HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

PRIVACY AND SOCIAL MEDIA IN THE AGE OF BIG DATA

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

Pierre-Luc Dusseault, M.P.
Chair

APRIL 2013

41st PARLIAMENT, FIRST SESSION

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

SPEAKER'S PERMISSION

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 Parliament of Canada Web Site
at the following address: http://www.parl.gc.ca

PRIVACY AND SOCIAL MEDIA IN THE AGE OF BIG DATA

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

Pierre-Luc Dusseault, M.P.
Chair

APRIL 2013

41st PARLIAMENT, FIRST SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Pierre-Luc Dusseault

VICE-CHAIRS

Scott Andrews

Patricia Davidson

MEMBERS

Charlie Angus	Brad Butt	Dean Del Mastro
Charmaine Borg	Blaine Calkins	Earl Dreeshen
Alexandre Boulerice	John Carmichael	Colin Mayes

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Mike Allen	Jinny Jogindera Sims	Joe Preston
Dean Allison	Daryl Kramp	James Rajotte
Kelly Block	Jean-François Larose	Hon. Geoff Regan
Marjolaine Boutin-Sweet	Laurin Liu	Kennedy Stewart
Rod Bruinooge	Hon. Lawrence Mac Aulay	Merv Tweed
Sean Casey	Joyce Murray	Chris Warkentin
Hon. Denis Coderre	Tilly O'Neill Gordon	
Richard M. Harris	François Pilon	

CLERK OF THE COMMITTEE

Chad Mariage

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Miguel Bernal-Castillero

Dara Lithwick

Maxime-Olivier Thibodeau

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

FIFTH REPORT

Pursuant to its mandate under Standing Order 108(3)(h), the Committee has studied privacy and social media and has agreed to report the following:

TABLE OF CONTENTS

PRIVACY AND SOCIAL MEDIA IN THE AGE OF BIG DATA

THE COMMITTEE'S STUDY

On May 8, 2012, the House of Commons Standing Committee on Access to Information, Privacy and Ethics ("the Committee") agreed to undertake a study on the efforts and the measures taken by social media companies to protect the personal information of Canadians, and to report the Committee's findings back to the House of Commons.[1]

On May 29, 2012, the Committee held its first hearing on this matter. Jennifer Stoddart, the Privacy Commissioner of Canada, appeared before the Committee and gave a brief overview of the social media industry, what it does and how its activities have an impact on the privacy of Canadians. In the Commissioner's words:

> Social media involve applications that allow individuals, organizations, and communities to share information and to generate content.[2]

Commissioner Stoddart went on to highlight the four areas of privacy protection which most concerned her Office — accountability, meaningful consent, limiting use, and retention — giving the Committee a first framework for studying this vast issue.

Between May 29 and December 11, 2012, the Committee dedicated 15 meetings to the study, heard over 30 witnesses representing government, academia, public interest groups and the private sector, and received several written submissions. The Committee also travelled to Washington, D.C. in early October to meet with U.S. privacy experts and officials.

THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)[3] is the primary piece of legislation for protecting individuals' privacy in their dealings with social media companies and other organizations in the private sector. PIPEDA establishes ground rules for the management of personal information in the private sector and aims to strike a balance between the right to privacy and the need of organizations to collect, use and disclose personal information for legitimate business purposes. PIPEDA applies to organizations engaged in commercial activities across Canada, except those governed by

---

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Minutes of Proceedings*, 1st Session, 41st Parliament, May 8, 2012.

2 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1145 (Jennifer Stoddart, Privacy Commissioner).

3 *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c. 5.

provinces with legislation that is substantially similar to the federal legislation.[4] PIPEDA also protects the information of employees working in sectors governed by federal regulations.

Since January 1, 2004, PIPEDA has applied to the collection, use and disclosure of personal information during the course of any commercial activity in Canada. It also applies to personal information collected in all inter-provincial and international commercial transactions.[5] Businesses engaged in social media activities are therefore subject to PIPEDA.

As constituted, PIPEDA is technology-neutral and is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information*.[6] The Code, which is incorporated into the legislation, came out of a collaborative effort by representatives of government, consumers and business groups, and lists 10 principles of fair information practices, including the requirement for an individual's knowledge and consent, subject to limited exceptions, when collecting, using or disclosing the individual's personal information. Further, the purposes for which an organization can collect, use or disclose personal information are to be limited to those that "a reasonable person would consider are appropriate in the circumstances."[7] Personal information can only be used for the purpose for which it was collected and, where an organization is going to use it for another purpose, consent must be obtained again. Lastly, PIPEDA upholds the obligation for openness and accessibility of an organization's policies and practices for the management of personal information, as well as the right of individuals to access any personal information an organization may have about them and to have this information corrected or amended if its accuracy and completeness are found to be deficient.[8]

CONCERNS SPECIFIC TO PRIVACY AND SOCIAL MEDIA

The Committee heard evidence regarding how social media has spurred a change in how individuals and organizations view and protect personal information. Personal information, defined in PIPEDA as "information about an identifiable individual",[9] has become valuable and quantifiable data — easy to collect, process and use for new,

---

4 To date, Alberta, British Columbia and Quebec have substantially similar privacy legislation. New Brunswick, Newfoundland and Labrador, and Ontario also have substantially similar laws with respect to health information custodians. Even in these provinces, PIPEDA continues to apply to the federally regulated private sector and to personal information in inter-provincial and international transactions.

5 Office of the Privacy Commissioner of Canada (OPC), "The *Personal Information Protection and Electronic Documents Act*", *Fact Sheets*.

6 National Standard of Canada, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96.

7 PIPEDA, s. 4.

8 For more details on the principles, see OPC, "Complying with the *Personal Information Protection and Electronic Documents Act*," *Fact Sheets*, and Nancy Holmes, *Canada's Federal Privacy Laws*, Publication No. PRB 07-44E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, September 25, 2008.

9 PIPEDA, s. 2.

different and ever-evolving purposes. This evolution has called into question how social media treats personal information and what measure they take to comply with Canadian privacy laws.

A. The Changing Practices of Individuals and Social Media Companies

> *This is the age of big data where personal information is the currency that Canadians and others around the world freely give away.*[10]
>
> *- Jennifer Stoddart, Privacy Commissioner of Canada*

A first component of the issue of privacy and social media is that individuals give their personal information willingly on social media sites, but may not fully understand the way their information is used, or the associated privacy risks.[11] Professor Normand Landry of TELUQ identified six risks and pitfalls associated with the disclosure of personal information on social media sites, some of which particularly impact minors: the loss or absence of anonymity on social media sites and the disclosure of information deemed to be private or confidential; identity theft; employment-related dangers and risks; multiple attacks on honour and reputation; cyber-bullying; and psychological and sexual violence.[12]

It was put to the Committee that the lack of understanding among users is the result of several factors beyond the control or technological sophistication of the individual users, such as the business design and interests of social media companies,[13] a dated notion of what constitutes personal information in Canadian law,[14] and the absence of a clear framework to provide social media users with a set of standards on the protection of personal information.[15]

For example, social media companies compile user-generated data and use or share this information in ways that may not be clear to users. As Commissioner Stoddart pointed out:

> Social media companies can quickly amass a staggering amount of personal information. In addition to the preferences, habits, and social interactions of their users, these companies also collect vast amounts of background information that is not visible on public profiles, including search histories, purchases, Internet sites visited, and the content of private messages. This collection of billions of data points allows social media companies—using sophisticated algorithms—to analyze user behaviour in order to refine their services, and to identify ways to generate revenue. It can also enable others, such

---

10 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1145 (Jennifer Stoddart, Privacy Commissioner).

