non-binding advance opinions to organizations proposing new programs, technologies, methodologies, or specific transactions."[251] In addition, Ms. Morin said that it would be prudent to wait and see how the OPC's new power to issue and enforce binding compliance agreements through the courts will be interpreted and used, and how the new breach reporting regime, which allows for fines, will unfold in 2018.[252]

Similarly, Molly Reynolds, Senior Associate with Torys LLP, recommended amending PIPEDA to allow the OPC to issue advance compliance rulings.[253] As she explained, advance rulings would lead to four main outcomes:

- Canadians would be better protected;
- the OPC would gain better insight into new technologies;
- there would be greater certainty for all parties involved; and
- private-sector risk assessment would improve.[254]

Ms. Reynolds specified that advance compliance rulings should not be binding.[255]

248 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1530 and 1605 (Michael Karanicolas).

249 Ibid.

250 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1640 (Suzanne Morin).

251 Ibid., 1645.

252 Ibid.

253 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1620 (Molly Reynolds, Senior Associate, Torys LLP).

254 Ibid.

255 Ibid., 1625.

David Young of David Young Law told the Committee that the current ombudsman model is working well.[256] However, he was open to giving the Commissioner order-making powers "if it is determined that the current model does not provide sufficient enforcement tools."[257] In Mr. Young's view, empowering the Commissioner to impose financial penalties "would be a dramatic departure from his existing authority and would not be consistent with an ombudsperson model."[258] However, he proposed adding a provision to impose financial penalties for offences such as an intentional breach of the law. This type of provision would be consistent with the pending offence of failure to comply with breach reporting requirements.[259]

In light of the evidence and briefs presented, the Committee believes there is a demonstrated need to grant the Privacy Commissioner enforcement powers related to PIPEDA. Therefore, the Committee recommends using the system currently in place in the United Kingdom as a model and recommends:

Recommendation 15 on the Privacy Commissioner's enforcement powers:

That the *Personal Information Protection and Electronic Documents Act* be amended to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance.

In addition to recommending that the Commissioner have the power to impose fines, Ms. Stoddart recommended that PIPEDA authorize the Commissioner to choose which complaints to investigate.[260] This power would be accompanied by broad audit or self-initiated investigation powers. She also stated that the OPC should be given more flexibility to implement a wider range of regulatory approaches.[261]

In keeping with Ms. Stoddart's recommendation, the Committee recommends:

256 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1615 (David Young).

257 Ibid.

258 Ibid.

259 Ibid.

260 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1620 (Jennifer Stoddart).

261 Ibid., 1625.

Recommendation 16 on the Privacy Commissioner's audit powers:

That the *Personal Information Protection and Electronic Documents Act* be amended to give the Privacy Commissioner broad audit powers, including the ability to choose which complaints to investigate.

PART 5: ADEQUACY OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* UNDER THE EUROPEAN UNION *GENERAL DATA PROTECTION REGULATION*

A. The European Union *General Data Protection Regulation*

In 1995, the EU adopted a directive – which became applicable in 1998 – concerning the protection of personal data and its free movement within the EU. The directive requires all member states to comply by passing legislation on personal data or by amending existing legislation. Article 25 extends the scope of the directive beyond the EU by prohibiting member states (and companies within their borders) from transferring personal data to any non-member state whose laws do not adequately protect this data.[262]

This directive will be replaced in May 2018 when the GDPR comes into force throughout the EU. Under the GDPR, the EU will have to "assess the adequacy of PIPEDA's protection."[263] According to the Commissioner in his brief to the Committee from 2 December 2016, the GDPR "contains some provisions that did not appear in the current Directive and also do not appear in PIPEDA, such as data portability, data erasure, and privacy by design and default."[264]

The EU institutions have summarized the main provisions of the GDPR and divided them into two categories: citizens' rights and rules for businesses.[265] With regard to citizens' rights, the EU institutions have stated that the GDPR "strengthens existing rights,

---

262 European Parliament, Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995.

263 ETHI, Brief by the Privacy Commissioner of Canada, 2 December 2016; Council of the European Union, *General Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, arts. 103–108.

264 ETHI, Brief by the Privacy Commissioner of Canada, 2 December 2016.

265 Europa, *EU law and publications*, Protection of personal data (from 2018).

provides for new rights and gives citizens more control over their personal data."[266] These rights include:

- **easier access to their data** — including providing more information on how that data is processed and ensuring that that information is available in a clear and understandable way;
- **a new right to data portability** — making it easier to transmit personal data between service providers;
- a clearer **right to erasure ("right to be forgotten")** — when an individual no longer wants their data processed and there is no legitimate reason to keep it, the data will be deleted;
- **right to know when their personal data has been hacked** — companies and organisations will have to inform individuals promptly of serious data breaches. They will also have to notify the relevant data protection supervisory authority.[267]

With regard to the rules for businesses, the EU institutions have stated that the GDPR "is designed to create business opportunities and stimulate innovation"[268] through a number of steps, including:

- **a single set of EU-wide rules** — a single EU-wide law for data protection is estimated to make savings of €2.3 billion per year;
- **a data protection officer**, responsible for data protection, will be designated by public authorities and by businesses which process data on a large scale;
- **one-stop-shop** — businesses only have to deal with one single supervisory authority (in the EU country in which they are mainly based);
- **EU rules for non-EU companies** — companies based outside the EU must apply the same rules when offering services or goods, or monitoring behaviour of individuals within the EU;
- **innovation-friendly rules** — a guarantee that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default);

266 Ibid.

267 Ibid.

268 Ibid.

- **privacy-friendly techniques** such as **pseudonymisation** (when identifying fields within a data record are replaced by one or more artificial identifiers) and **encryption** (when data is coded in such a way that only authorised parties can read it);

- **removal of notifications** — the new data protection rules will scrap most notification obligations and the costs associated with these. One of the aims of the data protection regulation is to remove obstacles to free flow of personal data within the EU. This will make it easier for businesses to expand;

- **impact assessments** — businesses will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals;

- **record-keeping** — SMEs are not required to keep records of processing activities, unless the processing is regular or likely to result in a risk to the rights and freedoms of the person whose data is being processed.[269]

Additionally, the GDPR contains rigorous enforcement measures, such as administrative fines for the most serious infringements of up to €20 million or 4% of the organization's total worldwide annual turnover for the preceding fiscal year, whichever is higher.[270] Moreover, the GDPR will give European supervisory authorities investigative powers – including the power to carry out data protection audits within organizations subject to the GDPR – and the authority to impose a temporary or definitive limitation, including a ban on the processing of personal information.[271]

The Commissioner also referred in his brief from 2 December 2016 to the impact of *Schrems v. Data Protection Commissioner*, in which the CJEU ruled that U.S. legislation does not adequately protect personal data.[272] The *Schrems* decision invalidated the *Safe*

269 Ibid.

270 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Article 83.

271 Ibid., art. 58.

272 ETHI, Brief by the Privacy Commissioner of Canada, 2 December 2016.

Harbour Agreement[273] between the EU and the United States and it also addresses the issue of adequate protection:

> The Schrems decision, of course, demands a more holistic approach to adequacy than what was in force when Canada's PIPEDA was determined "adequate." Now, adequacy is not limited to a consideration of rules that protect personal data in the commercial sphere – one must also carefully consider how rights are protected by laws and practices related to national security and law enforcement.[274]

Given the differences between PIPEDA and the GDPR, and the fallout from the *Schrems* decision, the Commissioner stated that reassessing PIPEDA's adequacy status "is a pressing issue with possible far-ranging implications for Canada's trade relationship with the EU."[275]

B. Evidence

1. Achieving adequacy

During his appearance on 16 February 2017, the Commissioner asked that Committee members consider PIPEDA's adequacy under the GDPR during their study, given the major impact of adequacy on trade and the differences between PIPEDA and the GDPR.[276] He noted that the GDPR will require a review of adequacy decisions every four years, and that Canada's adequacy status, which has allowed data to flow from the EU to Canada since 2001, will have to be revisited.[277] The Commissioner also referred to a January 2017 communication from the European Commission stating that

> Canada's adequacy status is 'partial', in that it covers only PIPEDA, and that all future adequacy decisions will involve a comprehensive assessment of a country's privacy regime, including access to personal data by public authorities for law enforcement, national security, and other public interest purposes.[278]

---

273 The *Safe Harbour Agreement* is a mechanism available to EU businesses to ensure an adequate level of protection when transferring the personal data of EU citizens to the United States. The EU and the United States have reached a new agreement, the *EU–US Privacy Shield*; European Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU–US Privacy Shield," Press release, 2 February 2016.

274 OPC, *The Consent Dilemma: Remarks at the Privacy Laws and Business International Conference*, 5 July 2016.

275 ETHI, Brief by the Privacy Commissioner of Canada, 2 December 2016.

276 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 February 2017, 1540 (Daniel Therrien).

277 Ibid.

278 Ibid.

Ms. Campbell from Innovation, Science and Economic Development Canada called on the government to begin discussions with the European Commission on PIPEDA's adequacy status.[279] However, she made the following point:

> Our privacy regime needs to continue to evolve regardless of what the European Commission does, simply because the Internet of things is coming. Consent among children is a vital issue domestically as well as internationally. We need to make sure our regime is evolving because of changes in technology and the challenges we face—not just because the Europeans are doing it.[280]

Similarly, Ms. Reynolds of Torys LLP suggested that the Committee not focus on

> reforms that would merely encourage an adequacy ruling from the EU, but rather areas in which harmonization of international standards with Canadian privacy law would truly help consumers and businesses protect information more consistently and with more certainty across jurisdictions.[281]

Mr. Buttarelli, the European Data Protection Supervisor, stated that he sees "a line of continuity between current legislation and the future one in making existing and new rights and freedoms meaningful for ordinary people and more effective in practice."[282] He also noted that all existing adequacy decisions will remain in force until they are updated or repealed.[283] He added that the EU is not in a hurry to "put Canada on top of our decisions. You should now verify on the basis of the new, extensive list of criteria now listed in the GDPR for the assessment of that adequacy, what is needed."[284]

Mr. Buttarelli pointed out that the standard for adequacy is now "essentially the equivalent," following the CJEU's ruling in *Schrems*.[285] When considering PIPEDA's adequacy in relation to the GDPR, he recommended that Committee members

> not focus too much on the novelties in the GDPR, such as design, default, and portability. … We would encourage that there be a global approach and that you not have a sort of point-to-point replication of every single rule.… [T]he restrictions,

279 ETHI, *Evidence*, 1st Session, 42nd Parliament, 9 May 2017, 1650 (Krista Campbell).

280 Ibid., 1645.

281 ETHI, *Evidence*, 1st Session, 42nd Parliament, 6 April 2017, 1625 (Molly Reynolds).

282 ETHI, *Evidence*, 1st Session, 42nd Parliament, 13 June 2017, 1210 (Giovanni Buttarelli).

283 Ibid.

284 Ibid.

285 Ibid., 1215.

> exceptions, and derogations for law enforcement are more important than design and default.[286]

In short, law enforcement is Europe's paramount concern, according to Mr. Buttarelli.[287]

A number of witnesses stated that PIPEDA should be amended now in order to align it with the GDPR.[288]

Ms. Stoddart called on Committee members to aim high when considering updates to PIPEDA and to bear in mind that the GDPR also applies European standards to the use of personal information in the public sector.[289] She highlighted the problem resulting from the fact that the adequacy criteria in the GDPR, while more rigorous than those in PIPEDA, are not well defined.[290] As she told the Committee,

> The more serious problem is that in the European Union, in the study I made of all the adequacy decisions that had been made and the ones that had not been made for which analyses had been done, there is a very checkered history of evaluation of countries' personal information protection frameworks.[291]

Ms. Stoddart added that there is significant pressure within the EU to impose European standards on the rest of the world.[292]

In a perspective of trade between Canada and the EU, Ms. Bernier recommended that Canada strengthen its privacy protection measures to an acceptable level before the EU reviews Canada's adequacy status.[293]

Mr. Martin-Bariteau stated that, although the Canadian legislation needs to be updated to meet the GDPR's adequacy test, it is important to remember that the test does not require other laws to be a carbon copy of the GDPR and that it applies to all protection

---

286 Ibid., 1245 and 1250.

287 Ibid., 1250.

288 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2017, 1530 (Drew McArthur); ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2017, 1540 (Jill Clayton, Commissioner, Office of the Information and Privacy Commissioner of Alberta); ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 May 2017, 1600 (Dennis Hogarth).

289 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1620 (Jennifer Stoddart).