11 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1225 (Janet Goulding, Industry Canada).

12 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1550 (Normand Landry, TELUQ).

13 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1120 (Valerie Steeves, University of Ottawa).

14 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1640 (Colin Bennett, University of Victoria).

15 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1540 (Normand Landry, TELUQ).

> as researchers, employers, school administrators, and law enforcement, to learn more about individuals and their activities.[16]

Professor Teresa Scassa of the University of Ottawa added that social media companies play a central role in "harvesting or in facilitating the harvesting of massive amounts of information" about individuals by tracking users' online activity, consumption habits, and even patterns of movement.[17] Professor Normand Landry warned that "the risk is that, with the new techniques for cross-referencing data, you can track an individual's entire private life by multiplying the inquiries done on social media sites the user visits. The danger is there, and the problem is growing."[18]

Mr. Colin McKay, Policy Manager at Google Canada told the Committee that when information is used by social media companies, it is not necessarily information that pertains to the individual, but is de-identified — meaning that the information is made anonymous and reconfigured in a way that it can no longer be linked to an individual. This de-identified information is useful to companies like Google for developing new products and new tools.[19]

Several witnesses drew the Committee's attention to the fact that these changes in the way social media companies use information are what drive the modern digital world. Social media networks contribute to making the social, political, cultural and economic lives of Canadian more comprehensively intertwined — this sharing of information facilitates both the democratic exchange of ideas and new economic opportunities for Canadians and Canadian companies.[20] Mr. Warren Everson, Senior Vice-President, Policy, of the Canadian Chamber of Commerce commented that:

> Social media is experiencing a very dramatic growth. It's attracting millions of dollars of investment in Canada's digital economy and is creating thousands of jobs in Canada. These can be very high-quality and well-paying jobs.[21]

---

16 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1145 (Jennifer Stoddart, Privacy Commissioner).

17 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1100 (Teresa Scassa, University of Ottawa).

18 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1550 (Normand Landry, TELUQ).

19 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1625 (Colin McKay, Google Canada). For more information on Google, please see the section entitled Evidence Specific to Certain Private Companies below.

20 ETHI, *Brief submitted by B.C.Freedom of Information and Privacy Association* (FIPA), "Social Media, Big Data and Privacy: Protecting Citizen Rights in the Age of Connection," 1st Session, 41st Parliament, December 13, 2012, p. 8.

21 ETHI, *Evidence*, 1st Session, 41st Parliament, June 5, 2012, 1100 (Warren Everson, Canadian Chamber of Commerce).

B. Balancing Innovation and Regulation

> *Canadians should not be forced to choose between their privacy rights and their right to participate in this new interactive world.*[22]
>
> *- Tamir Israel, Canadian Internet Policy and Public Interest Clinic*

The Committee heard many witnesses speak about the need to strike a balance between social media companies' desire to innovate and experiment with new products and services, and the appropriate level of protection for Canadians' personal information.

Certainly, witnesses from academia and the private sector suggested the need for policies that encourage the development of Canadian e-commerce and social media, both to give this rising sector "an unmistakable Canadian stamp"[23] and to "ensure that Canada is a destination nation for business to grow and prosper."[24] However, some witnesses, mostly affiliated with regulatory agencies, academia, and public interest groups, argued that there is "unquestionably a role for government and regulators to set certain parameters about what is appropriate and to ensure that it reflects Canadian values about what's right from a privacy perspective."[25] By contrast, other witnesses, mainly representing industry associations and private companies, recognized the need to protect personal information, but preferred a self-regulated approach. Mr. David Elder of the Canadian Marketing Association (CMA) stated that "regardless of any legal requirements or sanctions, legitimate businesses have every incentive to anticipate consumer privacy needs and resolve any concerns."[26]

This preference for self-regulation, as opposed to legislated obligations, was repeated to the Committee by several witnesses, precisely because they believe it would be more adaptable to rapidly changing conditions. Professor Vincent Gautrais of the Université de Montréal suggested:

> That is why this notion of accountability should not be introduced through a piece of legislation, but rather through informal practice standards, through codes of conduct. With a more negotiated approach, there would be no law imposing things within a generally quite short time frame, and the situation would be conducive to dialogue for establishing practice standards.[27]

---

22 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1110 (Tamir Israel, Canadian Internet Policy and Public Interest Clinic – CIPPIC).

23 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1110 (Michael Geist, University of Ottawa).

24 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1535 (Karna Gupta, Information and Technology Association of Canada – ITAC).

25 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1150 (Michael Geist, University of Ottawa).

26 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1545 (David Elder, CMA).

27 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1230 (Vincent Gautrais, Université de Montréal).

As an example of one such self-regulating sector, the Committee heard evidence from the CMA which has published guidelines for its members on providing clear, easy to understand explanatory information to consumers.

> ... the [CMA] guidelines require that marketers using online, interest-based advertising should ensure that they, and the ad networks and website publishers that display interest-based ads on their behalf, provide clear explanatory information about how browsing information is collected and used, and provide an effective means to draw consumers' attention to that information.[28]

The Privacy Commissioner, for her part, expressed her concern that social media companies have an apparent disregard for Canadian privacy laws, a problem that is aggravated as they grow in size and become less inclined to be fully transparent with regulatory authorities.[29]

> In my view, with the emergence of Internet giants, the balance intended by the spirit and letter of PIPEDA is at risk. The quasi-monopoly of these multinationals has made PIPEDA's soft approach, based on non-binding recommendations and the threat of reputation loss, largely ineffective, I believe. We have seen organizations ignore our recommendations until the matter goes to court. We have seen large corporations, in the name of consultation with my office, pay lip service to our concerns and then ignore our advice. Moreover, with vast amounts of personal information held by organizations on increasingly complex platforms, the risk of significant breaches and of unexpected, unwanted, or even intrusive uses of that information calls for commensurate safeguards and financial consequences not currently provided for in PIPEDA.[30]

According to the witnesses, social media companies have, so far, not created industry standards for self-regulation. Nevertheless, the Committee appreciates that social media is a new, rapidly evolving industry, one that both experiments with the boundaries of privacy and needs privacy to ensure consumers' trust. As Mr. Alan Chapell, Outside Counsel and Privacy Officer for BlueKai Inc., a data management company, put it:

> … social media are participating in a developing culture regarding privacy. (…)
>
> Both from a legislative and a regulatory perspective, it's a delicate balance to define the balance between stifling innovation and protecting consumer privacy interests.[31]

The Committee was also apprised of the fact that, while Canadians are very active users of social media, they represent only a fraction of the business interest of major social media companies. Consequently, many of these companies' privacy policies are drafted

---

28 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1545 (David Elder, CMA).

29 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1145 and 1155 (Jennifer Stoddart, Privacy Commissioner). This view was also shared by Elizabeth Denham, Information and Privacy Commissioner of British Columbia: ETHI, *Evidence*, 1st Session, 41st Parliament, June 7, 2012, 1135.

30 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1615 (Jennifer Stoddart, Privacy Commissioner).

31 Ibid., 1655 (Alan Chapell, BlueKai). For more information on BlueKai, please see the section entitled Evidence Specific to Certain Private Companies below.

under legislative models different to PIPEDA, where the emphasis is not on personal information, but on personally identifiable information.[32] Mr. John Lawford of the Public Interest Advocacy Centre (PIAC) pointed out that:

> … major social networks define "personal information" in confusing ways, and none of them define it in the way it is defined in PIPEDA. (…)
>
> This non-definition of personal information matters because users reading the privacy policy are not able to understand their real rights under PIPEDA in order to launch a complaint or to bring the company into compliance or even to contact the company.[33]

PIAC submitted a table, included as Appendix A to this Report, which compares the definition of "personal information" in PIPEDA with the definitions found in a number of social media's privacy policies and terms of service.[34] The table serves to highlight the fundamental variations that exist between what Canadian law states and what social media companies practice. In his testimony, Mr. Lawford suggested that it be a requirement for organizations to, in their user agreements, define "personal information" in a way that is compatible and in accordance with the definition in PIPEDA.[35]

In his written submission to the Committee regarding this study, Mr. Christopher Parsons, a PhD candidate at the University of Victoria and co-investigator on a project examining how social networking companies comply with aspects of Canadian privacy laws, drew the Committee's attention to the fact that American laws are "*the* preeminent laws" that social networks agree to abide by, and that there is a reluctance by some of the large social networking companies to implement Canadian (or European) data protection laws because such laws "could hinder or forbid practices that the companies currently employ to benefit commercially."[36]

As a result of this testimony, the Committee is concerned that major social media companies, while doing business in Canada, prefer to be governed by laws other than those of this country. While the reasons for this may be economic, linguistic or business in nature, it is important that Canadians who use these services be protected by their own laws and values. This is particularly so with regard to the way in which "personal information" has come to be defined, in law and in practice, in Canada.

---

32 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1620 (John Lawford, PIAC).

33 Ibid., 1535.

34 ETHI, *Document submitted by the Public Interest Advocacy Centre (PIAC)*, "Comparing Definitions in Social Media Privacy Policies and Terms of Service", October 18, 2012.

35 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1550 (John Lawford, PIAC).

36 ETHI, *Brief submitted by Christopher Parsons*, "Social Networking and Canadian Privacy Law: Jurisdiction, Retention, and Disclosure," 1st Session, 41st Parliament, December 23, 2012, p. 3.

C. Shifts in Why and How Personal Information is Collected, Used and Disclosed

> *Legislation dealing with the protection of personal information is still based on personal information. I really feel that we are losing the meaning of that concept, of what personal information is. We recognize that it means a name, an address and other information that you might give to someone. But more and more, personal information is information about all our activities, about everything we do online, and even elsewhere.*[37]
>
> *- Professor Teresa Scassa, University of Ottawa*

Witnesses appearing before the Committee suggested that over the past few years, as social media networks have emerged, there has been a shift in how personal information is collected, used and disclosed. Where before personal information was gathered for transactional purposes, personal information is now itself the valued commodity. In Professor Scassa's view, the shift of personal information into valuable and transactionable data:

> … risks gutting the consent model on which the legislation is based. This new paradigm deserves special attention and may require different legal norms and approaches. (…)
>
> The data is used to profile us so as to define our consumption habits, to determine our suitability for insurance or other services, or to apply price discrimination in the delivery of wares or services. We become data subjects in the fullest sense of the word. There are few transactions or activities that do not leave a data trail.[38]

In addition to the shift to personal information as data, new technologies facilitate the manipulation of information and its use in different contexts and formats than those in which it was given. The result is easier collection, use and disclosure of personal information by companies, and a related loss of control over that information for individuals who must now be more cautious about how they share their information. Adam Kardash, Managing Director and Head of Access Privacy at law firm Heenan Blaikie emphasized that "as individuals we all have a responsibility to be careful with how we use our personal information in public contexts."[39]

Within this context, witnesses highlighted the fact that the use of personal information as data facilitates the aggregation of that data and creates opportunities to monetize a user's personal information. As Tamir Israel of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) put it, "all this data is collected, analyzed and refined into a sophisticated socio-economic categorization scheme."[40] The result, according to Professor Ian Kerr of the University of Ottawa, is that:

---

37 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1210 (Teresa Scassa, University of Ottawa).

38 Ibid., 1105.

39 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1130 (Adam Kardash, Heenan Blaikie).

40 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1110 (Tamir Israel, CIPPIC).

> … social media companies and other information brokers will partner with whoever they want to in order to make lucrative arrangements, the purpose of which is to do things to connect those bits of information in order to create certain kinds of profiles about us so that they can put us into categories for certain purposes that benefit us, etc.[41]

According to certain witnesses, this means that social media services are not free, but rather a means to commercialize access to users and their personal information. As noted by Mr. Jason Zushman of the Merchant Law Group, "the archiving and monitoring of information that's provided by users is what provides the monetary benefits to the companies."[42]

Mr. Colin McKay also acknowledged that there is "extreme value" to Google in the "vast quantity of information that's not specifically user data" because of the different uses available for this data, including using it to inform safer and more secure practices online.[43] For his part, Mr. Alan Chapell of BlueKai explained that the use of personal information for targeted advertising "actually funds a good deal of the [online] content that consumers enjoy for free."[44] Mr. Robert Sherman, Manager, Privacy and Public Policy at Facebook echoed that sentiment, noting how that social media company's business model is to "offer [Facebook] for free to users who want to use it. In exchange, we pay for it by showing advertising on Facebook."[45]

In defence of this practice, Mr. Brendan Wycks of the Marketing Research and Intelligence Association (MRIA), a not-for-profit association representing the market intelligence and survey research industry, explained that "legitimate survey researchers take great pains to respect the rules of the social media sites [they] monitor, respect the wishes of those who post personal information online, anonymize the personal information in the data [they] collect, and never attempt to sell anything or solicit in any form."[46]

However, several witnesses, including Professors Ian Kerr and Teresa Scassa, warned of profiling as a by-product of data aggregation; that is, the placing of users, accurately or inaccurately, into "social categories…on the basis of information-processing."[47] As noted by Professor Scassa:

> We are told that profiling is good because it means that we don't have to be inundated with marketing material for products or services that are of little interest. Yet there is also a flip side to profiling. It can be used to characterize individuals as unworthy of special

---

41 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1235 (Ian Kerr, University of Ottawa).

42 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1645 (Jason Zushman, Merchant Law Group).

43 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1555 (Colin McKay, Google Canada).

44 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1550 (Alan Chapell, BlueKai).