290 Ibid.

291 Ibid.

292 Ibid.

293 ETHI, *Evidence*, 1st Session, 42nd Parliament, 14 February 2017, 1650 (Chantal Bernier).

frameworks, not just PIPEDA.[294] In his view, certain amendments to PIPEDA are necessary and would be sufficient to meet the adequacy requirements, such as amendments concerning an organization's retention of data over time and direct rights of action.[295]

Other witnesses called on the Committee to be patient and advised that it would be premature to amend PIPEDA now.[296]

Mr. Bennett of the University of Victoria suggested that PIPEDA be modernized because it needs to be, and not simply for the sake of complying with the GDPR's adequacy requirements, which he considers quite vague.[297] He identified the three most glaring areas of discrepancy between PIPEDA and the GDPR: the Commissioner's enforcement powers; the Commissioner's access to all the privacy protection tools available; and the processing of sensitive data.[298]

2. The importance of enforcement in assessing the adequacy status

Regarding the Act's enforcement, Ms. Scassa noted that the Privacy Commissioner's lack of enforcement powers also constitutes the PIPEDA's greatest weakness vis-à-vis European standards, which echoes the European viewpoint expressed by Mr. Buttarelli previously in this report.[299]

Similarly, Mr. Israel of CIPPIC stated that enforcement could be a problem area in determining PIPEDA's adequacy under the GDPR. As he told the Committee, "[T]hat is one area where we are out of step with other data protection commissioners around the world, and where the EU has made substantive improvements recently."[300]

294 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1550 (Florian Martin-Bariteau).

295 Ibid., 1620.

296 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1645 (Suzanne Morin); ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2017, 1615 (David Young); ETHI, *Evidence*, 1st Session, 42nd Parliament, 11 May 2017, 1645 (Wally Hill); ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 May 2017, 1605 (Adam Kardash).

297 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 March 2017, 1640 (Colin Bennett).

298 Ibid., 1640 and 1645.

299 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 February 2017, 1620 (Teresa Scassa).

300 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 March 2017, 1705 (Tamir Israel).

3. Children's consent under the *General Data Protection Regulation*

Mr. Charters of the BGCC recommended following the EU's example in its new GDPR, which requires the consent of a parent or guardian to access online services for children under the age of 16 (or a younger age provided that it is not below 13).[301] As Mr. Charters explained,

> It is important … that parents be involved, as only parents or guardians should be able to provide informed and explicit consent for the collection of information. Parents should be aware, and responsible for the activities of their children online, and mechanisms that require explicit parental consent also serve to ensure engagement and awareness of what children are visiting and exploring online.[302]

The Committee supports the views of witnesses who recommended taking immediate action to ensure the adequacy of Canadian legislation vis-à-vis the GDPR, and acknowledges that PIPEDA is only one piece of that legislative framework and that adequacy must be achieved while preserving Canadian specificity. Therefore, the Committee recommends:

Recommendation 17 on the criteria to determine the adequacy status of the *Personal Information Protection and Electronic Documents Act* under the *General Data Protection Regulation*:

That the Government of Canada work with its European Union counterparts to determine what would constitute adequacy status for the *Personal Information Protection and Electronic Documents Act* in the context of the new *General Data Protection Regulation*.

Recommendation 18 on legislative amendments required to maintain the adequacy status:

a) **That the Government of Canada determine what, if any, changes to the *Personal Information Protection and Electronic Documents Act* will be required in order to maintain its adequacy status under the *General Data Protection Regulation*; and**

b) **That, if it is determined that the changes required to maintain adequacy status are not in the Canadian interest, the Government of Canada**

301 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2017, 1540 (Owen Charters).

302 Ibid.

create mechanisms to allow for the seamless transfer of data between Canada and the European Union.

Recommendation 19 on the collaboration with provinces and territories:

That the Government of Canada work with the provinces and territories to make sure that all relevant jurisdictions are aware of what would be required for adequacy status to be granted by the European Union.

THE COMMITTEE'S MISSION TO WASHINGTON, D.C., FROM 2 TO 4 OCTOBER 2017

From 2 to 4 October 2017, four members of the Committee travelled to Washington, D.C. in the context of its study on PIPEDA. The broad objective of this mission was to gain a better understanding of the United States (U.S.) privacy legislation and framework from a comparative approach. The members of the Committee met with different stakeholders to learn more about the issues regarding privacy in the U.S. The main topics discussed were enforcement powers, the safeguarding of personal information, principle-based legislation and the notion of consent and algorithmic transparency.

A. The United States Privacy Legislative Framework and overview of the Federal Trade Commission

1. Framework in the United States

Above all, it is worth noting that the U.S. does not have a comprehensive national privacy framework in place. In fact, the U.S. has not enacted baseline privacy legislation. There is a variety of Federal and State laws and regulations governing privacy in the U.S. Therefore, privacy protections vary at the State level.

For example, the State of California has enacted strong privacy legislation.[303] California's legal framework includes a Constitution that "gives each citizen an 'inalienable right' to pursue and obtain 'privacy'"[304] and has a series of privacy laws governing different sectors. Congressman Tony Cárdenas[305], member of the U.S. House of Representatives' Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce, and researchers from the Congressional Research Service

303 Congressman Cárdenas, District of California-29, Democratic Member, member of the subcommittee on of the Digital commerce and consumer protection.

304 United States (U.S.), State of California Department of Justice, Privacy Laws.

305 U.S., Congressman Tony Cárdenas, *Biography*.

mentioned that California is one of the most rigorous States in terms of privacy protection.

Accordingly, there exists no equivalent to PIPEDA in the U.S. Representatives of the Federal Trade Commission (FTC)[306] and representatives of the Center for Democracy and Technology (CDT)[307] mentioned that it is the "Wild West" at the moment with regards to the regulation of privacy in the U.S. and that better tools to protect privacy and deterrents are needed. Researchers from the Congressional Research Service mentioned that, in the U.S., it appears that privacy is very important with regards to government actions. However, when it involves companies, U.S. citizens are less concerned about privacy.

2. The Federal Trade Commission

The FTC, headquartered in Washington, is a bipartisan[308] federal agency with a dual mission to protect consumers and promote competition.[309] The FTC has a Bureau of Consumer Protection whose mission is to stop unfair, deceptive and fraudulent business practices.[310] One of its divisions is the Division of Privacy and Identity Protection.[311] This division oversees issues related to consumer privacy and information security, among other things.[312]

FTC representatives explained to members of the Committee that the FTC is the main law enforcement actor on the federal level with regards to privacy, although there is no

306 The FTC representatives were:

- Tom Pahl, Acting Director of the Bureau of Consumer Protection
- Kathleen Benway, Chief of Staff to Tom Pahl
- Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection
- Stacy Feuer, Assistant Director, Office of International Affairs
- Guilherme Roschke, Counsel for International Consumer Protection

307 U.S., Center for Democracy and Technology [CDT], *About CDT*; the representatives were Chris Calabrese, Vice President for Policy and Michelle de Mooy, Director of the Privacy and Data Project

308 "The Commission is headed by five Commissioners, nominated by the President and confirmed by the Senate, each serving a seven-year term. No more than three Commissioners can be of the same political party.", see FTC, Commissioners.

309 U.S., Federal Trade Commission [FTC], *What We Do*.

310 FTC, About the Bureau of Consumer Protection.

311 Ibid.

312 Ibid.

comprehensive legal privacy regime in place. For example, the FTC receives complaints regarding data security.

Primarily, the FTC enforces the *Federal Trade Commission Act* (the "FTC Act").[313] In general, the jurisdiction of the FTC with regards to data security and privacy arises from section 5 of the FTC Act which prohibits unfair and deceptive methods, acts or practices in or affecting commerce.[314] Please note that "'Unfair' practices are defined as those that 'cause or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'"[315]

The FTC also enforces specific-sector laws, such as the *Children's Online Privacy Protection Rule* (COPPA), which "imposes certain requirements on operators of websites or online services directed to children under 13 years of age"[316],the *Safeguards Rule*, which "requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure "[317] and the *Fair Credit Reporting Act* which "protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services."[318]

FTC representatives indicated that most of their privacy work is reactive, but that the organization has tried to publish more educational information about what businesses need to do to comply with the law. The FTC has therefore increased its focus on guidance for businesses.

B. Enforcement Powers

During their mission, Committee members discussed with stakeholders the current powers of the Privacy Commissioner of Canada and compared them to the current powers of the FTC.

313 U.S., 15 U.S.C. §§ 41-58, section 5.

314 Ibid.

315 U.S., FTC, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority.

316 U.S., Children's Online Privacy Protection Rule ("COPPA"), 16 CFR Part 312.

317 U.S., Safeguards Rule, 16 CFR Part 314.

318 U.S., FTC, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.

1. The Federal Trade Commission's Enforcement Powers

The FTC referred the Committee members to the brief that it submitted to the OPC in the context of the OPC's consultation on privacy and consent. In its brief, the FTC is in favour of granting more enforcement powers to the Privacy Commissioner of Canada.[319]

FTC representatives explained that the FTC Act provides the FTC with enforcement powers, such as the power to issue orders and seek consumer redress in certain circumstances.

With regards to orders, in its brief to the OPC, the FTC highlighted that it:

> can obtain legally enforceable orders in its administrative and federal court proceedings, either via settlement ("consent orders") or through litigation. The agency's ability to obtain orders is the cornerstone of its robust enforcement program and provides a strong incentive for business compliance. Indeed, the power to issue or seek such orders is consistent with the international best practice set forth in the OECD Privacy Enforcement Guidelines, which calls for member countries to ensure that privacy enforcement authorities have the ability to deter, sanction, and take "corrective action" against companies for practices that violate their domestic laws.
>
> The FTC's authority to issue orders derives from the FTC Act, which authorizes agency enforcement through both administrative and judicial processes. In the administrative process, the agency, after an investigation and administrative settlement or adjudication, may issue an order enjoining specific practices and imposing requirements to ensure the defendant's future compliance. In the judicial process, the FTC may seek preliminary and permanent injunctions in federal court to remedy any provision of law enforced by the Federal Trade Commission.
>
> …
>
> administrative orders and court orders obtained by the FTC may include several key injunctive provisions, depending on the circumstances of the particular enforcement action. These may include: (1) a prohibition on engaging in the challenged conduct, or similar conduct, in the future; (2) in the appropriate case, a requirement to implement a comprehensive privacy or data security program, with specific components set forth in the order; and (3) affirmative monitoring and compliance provisions that last for a specified period of time (*e.g.*, requirements to keep relevant business records; notify employees of the existence of the order; and notify the Commission of any changes that may affect compliance obligations). The affirmative requirements enhance the FTC's ability to monitor ongoing compliance with the order and the FTC Act.[320]

319 OPC, Submission to the OPC's Consultation on Consent under PIPEDA (FTC).

320 Ibid.

FTC representatives also informed Committee members that the FTC has brought enforcement actions addressing a wide range of privacy issues, such as spam, spyware mobile, social networking, etc.[321] The FTC indicated that these privacy issues included more than 130 spam and spyware cases and more than 40 lawsuits regarding privacy in general.[322] FTC representatives also observed that, since 2002, the agency "has brought over 60 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk."[323] They clarified that, where it has found that companies did not protect data appropriately, the FTC usually requires companies to have a comprehensive information security program, in other words a safeguard plan, which is subject to assessments and audits. FTC representatives mentioned that Facebook and Google are under order with the FTC, which means that they are under greater scrutiny. They summarized the cases and indicated that they were made public. The following are the conclusions of investigations and negotiated settlements for Google and Facebook cases:

- **Google**: In 2010, the company launched Google Buzz, a new social network through the Gmail product. In summary, "although Google led Gmail users to believe that they could choose whether or not they wanted to join the network, the options for declining or leaving the social network were ineffective."[324] It led to a complaint with the FTC. In March 2011, the FTC announced that Google had agreed

  > to settle Federal Trade Commission charges that it used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010. The agency alleges the practices violate the FTC Act. The proposed settlement bars the company from future privacy misrepresentations, requires it to implement a comprehensive privacy program, and calls for regular, independent privacy audits for the next 20 years.[325]

- **Facebook**: In 2011, the FTC announced that Facebook agreed "to settle Federal Trade Commission charges that it deceived consumers by telling

321 U.S., FTC, Privacy & Data Security- Update: 2016.

322 Ibid.

323 Ibid.

324 U.S., FTC, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network, Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data, 30 March 2011.

325 Ibid.

> them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[326]
>
> The proposed settlement bars Facebook from making any further deceptive privacy claims, requires that the company get consumers' approval before it changes the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years.[327]

Finally, FTC representatives discussed their power to seek monetary remedies. In its submission, the FTC explains it as follows:

> The FTC routinely seeks monetary remedies in consumer fraud and deceptive advertising cases, both to remedy financial injury to consumers and deprive defendants of wrongful monetary gains. This authority to obtain monetary remedies stems from three legal sources. First, the FTC Act authorizes the FTC to bring federal district court lawsuits seeking preliminary and permanent injunctions for unfair or deceptive trade practices in violation of the FTC Act. These injunctions can include not only "conduct remedies" such as those described above, but also in appropriate cases equitable monetary relief, such as restitution for consumers and disgorgement of profits. Second, the FTC has the ability to seek civil penalties for violations of administrative orders. Third, the FTC has the authority to obtain monetary civil penalties when a statute expressly provides for such penalties, based on statutorily determined maximum penalty amounts.[328]

It is to be noted that FTC representatives underlined that proof of substantial injury is required in order to get remedies under the FTC Act. However, they indicated that it is hard to characterize the injuries consumers suffer in the case of data security incidents and that it is unclear how to measure injuries. FTC representatives pointed out that they would hold a conference regarding this issue in a near future.[329]

2. The Privacy Commissioner of Canada's Powers

i) The Federal Trade Commission's View

FTC representative stressed that the Privacy Commissioner of Canada should have more enforcement powers and referred again the Committee members to its submission to the OPC.