45 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1550 (Robert Sherman, Facebook). For more information on Facebook, please see the Section on Testimony Concerning Certain Private Companies below.

46 ETHI, *Evidence*, 1st Session, 41st Parliament, June 5, 2012, 1115 (Brendan Wycks, MRIA).

47 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1235 (Ian Kerr, University of Ottawa).

> discounts or promotional prices, unsuitable for credit or insurance, uninteresting as a market for particular kinds of products and services. Profiling can and will exclude some and privilege others.[48]

Commissioner Stoddart added to these concerns, mentioning that:

> The fact that [the ad server] will determine the information you get, the ads you get, and sometimes, I believe, the rankings in search engines — I'm not sure about that — means that your experience of the Internet and the world of knowledge that the Internet represents will be limited. It will be based on what may be a true or a false or a partly true profile that algorithms are determining for you.[49]

As part of her testimony, Commissioner Stoddart drew the Committee's attention to a recent article by Professor Jeffrey Rosen of George Washington University that explains the effects of online profiling on consumers.[50] In it, Professor Rosen explains how Web-based interactions — such as participation in social networks, Internet searches and online shopping — are compiled by companies like Google, Facebook and BlueKai in order to create consumer profiles. These consumer profiles, in turn, allow individuals to be placed into categories based on interests and purchasing power and these, in turn, are sold to online advertisers through real-time bidding auctions. As such, individuals pass from being consumers to being a product sold to advertisers at different values. The danger is that these "profiles that define us forever can also be technologies of classification and exclusion (…) Unlike a marketplace where individuals haggle with sellers on equal terms, the new world of price discrimination is one where it's hard to escape your consumer profile, and you won't even know if companies are offering discounts to higher-status customers in the first place."[51]

Based on the research he has conducted, Professor Normand Landry identified for the Committee what he considers to be the four general dimensions encompassed by the right to privacy, along with the nine specific criteria applied to the protection of personal information. The four dimensions are: preservation of anonymity, freedom from surveillance, preservation of private space, and access to sound management of personal information. The individual, according to Professor Landry, must be able to "control access, circulation, sharing and accuracy of their personal information."[52] As for the specific criteria applicable to the protection of personal information, Professor Landry holds that everyone about whom information is collected should:

> … be properly informed that information is being collected; voluntarily participate in the collection; be able to identify the actors who are collecting the information; know the ways in which the information is being collected; be able to identify the nature of the

---

48 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1105 (Teresa Scassa, University of Ottawa).

49 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1655 (Jennifer Stoddart, Privacy Commissioner).

50 Ibid.

51 Jeffrey Rosen, "Who Do Online Advertisers Think You Are?" *The New York Times*, November 30, 2012.

52 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1540 (Normand Landry, TELUQ).

> information collected; know what uses will be made of the information; be able to identify the actors who may have access to the information and the rules that govern the confidentiality of the information; be able to assess whether the information is properly protected; and be able to access the information collected and rectify or remove personal information collected elsewhere.[53]

The importance of individual control was not solely cause for concern for academics and public interest groups. Mr. Robert Sherman of Facebook agreed that individuals must be able to exercise control over their information. "People will only feel comfortable sharing online if they have control over who will see their information and if they have confidence in the people who will receive it."[54]

D. Accountability and Openness

> *Collection no longer occurs right in front of you. It occurs in the background.*[55]
>
> *- Professor Valerie Steeves, University of Ottawa*

Accountability is the first of PIPEDA's 10 fair information principles, and it places an obligation on organizations to "designate an individual or individuals who are accountable for the organization's compliance" with the principles.[56] It is the first among the principles "because it is the means by which organizations are expected to give life to the rest of the fair information principles that are designed to appropriately handle and protect the personal information of individuals."[57] PIPEDA also upholds the principle of openness, which enunciates how "an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."[58]

According to the Privacy Commissioner, accountability goes to the range of a company's obligations under the law:

> It basically means being able to demonstrate that you have done all the things to make sure that you are privacy compliant: that you have a chief privacy officer, that your staff has been trained, that they know what to do, that you don't retain data longer than necessary, that you've invested in securing personal information, that you have the right

---

53 Ibid., 1540.

54 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1530 (Robert Sherman, Facebook).

55 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1120 (Valerie Steeves, University of Ottawa).

56 PIPEDA, Schedule 1, s. 4.1.

57 ETHI, Document submitted by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta, the Office of the Information and Privacy Commissioner of British Columbia, "Getting Accountability Right with a Privacy Management Program," p. 3.

58 PIPEDA, Schedule 1, s. 4.8.

> procedures so that when people come under the law asking to see their personal information, you know how to handle that, and so on.[59]

Witnesses mentioned that PIPEDA's current accountability model is well regarded internationally, in part because it is industry- and technology-neutral, and also because it promotes self-regulation by industry associations. As such, Mr. Adam Kardash of Heenan Blaikie stated that PIPEDA is "well positioned to appropriately address the privacy concerns that may arise in the online sector, and otherwise in the technological context."[60]

The Office of the Privacy Commissioner of Canada (OPC) and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia submitted a brief to the Committee that was developed together and intended for organizations subject to their respective private-sector privacy legislation. This document provides guidance on what it means to be an accountable organization and outlines the expectations of these offices regarding a privacy management program.[61]

Mr. David Elder of the CMA noted his organization's Code of Ethics and Standards of Practice is a model for how self-regulation can promote accountability within an industry.[62] Mr. Elder noted how the Code, which echoes the 10 privacy principles in PIPEDA, "strives to give consumers control of their personal information and to make the process of gathering and using customer information by marketers more transparent."[63]

Several witnesses, however, pointed out that accountability problems arise where there is a lack of openness or transparency by companies and in circumstances where the self-regulation model breaks down.[64] The Privacy Commissioner noted that this is particularly so in the social media world, as it is "constantly evolving with new entities popping up regularly in a hurry to get their new service on the market. Privacy does not appear to be a top priority for them."[65]

Social media companies have, so far, not created industry standards on accountability or transparency, leading Professor Ian Kerr to highlight the "need to mandate far greater transparency, not only about the collection of personal information,

---

59 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1650 (Jennifer Stoddart, Privacy Commissioner).

60 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1120 (Adam Kardash, Heenan Blaikie).

61 ETHI, Document submitted by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta, the Office of the Information and Privacy Commissioner of British Columbia, "Getting Accountability Right with a Privacy Management Program."

62 The CMA's *Code of Ethics and Standards of Practice* is available at http://www.the-cma.org/regulatory/code-of-ethics.

63 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1540 (David Elder, CMA).

64 See, for example, ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1225 (Michael Geist, University of Ottawa).

65 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1145 (Jennifer Stoddart, Privacy Commissioner).

but about how it is being used and to whom it's being disclosed. We need this both at the front and at the back end of social media transactions."[66]

In the Privacy Commissioner's opinion, "self-regulation is fine" but "it needs legislation to back it up."[67] Professor Kerr also supports setting minimum standards through legislative means, arguing that:

> … this is not just a point about tweaking privacy policies or making more understandable notice provisions. It is about legislating what I would call mandatory minimums—mandatory minimum standards for privacy transparency, requiring that they be embedded into technologies and in social techniques. We don't sell cars without speedometers, odometers, or fuel or pressure gauges. Likewise, our social media should be required to have feedback mechanisms that allow us to look under the hood and to warn us when conditions are no longer safe.[68]

The evidence before the Committee points to the need for increased accountability and openness on the part of social media companies. While these principles are already outlined in PIPEDA, current practices do not suggest that they are being adhered to their fullest effect.

Recommendation 1

The Committee recommends that the Privacy Commissioner of Canada establish guidelines directed at social media and data management companies to help them develop practices that fully comply with PIPEDA, particularly accountability and openness.

---

66 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1205 (Ian Kerr, University of Ottawa).

67 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1715 (Jennifer Stoddart, Privacy Commissioner).

68 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1205 (Ian Kerr, University of Ottawa).

E. Obtaining Consent in Social Media Contracts and Agreements

> *Social media companies need to clearly explain the purpose behind their collection, use, and disclosure of personal information, and what third parties, such as application developers they are sharing this information with. And they have to clearly obtain users' consent.*[69]
>
> *- Jennifer Stoddart, Privacy Commissioner of Canada*

The Committee heard evidence from Industry Canada explaining how Canada's privacy legislation "is founded on the principle of consent, whether that be expressed or implied, to collect, use, and disclose personal information."[70] Indeed, PIPEDA Principle 3 dictates that the "knowledge and consent of the individual are required for the collection, use or disclosure of personal information"[71] and places on organizations both an obligation to "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used," as well as to adjust the form of consent to "the sensitivity of the information" sought.[72]

However, witnesses pointed out a problem to the Committee in that consent-seeking forms are not placed or written in ways that are accessible to users who may not read these agreements and may not fully understand what they are consenting to. According to Professor Vincent Gautrais:

> An average social media user would have to spend 20 hours a month to read the privacy policies that apply to Google and all the websites they visit. That is unfeasible. Saying that protection goes through information and consent is an illusion.[73]

The Committee was apprised by many witnesses as to the problem of unclear or inaccessible language in consent forms; witnesses pointing out that such forms were impractical and placed unrealistic expectations on users. Professor Michael Geist of the University of Ottawa stated that:

> Even if we did have better language, the reality is that given the number of sites people visit and interact with, and given the move towards mobile and wireless environments, the notion that people are going to sit and read the privacy policy before they engage in a website every time is unrealistic.[74]

---

69 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1150 (Jennifer Stoddart, Privacy Commissioner).

70 Ibid., 1220 (Janet Goulding, Industry Canada).

71 PIPEDA, Schedule 1, s. 4.3.

72 PIPEDA, Schedule 1, ss. 4.3.2 and 4.3.4.

73 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1230 (Vincent Gautrais, Université de Montréal).

74 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1140 (Michael Geist, University of Ottawa).

Professor Scassa went further, arguing that the way these consent-seeking forms are worded means that they encompass matters that go beyond the protections afforded by privacy laws.[75] At present, these forms, also known as end-user license agreements, are consumer contracts or contracts of adhesion. As such, users should also be afforded the protections and safeguards currently present in both competition and consumer protection law. Such protection would include, for example, ensuring truth in advertising and additional protection for the weak and those unable to take care of themselves.

Professor Normand Landry noted that the language used in these binding agreements "makes it difficult for users to know exactly to what extent and which parameters are being used to protect their personal information";[76] while Mr. Pierrot Péladeau, a researcher and consultant appearing as an individual, pointed out that, generally speaking, the language used is "not appropriate for explaining the processes involved"[77] in the collection, use and disclosure of personal information. These concerns point to problems in how consent, while gained, may not be meaningful or informed.

Mr. Colin McKay of Google Canada acknowledged that companies are aware of the problem of long, complex agreements. He noted that his company is still in the process of evaluating and trying to identify the appropriate format, time and content to help users make appropriate decisions about their data. As part of this process, he said, Google recently unveiled changes to its privacy policy, taking what previously was "a very long and complex document" and breaking it down into "several simple elements for users to really understand how we're asking for information and what we're using it for."[78] The result, according to Mr. McKay, is that Google is "very specific about the information [they] collect and why [they] are collecting it from users."[79]

Mr. Robert Sherman of Facebook also told the Committee that his company has recently changed its "data use policy" — formerly its privacy policy — as a result of their recognition "that long and complex privacy policies can make it difficult for people to understand how their information is being used" and their desire to balance that with providing "people with specific and concrete information about our data management practices."[80] As he put it, this new policy is written in "plain language" meant to be "both easy to understand and comprehensive" and is accompanied by a "straightforward guide to privacy on Facebook."[81] And while Facebook does not allow users to accept only

---

75 Ibid., 1105 (Teresa Scassa, University of Ottawa).

76 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1545 (Normand Landry, TELUQ).

77 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1530 (Pierrot Péladeau, Researcher and Consultant in social assessment of information systems).

78 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1600 (Colin McKay, Google Canada).

79 Ibid., 1625.

80 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1530 (Robert Sherman, Facebook).

81 Ibid., 1530.

certain portions of the policy and not others, this is only because it would not be efficient "to provide different versions of Facebook for different people."[82]

Several witnesses, including Professor Ian Kerr and Mr. John Lawford of PIAC, saw reason for concern in the use of standard-form, "take it or leave it" contracts that leave users in a vulnerable position. Professor Kerr told the Committee that:

> The biggest threat to privacy is the standard form contract. Under our current law, almost all privacy safeguards that are built into our privacy legislation can easily be circumvented by anyone who provides goods or services by way of a standard form agreement. By requiring users to click "I agree" to their terms on a "take it or leave it" basis, companies can use contract law to sidestep privacy obligations. In short, this is based on a mistaken approach to the issue of consent.[83]

Mr. Lawford, for his part, added that:

> Social network privacy policies are "take it or leave it" contracts. The burden of determining what is done with personal information is borne by the user. Yet social networks regularly rely on the consent of users to justify practices and point to the use of the site as the equivalent of consent to the entire privacy policy.[84]

The Committee was further cautioned about the unilateral modification of contracts by service providers and the need for ongoing and informed consent from users. Mr. Jason Zushman emphasized that:

> … the provision of informed consent by the user is a necessity. That means when a user gives their consent to utilize the service, they must be asked to give consent throughout the entire process and for any subsequent evolution of that service or its terms of use. Users shouldn't be asked merely to provide their initial grant of consent to terms that could then be unilaterally modified by the service provider.[85]

In addition to changes made to privacy or data policies, witnesses warned about problems to the current consent model posed by changes in the context under which the information was collected — what Professor Avner Levin of Ryerson University calls "contextual privacy."[86]

Changes in context refer to the use or collection of information in one context, and its later use in another — either because of technological innovation or the use of the information by a third party. Contextual privacy speaks to the user's expectations of privacy and the challenges posed by social media in expanding the reach and use given to this information. Professor Avner Levin spoke to the issue as follows:

---

82 Ibid., 1625.

83 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1210 (Ian Kerr, University of Ottawa).

84 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1535 (John Lawford, PIAC).