---

326 U.S., FTC, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises."

327 Ibid.

328 Ibid.

329 The FTC held an Informational Injury Workshop on 12 December 2017, see FTC, Informational Injury Workshop.

First, in its submission, the FTC specified that "the OPC would improve privacy protection by engaging in proactive enforcement activity rather than relying primarily on complaints."[330] The FTC explained that, in its experience,

> complaints do not provide a sufficient source of information for authorities to identify and investigate new and emerging privacy issues and prioritize those that raise greatest privacy concerns. This is due, in large part, to the sheer volume of personal data generated and the complex systems that facilitate its collection, which often makes it difficult or impossible for consumers to identify and complain about privacy violations.… it is helpful for enforcers to use multiple sources of information – including news reports, internal and academic research by privacy and security experts, Congressional referrals, company and competitor disclosures, and information from domestic and international enforcement partners – to learn about privacy threats and to set their enforcement priorities.[331]

Second, in its submission, the FTC asserted that if the OPC had the ability to issue orders, it could better protect privacy. The FTC indicated that "orders not only provide a crucial basis for compliance monitoring and future enforcement by the FTC, but they also can provide the broader benefit of communicating the FTC's expectations to companies more generally."[332]

Third, in its submission, the FTC emphasized that if the OPC had the authority to seek monetary remedies, it could better protect privacy. The FTC explained that "the ability to obtain monetary remedies—whether in the form of statutory fines or equitable remedies such as disgorgement and restitution (in those instances when consumers suffer economic losses)—can serve as an important tool to encourage compliance and deter unlawful conduct."[333]

ii) Facebook's View

Facebook representatives[334] emphasized the fact that they constantly consult with the OPC and have asked for guidance on several occasions in the past. They indicated that the PIPEDA regime allows for a collaborative approach and specified that they find this approach to be effective. They added that giving the Privacy Commissioner more powers such as order-making powers would change the relationship between companies and

330 OPC, Submission to the OPC's Consultation on Consent under PIPEDA (FTC).

331 Ibid.

332 Ibid.

333 Ibid.

334 The representatives were, Rob Sherman, Deputy Chief Privacy Officer, Claire Gartland, Manager, Privacy and Public Policy and Kevin Chan, Head of Public Policy, Canada.

the OPC. They also underlined that proactive powers, such as the power to conduct audits and to issue orders, can generate costs for companies. They suggested that the collaborative approach that PIPEDA allows in Canada is a serious consideration and a positive factor that companies take into account when they decide where to invest.

C. Safeguarding Personal Information and the Equifax Data Breach

In the course of their activities, companies, in the data-driven industry, collect consumers' personal information. Safeguards to protect personal information are important as data breaches can cause harm to consumers as observed in the recent Equifax data breach. However, stakeholders mentioned that it is difficult to achieve the right balance between innovation and economic growth, and regulation.

1. Equifax Breach

On 3 October 2017, the U.S. House of Representatives' Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce held a hearing titled "Oversight of the Equifax Data Breach: Answers for Consumers" where former Equifax CEO testified about the data breach.[335] The members of the Committee in Washington attended that meeting.

i) Context

Equifax is a credit analysis and reporting company headquartered in Atlanta, Georgia. "The company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers."[336] Equifax "employs approximately 9,900 employees worldwide."[337] Equifax "operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. It is a member of Standard & Poor's (S&P) 500® Index, and its common stock is traded on the New York Stock Exchange (NYSE) under the symbol EFX."[338]

335 U.S., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, 3 October 2017.

336 Equifax, *Company Profile*.

337 *Ibid.*

338 *Ibid.*

On 7 September 2017, Equifax representatives "announced that criminals exploited a U.S. website application vulnerability to gain access to certain files"[339] and that "[b]ased on the company's investigation, the unauthorized access occurred from mid-May through July 2017."[340] In the United States, the incident potentially impacted 143 million American consumers.[341] According to Equifax, "the incident involves potential access to the personal information of approximately 100,000 Canadian consumers, and that the information that may have been breached includes name, address, social insurance number and, in limited cases, credit card numbers."[342]

On 26 September 2017, Equifax announced that Richard Smith retired from his position of Chairman of the Board and Chief Executive Officer (CEO).[343]

On 2 October 2017, Equifax Canada stated that approximately 8,000 Canadians were impacted by the privacy breach, down from its previous estimate of 100,000.[344] Equifax Canada also revealed that it had learned of the incident on 29 July 2017.[345]

On 28 November 2017, Equifax Canada increased its estimate of the number of Canadians affected by the privacy attack.[346] Equifax revealed that the credit cards of 11,670 Canadians had been hacked; bringing the total number of customers impacted to about 19,000, up from the previous 8,000. Equifax also confirmed that its investigation revealed that the hacked credit card records contain names, addresses, credit or debit card numbers (and expiry dates) and social insurance numbers of the customers impacted. Equifax Canada said that Canadian systems were not affected and are "entirely separated" from the U.S.-based systems.[347]

---

339 Equifax, Press Releases, "Equifax Provides Canadians with Additional Clarity on Cybersecurity Incident Involving Consumer Information," 19 September 2017.

340 Ibid.

341 Equifax, *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*.

342 Equifax, Press Releases, "Equifax Provides Canadians with Additional Clarity on Cybersecurity Incident Involving Consumer Information," 19 September 2017.

343 Equifax, *Equifax Chairman, CEO, Richard Smith Retires; Board of Directors Appoints Current Board Member Mark Feidler Chairman; Paulino do Rego Barros, Jr. Appointed Interim CEO; Company to Initiate CEO Search*.

344 Equifax, *Cybersecurity Incident & Important Consumer Information*.

345 *Ibid.*

346 The Canadian Press, "Equifax says more than 19,000 Canadians affected by security breach," *CBC News*, 28 November 2017.

347 *Ibid.*

The Staff from the House Energy and Commerce Committee gave Committee members a memorandum which explains the privacy safeguards requirements in U.S. law that apply to Equifax.[348]

ii) The Hearing

The hearing held by the U.S. House of Representatives' Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce was meant to help consumers understand what steps were taken by Equifax in order to safeguard personal information going forward and to help individuals who were impacted. Therefore, during the hearing, the discussions focused on a number of issues including how Equifax responded to the breach, how it had patched the vulnerability in its system, and how it had notified the impacted individuals. There were also discussions about how the industry is now unregulated and that privacy safeguards need to be put in place. Moreover, it was raised that consumers need the services of companies like Equifax to participate in the economy: they do not have any other choice.

During his opening statement, Congressman Latta[349], Chair of the U.S. House of Representatives' Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce said the following:

> … I often speak about the fact that we live in a digitally-connected world. That fact of life can have many positive implications, far and wide-ranging, for commerce, trade, communications and entertainment. This Equifax breach is a massive reminder of the bad actors that exist and of the security challenges confronting our digitally-integrated and data-powered economy. In this case, sensitive personal information that is used to build credit histories and allow individuals to engage in commerce—open credit cards, buy cell phones and appliances, and secure mortgages has been compromised. Reasonable security measures must be implemented, practiced, and continually improved by companies that collect and store data in order to guard against unauthorized access to sensitive personal information. Otherwise, consumers can face substantial financial harm.[350]

Furthermore, Congresswoman Schakowsky, ranking member of the U.S. House of Representatives' Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce said the following during the hearing:

---

348 U.S., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, Background Memo, 3 October 2017.

349 U.S., Congressman Bob Latta, *Biography*.

350 U.S., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, Opening Statement of Chairman Bob Latta, 3 October 2017.

> We have these underregulated, private, for-profit credit reporting agencies collecting detailed personal and financial information about American consumers. It is a treasure trove for hackers. Consumers don't have a choice over what information Equifax or, for example, TransUnion, or Experian have collected, stored, and sold. If you want to participate in today's modern economy, if you want to get a credit card, rent an apartment, or even get a job, often then a credit reporting agency may hold the key. Because consumers don't have a choice, we can't trust credit reporting agencies to self-regulate. It is not like when you get sick at a restaurant and decide not to go there anymore. Equifax collects your data whether you want to have it collected or not.[351]

Congresswoman Schakowsky added that she had reintroduced, along with other members of the House Commerce and Energy Committee, a bill that would establish strong data security standards, require breach notification and provide for relief for victims of data breaches.[352]

2. The Safeguarding of Personal Information

During their mission, Committee members discussed with stakeholders the Equifax breach and the safeguarding of personal information. It was a consensus among stakeholders that the Equifax privacy breach could cause important injury to consumers since the stolen personal information was very sensitive and that the impacts of the breach could emerge for a long time. However, there was no consensus on the best ways to safeguard personal information as technology changes and evolves. On the one hand, some stakeholders advocated for the establishment in U.S. law of prescriptive measures to safeguard personal information. On the other hand, some stakeholders highlighted that the establishment of prescriptive measures could hinder or harm the innovation and growth of the industry. Therefore, some stakeholders stressed that the important question is how to strike the right balance between the safeguarding of privacy and economic growth and innovation.

CDT representatives and Howard Beales, Professor of Strategic Management and Public Policy at George Washington University[353] mentioned that there are effective ways to safeguard information. Mr. Beales added that there is no way to be sure that safeguards will always work and protect effectively personal information. In fact, risks change and the industry constantly needs to update the safeguards in place. The CDT indicated that

351 U.S., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, Unedited Transcripts, 3 October 2017.

352 U.S., Committee on Energy and Commerce, *Oversight of the Equifax Data Breach: Answers for Consumers*, Unedited Transcripts, 3 October 2017.

353 U.S., George Washington University, Howard Beales.

an approach to safeguard personal information based on reasonable steps would be efficient.

Some stakeholders indicated that, in order to foster innovation and economic growth, companies should not be regulated too much. For instance, Congressman Latta suggested that "soft touch" regulations are a better way to regulate companies as it provides them with more flexibility. Congressman Harper[354], Vice-Chairman of the U.S. House of Representatives' Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce, thinks there should be more safeguards required to protect personal information. He indicated that self-driving cars, for instance, is a big issue and that legislation has been adopted by the U.S. House of Representatives. He also indicated that "stress tests" where systems are tested and where fishing attempts are sent to employees, is a good way to ensure the safeguarding of privacy. Congressman Cárdenas thinks that there should be more prescriptive standards to protect consumers' personal information. However, he indicated that big companies are not in favour of such prescriptive measures. Congressman Johnson[355], member of the U.S. House of Representatives' Subcommittee on Communications and Technology of the Committee on Energy and Commerce, indicated that there is a very delicate balance between privacy and the industry. In his view, the technology industry has not been much regulated in the past and it is why it has evolved and grown so much and so rapidly.

Staff from the House Energy and Commerce Committee believed that "soft touch" regulations allow a certain oversight, but maintains the flexibility of the industry. However, they agreed that the way to achieve the balance between the safeguarding of personal information and the innovation and growth of the industry is a hard question. They also mentioned that the Department of Homeland Security tests programs to make sure companies have appropriate safeguards in place.

Some stakeholders underscored that privacy and the impact it can have on companies' reputation may encourage companies to put in place strong privacy safeguards. In fact, privacy breaches can have far-reaching consequences for companies, as they are at risk of losing consumers' trust. For instance, the FTC mentioned that reputation is an important factor for companies when they consider privacy safeguards. Congressman Johnson also indicated that companies that are the subject of a breach sometimes cannot overcome the negative reputation impact. Facebook representatives remarked that 23 million Canadians are on Facebook and that consumer trust is essential to them.

354 U.S., Congressman Gregg Harper, *Biography*.

355 U.S., Congressman Bill Johnson, *Biography*.

They indicated that they ensure that people are informed and empowered with regards to privacy. Their vision is to make sure that people have all the information they need to ensure that the "trace" they leave on the Internet suits them.

Finally, FTC representatives mentioned the importance of breach notification legislation. Almost all of the states have enacted data breach notification legislation that requires private and governmental entities to notify individuals when security breaches involving personal information occur. The staff of the U.S. House of Representatives' Energy and Commerce Committee confirmed that 48 States, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted privacy breach notification requirements.

D. Principle-based Legislation and the Notion of Consent

During their mission, Committee members discussed with stakeholders principle-based legislation and the notion of consent.