85 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1550 (Jason Zushman, Merchant Law Group).

86 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1215 (Avner Levin, Ryerson University).

> There is a notion that is very relevant to social privacy, and it's the notion of network or contextual privacy … The key to understanding that is to understand that people, when they share information or they post information, don't actually think about how many people potentially have access to the information; they are really focused on who has access to that information at that point in time.[87]

In both circumstances, Professor Teresa Scassa noted that it is difficult for users to determine "what information is being collected, how it's being shared and with whom."[88] Yet, given the protection presently afforded by PIPEDA, the Privacy Commissioner emphasized that "[i]t is important to keep users properly informed, explaining new features in a timely fashion, and seeking their informed consent for new uses of personal information."[89]

The Committee received several recommendations that addressed these consent-related concerns, including, from Mr. Alan Chapell of BlueKai, that companies should provide "additional granularity in privacy statements and end-user licence agreements,"[90] and, from Professor Michael Geist, that informed consent could be achieved by "ensuring that there's respect for people's choices about consent and that there's adequate disclosure from the organizations collecting the information."[91]

Another recommendation put to the Committee would require companies to inform users of any changes to their privacy or data use, collection and disclosure practices and to seek their consent on the basis of any new conditions. In this vein, the Privacy Commissioner stated that:

> I think that companies should let their members, or their clientele, know that the conditions have changed, since the consent the consumer gave when subscribing did not apply to the new conditions. The company should at least indicate that the rules of the game have changed, so that the consumer can have the option to keep or cancel their subscription.[92]

A number of witnesses also proposed that companies be more transparent with regard to how user information is shared within organizations and with third parties. Mr. Jason Zushman suggested that:

> Users should also be told to what degree this information is shared not only within the organization but also with the public and also how it is shared with any third parties for

---

87 Ibid.

88 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1100 (Teresa Scassa, University of Ottawa).

89 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1150 (Jennifer Stoddart, Privacy Commissioner).

90 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1550 (Alan Chapell, BlueKai).

91 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1110 (Michael Geist, University of Ottawa).

92 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1630 (Jennifer Stoddart, Privacy Commissioner).

which certain uses of that information are not necessarily foreseen by the initial contract that the user enters into with the social media provider.[93]

Lastly, Ontario Information and Privacy Commissioner Ann Cavoukian suggested that "one way of trying to restrict the collection of personal information is by identifying specifically, very narrowly, that which you are permitting."[94]

The evidence before the Committee points to the difficulties faced by Canadians when they are asked to provide their knowledge and consent for social media contracts and agreements. It is imperative for the healthy operation of Canada's privacy laws and the safeguarding of individuals' privacy interests that, when consent is given, such consent be meaningful and appropriate in the circumstance, as provided in the PIPEDA principles. The Committee notes that to achieve this, the language put before individuals should be clear and accessible.

Recommendation 2

The Committee recommends that the Privacy Commissioner of Canada establish guidelines directed at social media and data management companies to help them develop policies, agreements and contracts that are drafted in clear, accessible language that facilitates meaningful and ongoing consent.

93 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1550 (Jason Zushman, Merchant Law Group).

94 ETHI, *Evidence*, 1st Session, 41st Parliament, June 7, 2012, 1225 (Ann Cavoukian, Information and Privacy Commissioner of Ontario).

F. Retaining and Deleting Personal Information

> *A basic privacy principle is the right to be forgotten, so in our laws, organizations can only retain information as long as they need it for business purposes and then it should be destroyed.*[95]
>
> *Elizabeth Denham,*
> *Information and Privacy Commissioner of British Columbia*

The Committee heard evidence from three federal and provincial privacy regulators, all of whom agreed that, while Canada's laws limit how long organizations can retain information, there is currently no effective way to enforce this limit. Commissioner Stoddart, in particular, lamented that "in fact, there may be no limits as to how long many companies keep information."[96]

This issue regarding the retention or deletion of information, the so-called "right to be forgotten", is compounded in social media, where personal information put forth by users may quickly be shared and distributed in ways that may make deletion difficult. Furthermore, the information may be subject to collection and use by third parties unknown to the user. As Mr. Jason Zushman put it:

> If consumers choose to share information with other third-party sites, the means to compel the destruction of any data they share should be available at the avenue through which they share with the third party. It is difficult when it trees down like that to enforce production and destruction of user data.[97]

Ontario Information and Privacy Commissioner Ann Cavoukian suggested that Canada's regulatory scheme learn from what its international counterparts are already doing:

> What the FTC and other organizations are doing now is building in the need for independent third-party audit, so that if the destruction of records has been ordered or required, it can then be confirmed after the fact.[98]

In addition to increased transparency on how long personal information is retained and how de-activated and deleted accounts are treated,[99] witnesses suggested that companies ought to build in mechanisms for the deletion of records, particularly when it

---

95 Ibid., 1250 (Elizabeth Denham, Information and Privacy Commissioner of British Columbia).

96 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1205 (Jennifer Stoddart, Privacy Commissioner).

97 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1655 (Jason Zushman, Merchant Law Group).

98 ETHI, *Evidence*, 1st Session, 41st Parliament, June 7, 2012, 1250 (Ann Cavoukian, Information and Privacy Commissioner of Ontario).

99 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1150 (Jennifer Stoddart, Privacy Commissioner).

comes to young people's personal information.[100] In a similar vein, Tamir Israel of CIPPIC argued for there being "a centralized place where individuals can ping data brokers and do searches of these data brokers all in one place" to determine who may have information on those individuals, what that information is and, where necessary, request corrections to that information.[101] Further, according to Mr. Israel and given PIPEDA's principles of individual access and openness, a mechanism could be put in place "that would talk to these organizations and get a sense of where their data's going, how it's being used, and where it's being collected from. That's a fact-finding type of expedition that I think would be really useful, but it's very difficult for individuals to undertake on their own.[102]

Certain companies that came before the Committee addressed the concern that they keep individuals' personal information indefinitely or that they do not facilitate requests for the deletion of data. In their appearances before the Committee, both Google and Facebook mentioned new services — Google's Takeout and Facebook's "download your information" — that allow users to download their information and take it with them if they want to use it elsewhere. They both also mentioned "dashboard" services that allow users to review the specific information those companies hold about them and ask for any correction to or deletion of that information. BlueKai also has a similar product, the BlueKai Registry, which allows users to see what tracking cookies BlueKai has stored on their computers, manage their topics of interest in their anonymous profile and "actually opt out from further use of their preference data."[103]

Mr. Colin McKay, on behalf of Google Canada, assured members that they "do not retain all the data that [they] collect" — that Google deletes it when it no longer becomes useful. As Mr. McKay put it, Google is "not in the business of creating a very large bucket of information about you. We're in the business of providing very useful services and products to you as an individual."[104]

Mr. Kevin Bartus, of Nexopia.com, a Canadian-based social networking site, explained that there are difficulties when it comes to developing retention and deletion policies and technologies, particularly for smaller companies with fewer resources. According to Mr. Bartus:

> Regarding keeping data of users who have gone, the only reason it's there is we're trying to figure out how to get rid of it technically, and from a business perspective, which parts of it to get rid of. Our feeling now is that certainly the profile data and any data—a blog, for example, that the user has posted—should vanish when the user leaves. Our thought is that perhaps you want to keep the data around for a little while in case the user wants

---

100 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1705 (Jennifer Stoddart, Privacy Commissioner).