Facebook representatives specified that PIPEDA, as it is principle-based, is very efficient as it can adapt to new technologies. They indicated that Facebook submitted a brief in the context of the OPC's consultation on privacy and consent, which states the following:

> Facebook agrees with the OPC that new technologies, services, uses of data and business models have presented, and will likely continue to present, challenges to older, more traditional ways of thinking about consent. We are confident not only that the existing PIPEDA framework can meet these challenges, but that the OPC can use them as an occasion to highlight the strength and flexibility of Canada's privacy regime relative to those in use in other parts of the world.
>
> Many of the issues and concerns may be managed through the use of enhanced consent approaches, which focus on innovative and user-friendly ways to present an organization's information management practices, and provide users with clear information regarding their choices with respect to the collection and use of their data, as well as the ways in which those choices might be expressed. Privacy governance approaches to product development can also go a long way to strengthening accountability and enhancing consumer trust.
>
> We believe that a model for privacy protection that is flexible and recognizes a range of approaches to consent that are appropriate to the context in which data is used, continues to be the best approach for enabling people to make choices about their information, and an appropriate basis for a legislative framework. This is the approach currently embodied in PIPEDA, a law that continues to build trust and drive growth in the digital economy.[356]

356 OPC, Consent and Privacy: Facebook Comments on the OPC Discussion Paper, October 2016.

Mr. Beales said he is not in favour of a privacy regime based on fair information principles.[357] According to him, it is too burdensome for consumers as principles usually focus on consumer's choice. Moreover, Mr. Beales indicated that we are seeing incidental uses of data that are of great value, but that nobody thought of at the time. Mr. Beales argued that the right solution would be to focus on the risks and the costs. Therefore, Mr. Beales appeared to be in favour of a risk-based approach.

CDT representatives indicated that they have a positive view of the fair information principle approach. They pointed out that the society is entering a strange period with the development of big data and the Internet of Things[358], for example. Therefore, CDT representatives proposed that it would be a good opportunity to update the principles. Also, the CDT underlined that it is important to take into account the consumer perspective. The emerging new technology makes it difficult for consumers to understand how companies use their personal information and to distinguish a bad use from a good use. Also, CDT representatives indicated that, in the world of big data, individual control over personal information is not possible. Data ownership does not appear to be something that companies are willing to discuss and consider. However, data portability, as provided for in the GDPR, is a possibility and the industry is more open towards that.

FTC representatives indicated that prohibited use of personal information, in other words, no-go zones, would be a very good protection for consumers. The FTC also raised the question as whether there should be a no "opt-out" option for certain protections of personal information.

Facebook representatives specified that Privacy by Design is used by Facebook. They highlighted that privacy is considered on many levels and at many steps of the development of features. They highlighted that the concept of Privacy by Design needs to be flexible as it means different things to big companies and small companies.

Finally**,** researchers from the Congressional Research Service specified that the right to erasure is an interesting option, but that it may not be efficient when data has already been generated from the data that it supposed to be erased. Facebook representatives indicated that they allow people on their platform to delete things they have posted.

---

357 For example, the Fair Information Practice Principles are principles that were set forth by the FTC for the use, collection and safeguarding of personal information. PIPEDA is also based on principles set out in the Model Code for the Protection of Personal Information.

358 The Internet of Things "is the networking of physical objects connecting through the Internet." See Privacy Commissioner of Canada, The Internet of Things.

E. Algorithmic transparency

During their mission, Committee members had discussions regarding algorithmic transparency. As algorithms are used more and more, notably in order to make decisions, many stakeholders drew the attention of the Committee members to the possible consequences of algorithms. Stakeholders underlined that algorithms may have undesirable effects, such as the targeting of certain groups based on race, ethnic origin or socio-economic considerations. Therefore, their use raises ethical issues and questions.

The CDT argued that it is very important for companies to incorporate ethics and privacy in the process of developing an algorithm from the design to the testing stages. In fact, companies should create a culture that includes privacy, security and ethics and that would appear through their decision. Not only would that increase the faith of employees in the company, it would help mitigate the risk of the use of algorithms. The CDT commented that there is not much training available at the moment for people that elaborate algorithm, but that it is improving.

Facebook representatives indicated that they have put in place ethical standards for their use of algorithms.

With regards to the amount of personal information that is being collected in the Big Data era, CDT representatives underlined that it might be useful in certain circumstances to have lots of data, but that the assumption that more data is better is not a true statement. Furthermore, CDT representatives indicated that the accuracy of the information that is collected and used as well as error rates and redress for individuals are important issues to consider. Nevertheless, Mr. Beales suggested that more data, in the big data context, is better as it allows information to be confirmed. He added that mistakes also arise if decisions are based on humans. Mr. Beales argued that algorithms have to be considered from the costs and consequences perspective.

CDT representatives emphasized the fact that the information processed by an algorithm and the algorithm itself have to be accurate and reliable with the following example: If an algorithm has a 99% rate efficiency to identify terrorists, it means that, because of the 1% error rate, millions of Americans would be identified as terrorists. Mr. Beales indicated that, if the algorithm is wrong a few times, but always finds the terrorists, it may be worth if the people that are wrongly identified are not too much impacted.

GLOSSARY

algorithmic transparency. when users have complete information about the workings of the artificial intelligence programs behind the websites they visit, the data they collect and how they are used

CASL. *Canada's Anti-spam Law*

CJEU. Court of Justice of the European Union

CRTC. Canadian Radio-television and Telecommunications Commission

depersonalized data. data that has been aggregated and presented in such a way that it is impossible to identify the owner (also known as "anonymous" or "de-identified" data)

EU. European Union

GDPR. the European Union *General Data Protection Regulation*, which will come into force in May 2018

Model Code. *Model Code for the Protection of Personal Information* developed by the Standards Council of Canada, reproduced in Schedule 1 of the *Personal Information Protection and Electronic Documents Act* and to the principles of which organizations are required to adhere

OPC. Office of the Privacy Commissioner of Canada

PIPEDA. *Personal Information Protection and Electronic Documents Act*, which applies to the private sector

***Privacy Act*.** which applies to the public sector

right to be forgotten. usually refers to one of the following two concepts:

- "right to erasure"—the right to have information removed from a website
- "right to de-indexing" (or "right to dereferencing " or "right to delisting")—the right to have a website containing personal information removed from the results of search engines such as Google

APPENDIX A
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
As individuals	2017/02/14	46
Robert Gary Dickson, Consultant, Former Saskatchewan Information and Privacy Commissioner		
Éloïse Gratton, Partner and National Co-Leader, Privacy and Data Protection Practice Group, Borden Ladner Gervais		
Dentons Canada		
Chantal Bernier, Counsel,Global Privacy and Cybersecurity Group		
Public Interest Advocacy Centre		
Alysia Lau, Legal Counsel		
John Lawford, Executive Director and General Counsel		
As an individual	2017/02/16	47
Valerie Steeves, Full Professor, Department of Criminology, University of Ottawa		
BC Freedom of Information and Privacy Association		
Vincent Gogolek, Executive Director		
Office of the Privacy Commissioner of Canada		
Brent Homan, Director General, Personal Information Protection and Electronic Documents Act Investigations		
Patricia Kosseim, Senior General Counsel and Director General Legal Services, Policy, Research and Technology Analysis Branch		
Daniel Therrien, Privacy Commissioner of Canada		
Commission d'accès à l'information du Québec	2017/02/21	48
Cynthia Chassigneux, Administrative Judge, Surveillance		
Office of the Information and Privacy Commissioner for British Columbia		
Drew McArthur, Acting Commissioner		
Michael McEvoy, Deputy Commissioner		

Organizations and Individuals	Date	Meeting
Office of the Information and Privacy Commissioner of Alberta Sharon Ashmore, General Counsel Jill Clayton, Commissioner Kim Kreutzer Work, Director, Knowledge Management	2017/02/21	48
As individuals Florian Martin-Bariteau, Assistant Professor, Common Law Section, Faculty of Law, and Director, Centre for Law, Technology and Society, University of Ottawa Teresa Scassa, Full Professor, Canada Research Chair in Information Law, University of Ottawa **Centre for Law and Democracy** Michael Karanicolas, Senior Legal Officer	2017/02/23	49
As individuals Colin J. Bennett, Political Science Professor, University of Victoria David Fraser, Partner, McInnes Cooper Michael Geist, Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa **British Columbia Civil Liberties Association** Micheal Vonn, Policy Director	2017/03/21	52
As an individual Jennifer Stoddart **Canadian Bar Association** Suzanne Morin, Vice-President, Privacy and Access Law Section **Canadian Internet Policy and Public Interest Clinic** Tamir Israel, Staff Lawyer	2017/03/23	53
As individuals Vincent Gautrais, Full Professor, Director of the Centre de recherche en droit public, Faculty of Law, University of Montreal Ian Kerr, Professor and holder of the Canada Research Chair in Ethics, Law and Technology, University of Ottawa	2017/04/04	54

Organizations and Individuals	Date	Meeting
As individuals Robert G. Parker, Advisory Consultant, Risk Masters International Inc. David Young, Principal, David Young Law	2017/04/04	54
As individuals Paige Backman, Partner, Aird and Berlis LLP Alex Cameron, Partner and Chair, Privacy and Information Protection Group, Fasken Martineau DuMoulin LLP Molly Reynolds, Senior Associate, Torys LLP	2017/04/06	55
Canadian Radio-television and Telecommunications Commission Steven Harroun, Chief Compliance and Enforcement Officer Daniel Roussy, General Counsel and Deputy Executive Director **Competition Bureau** Morgan Currie, Associate Deputy Commissioner, Deceptive Marketing Practices Directorate Josephine Palumbo, Deputy Commissioner, Deceptive Marketing Practices Directorate **Department of Industry** Krista Campbell, Director General, Digital Policy Branch, Spectrum, Information Technologies and Telecommunicatons Sector Steve Joanisse, Legal Counsel Innovation, Science and Economic Development Legal Services Charles Taillefer, Director, Digital Policy Branch, Spectrum, Information Technologies and Telecommunicatons Sector	2017/05/09	59
Canadian Bankers Association Charles Docherty, Senior Legal Counsel Linda Routledge, Director, Consumer Affairs **Canadian Marketing Association** David Elder, Special Digital Privacy Counsel Wally Hill, Vice-President, Government and Consumer Affairs	2017/05/11	60

Organizations and Individuals	Date	Meeting
Canadian Wireless Telecommunications Association Robert W.J. Ghiz, President and Chief Executive Officer	2017/05/11	60
Canadian Chamber of Commerce Scott Smith, Director, Intellectual Property and Innovation Policy	2017/05/16	61
Consumers Council of Canada Dennis Hogarth, Vice-President		
Information Technology Association of Canada André Leduc, Vice-President, Government Relations and Policy Robert Watson, President and Chief Executive Officer		
Canadian Life and Health Insurance Association Anny Duval, Counsel Frank Zinatelli, Vice-President and General Counsel	2017/05/30	62
Insurance Bureau of Canada Randy Bundus, Senior Vice-President, Legal and General Counsel Steven Lingard, Director, and Chief Privacy Officer, Legal Services		
Interactive Advertising Bureau of Canada Sonia Carreno, President Adam Kardash, Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP		
Association of Canadian Archivists Greg Kozak, Representative, Ethics Committee	2017/06/01	63
Canadian Association of Research Libraries Donna Bourne-Tyson, President Susan Haigh, Executive Director		
Google Canada Colin McKay, Head, Public Policy and Government Relations		
Retail Council of Canada Jason McLinton, Vice-President, Grocery Division and Regulatory Affairs		

Organizations and Individuals	Date	Meeting
European Data Protection Supervisor Giovanni Buttarelli, Supervisor	2017/06/13	64
As an individual Jane Bailey, Professor, Faculty of Law, University of Ottawa	2017/09/25	68
Boys and Girls Clubs of Canada Owen Charters, President and Chief Executive Officer Rachel Gouin, Director, Research and Public Policy		
National Association for Information Destruction - Canada Kristjan Backman, Chair		
Office of the Privacy Commissioner of Canada Vance Lockton, Strategic Policy and Research Analyst Regan Morris, Legal Counsel Daniel Therrien, Privacy Commissioner of Canada	2018/02/01	88

APPENDIX B
LIST OF BRIEFS

Organizations and Individuals

Backman, Paige

Baer, Aaron

Martin-Bariteau, Florian

Young, David

Association of Canadian Archivists

Boys and Girls Clubs of Canada

Canadian Association of Research Libraries

Canadian Bar Association

Canadian Marketing Association

National Association for Information Destruction - Canada

Office of the Privacy Commissioner of Canada

Option consommateurs

Public Interest Advocacy Centre

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 46, 47, 48, 49, 52, 53, 54, 55, 59, 60, 61, 62, 63, 64, 68, 70, 79, 87, 88, 90 and 91) is tabled.

Respectfully submitted,

Bob Zimmer
Chair