101 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1210 (Tamir Israel, CIPPIC).

102 Ibid.

103 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1530 (Alan Chapell, BlueKai).

104 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1610 (Colin McKay, Google Canada).

> to come back (...) But certainly there is no business reason that I'm aware of for keeping the data longer than perhaps two years.[105]

In his appearance before the Committee, Mr. Robert Sherman of Facebook recognized that his company collects certain data from users and stores it in an activity log. This log is accessible to users who can then opt to delete this information. According to him, the goal is "to be transparent with people about the information we have" and the reason that information is kept is to make Facebook's "search functionality better by knowing what people are searching for and what they're clicking on" as well as for other "technical, debugging kinds of uses."[106] When users do chose to delete their information, Facebook begins a process they call 'active deletion' whereby "the content is deleted or logs that have identifying information are removed."[107] The timeframe for this process is not clear and, while Facebook may keep information logs that are anonymous after deletion, the "idea is generally that the information will get deleted."[108]

For its part, social media company Twitter's process for account deletion follows a "30-day grace period" during which the account is deactivated.[109] It is only after these 30 days pass that the deletion process begins. It was not clear to the Committee how long this additional process would take.

The evidence suggests that, while PIPEDA and its principles create limits for how long organizations can keep personal information and allow an individual to have access to that personal information, mechanisms are not always in place to ensure that these limits and right to access are being respected. Furthermore, the evidence before the Committee indicates that there exists an interest for individuals to request the deletion of any personal information that an organization may have about them.

Recommendation 3

The Committee recommends that the Privacy Commissioner of Canada establish guidelines directed at social media and data management companies to help them put in place mechanisms that ensure individuals have access to any personal information that those companies may hold about them, that limit how long those companies hold on to that information and that facilitate the deletion of such information.

---

105 ETHI, *Evidence*, 1st Session, 41st Parliament, November 6, 2012, 1540 (Kevin Bartus, Nexopia). For more information on Nexopia, please see the section entitled Evidence Specific to Certain Private Companies below.

106 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1550 (Robert Sherman, Facebook).

107 BlueKai, 1625.

108 Ibid.

109 ETHI, *Evidence*, 1st Session, 41st Parliament, December 6, 2012, 1550 (Laura Pirri, Twitter). For more information on Twitter, please see the section entitled Evidence Specific to Certain Private Companies below.

CHILDREN AND SOCIAL MEDIA

> *I would suggest to you being very cautious about any claim that kids don't care about privacy because they post their lives on Facebook. Anyone who says that just hasn't taken the time to talk to kids; they care deeply about online privacy.*[110]
>
> *- Professor Valerie Steeves, University of Ottawa*

Presently, PIPEDA does not make specific provisions regarding the personal information of children or young persons. Rather, the collection, use, or disclosure of a minor's personal information is more generally governed by provisions on consent and the requirement that the knowledge and consent of the individual be obtained, as well as the responsibility placed upon companies to achieve both meaningful consent and take into account the sensitivity of the information. Based on this, social media companies have developed the practice of having different privacy protections for young users (such as requiring a parent or guardian's consent) and, in some cases, not allowing minors under the age of 13 to join their social networks.

Bill C-12, An Act to amend the Personal Information Protection and Electronic Documents Act,[111] addresses how valid consent would be achieved under PIPEDA by adding a new section 6.1 that stipulates as follows:

> For the purposes of clauses 4.3 to 4.3.8 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting.[112]

According to Industry Canada, these changes to PIPEDA would result in enhancements to the consent provisions under the law and "are designed to protect the privacy of minors online."[113] Ms. Janet Goulding further explained that this provision would require organizations to make a reasonable effort when collecting the personal information of minors to clearly communicate why the information is being collected and to do so in a way that they would understand.[114]

The Committee heard a significant amount of evidence regarding the particular situation and vulnerability of children and youth when it comes to their use of social media. In particular, witnesses expressed the concern that children and youth are particularly targeted by online companies for their personal information, often without the necessary safeguards to ensure the full knowledge or consent of the children or their parents.

---

110 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1120 (Valerie Steeves, University of Ottawa)

111 Bill C-12: An Act to Amend the Personal Information Protection and Electronic Documents Act, 1st Session, 41st Parliament. The Bill is discussed in detail further below in the section entitled "Canada's Legislative Framework in an Evolving Landscape."

112 Bill C-12, c. 5.

113 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1225 (Janet Goulding, Industry Canada).

114 Ibid.

These witnesses also spoke at length about balancing the privacy rights of children with the responsibilities that parents and guardians have in ensuring that children's interactions with social networks are safe.

A. The Targeting of Children by Social Media Companies

Witnesses repeatedly pointed to research showing the particular situation confronting children when they go on the Internet. According to Ms. Janet Goulding:

> Research shows that children may not have the capacity to understand the consequences of sharing personal information. Not all marketing activity directed at children is inappropriate; however, some online services surreptitiously collect personal information about children in an environment that is often designed to look like playgrounds or educational websites.[115]

Professor Sara Grimes of the University of Toronto explained to the Committee that studies show that "since the very early days of the World Wide Web, kids' privacy rights have been infringed upon for commercial purposes within certain online social forums."[116] She finds that this happens with much greater frequency than with most of the other risks associated with children online; children's online interactions, she said, "are being surveilled and data-mined, most often without the full knowledge or consent of the kids involved, or that of their parents and guardians."[117]

Mr. Matthew Johnson of MediaSmarts, a non-profit centre for digital and media literacy, drew attention to his organization's research and that of others around the world that demonstrate how "the landscape online for young people is tremendously commercialized; that the majority of the sites most popular with young people are commercial sites," resulting in young people being "tracked online more aggressively than adults."[118] Consequently, he cautioned, young people are subject to greater risks than adults when it comes to their online privacy.

Indeed, the testimony before this Committee from Nexopia indicated how members of their site, which is specifically youth-oriented, "are more engaged than members on most other social networks, with about six minutes and 14 pages per visit, compared to an average of about five minutes and 10 pages … of [other] social networking sites."[119] Such high engagement demonstrates how much children and youth may be exposing their personal information and online practices to social media companies.

---

115 Ibid.

116 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1100 (Sara Grimes, University of Toronto).

117 Ibid.

118 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1615 and 1620 (Matthew Johnson, MediaSmarts).

119 ETHI, *Evidence*, 1st Session, 41st Parliament, November 6, 2012, 1530 (Kevin Bartus, Nexopia)

Ms. Jane Tallim, Co-Executive Director of MediaSmarts, underscored the fact that young people do care about their privacy even if their understanding of privacy or how they exercise it may differ from adults.

> It's a widely held belief that young people, whether they be Facebook addicts or aspiring YouTube celebrities, don't care about privacy. This isn't true. In fact, the way youth understand privacy may be more relevant than how most adults view it, because they see it not as a matter of deciding whether or not to share, but as having control over the things they want to share.[120]

In response to the Committee's concern over social media companies' specific practices towards young users and their unique vulnerability, Mr. Robert Sherman noted that Facebook's default settings "in general are more limited for teenagers" and that Facebook wants to put "minors in a place that's a bit more limited, speaking in a smaller community."[121]

Other companies, including Twitter, do not allow the participation of users under 13 at all. Where, counter to the privacy policy, users under that age do join and Twitter becomes aware of the situation, the account is deleted.[122] Additionally, Twitter provides resources for parents and teens on how to use its platform, including how to report harassment.[123]

In discussing ways to protect children from data-mining and potentially privacy-breaching practices, Professor Grimes suggested looking at other countries that have enacted child-specific privacy legislation:

> The key example here is the U.S. Children's Online Privacy Protection Act, or COPPA, which was initially created in response to the then growing practice of soliciting names and addresses from children in order to direct-market to them.[124]

Other witnesses focused on what could be done by children and parents to protect themselves. Mr. Jason Zushman of the Merchant Law Group suggested supporting "education and public awareness programs that let kids know that the Internet isn't necessarily a safe place and that provide for different educational initiatives to help them realize that when you put something out there you're not necessarily getting it back and that it can have lasting consequences would be worthwhile initiatives."[125] MediaSmarts also suggested education and the early development of digital literacy skills as ways to help prevent unwanted exposure of children's personal information online. As Jane Tallim

---

120 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1535 (Jane Tallim, MediaSmarts).

121 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1600 (Robert Sherman, Facebook).

122 ETHI, *Evidence*, 1st Session, 41st Parliament, December 6, 2012, 1555 (Laura Pirri, Twitter).

123 Ibid., 1620.

124 ETHI, *Evidence, 1st Session,* 41st Parliament, June 19, 2012, 1100 (Sara Grimes, University of Toronto).

125 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1700 (Jason Zushman, Merchant Law Group).

put it, “Privacy education must be supported on a national level, both through the K to 12 curriculum in schools and public awareness campaigns to inform all Canadians.”[126]

Recommendation 4

The Committee recommends that the Government of Canada and social media companies continue to provide support to organizations that provide education and training on digital activities and privacy.

B. Achieving Informed Consent

The Committee also heard important evidence concerning how social media companies request consent from children, young persons and parents. Mr. David Elder of the CMA reminded the Committee that PIPEDA’s provision on consent is “already flexible enough and recognizes that it requires a different standard when you’re talking to children.”[127] Nevertheless, other witnesses were concerned that, in spite of the flexibility afforded by PIPEDA, the protection provided is not enough and some companies are taking advantage of this gap.

Professor Sara Grimes relied on her research to conclude that children are regularly asked to agree to data-collecting activities through the privacy policies and terms of use required to participate on sites designed and targeted to younger children. This raises an issue of informed consent, as these “long and extremely complex documents…describe a wide variety of data collection activities and include a number of terms that are inappropriate and even inapplicable to ask children to agree to.”[128] In her opinion, these contracts could not actually be expected to be upheld, yet the practice and resulting risks remain.[129]

The concern over current practices that place the onus on young users to understand what they are agreeing to and having the necessary know-how to prevent unwanted invasions of privacy was also shared by Professor Normand Landry of TELUQ. He warned that, while young children have access to social networking sites, they are not able to exercise real control over their personal information; as such, more responsibility should be placed on the sites, as they are the ones who “take [the young children] in when

---

126 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1535 (Jane Tallim, MediaSmarts).

127 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1700 (David Elder, CMA).

128 ETHI, *Evidence, 1st Session,* 41st Parliament, June 19, 2012, 1100 (Sara Grimes, University of Toronto).

129 Ibid., 1145.

they don't have the training, resources or skills necessary to pay attention to the information provided."[130]

According to Professor Grimes, in order to address this problem, the Committee should consider current best practices, which would include:

> … providing a child-friendly version of both [privacy policies and terms of use] to ensure that children and their parents know exactly what they're agreeing to. While there are definitely some really great examples of this practice out there, overall very few sites for kids bother to do it. When they do, the child-friendly versions are rarely comprehensive: most don't explain the full reasons for user data collection or only describe items that present the social media company in a positive light.[131]

The witnesses representing MediaSmarts agreed, submitting to the Committee their position that young people do need to understand what they are agreeing to. According to Mr. Matthew Johnson, young people:

> … need to understand when they use any service, what information they are giving out, what information about their activities may be collected, and what will be done with that information by either the operator of the service or third parties to whom it may be sold.[132]

In the opinion of MediaSmarts, the solution to this problem would involve increased openness or transparency, more likely achievable "from a combination of legislation, industry regulation, consumer action," as well as educating young people on privacy "so that young people are able to understand that this information is available to them and to make use of it in an effective way."[133] Such education, they contend, would extend to having children and parents understand that they have a right to privacy, that their personal information has value and that they have legal and contractual recourse in protecting it.[134]

Recommendation 5

The Committee urges social media companies to play a larger role in promoting safe and active online activities that protect the privacy and personal information of individuals, particularly in regard to vulnerable groups such as children and young persons.

---

130 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1620 (Normand Landry, TELUQ).

131 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1100 (Sara Grimes, University of Toronto).

132 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1555 (Matthew Johnson, MediaSmarts).

133 Ibid.

134 Ibid., 1535 (Jane Tallim, MediaSmarts).

C. Balancing Children's Privacy Rights with Parental Duties and Concerns

While aware of the risks posed by social media and other Web sites to the personal information of children, witnesses also cautioned the Committee of the risks posed by overprotection; what Ms. Jane Tallim called "the constant surveillance by parents, schools, and corporations, and young people's acceptance of it."[135] According to Ms. Tallim:

> Privacy is a fundamental human right, and continuous surveillance chips away at our private space. Moreover, this constant scrutiny undermines the mutual trust, confidence, and communication between adults and youth that is essential to giving young people the autonomy they need to develop digital life skills.[136]

To address this, MediaSmarts proposed, in addition to privacy education, widening "the current focus on privacy safety risks to include privacy rights, ethical use, recourse mechanisms, and the civic and democratic dimensions of privacy."[137] By inculcating young people with the idea that privacy has an ethical dimension, MediaSmarts believes young people will be able to "expect and indeed demand that their personal information be treated ethically by the spaces, the corporations, to whom they give it."[138]

In addition to such calls for education and a wider scope for privacy rights, Professor Valerie Steeves of the University of Ottawa suggested that social media companies facilitate children's ability to delete the information about them online. As she put it, "you need a forget button", as "there is definitely something different when you're a minor."[139]

In their testimony, witnesses pointed to different tools that currently exist to help children and their parents protect their personal information and privacy online. MediaSmarts, for example, mentioned some of the programs and guidelines they have developed to help young people understand information privacy, such as their Privacy Pirates game and their Digital and Media Literacy Fundamentals program and the resources developed as a result of their survey of digital and media education across Canada.

The social media companies that appeared before the Committee noted that they are listening to the concerns of parents, teachers and regulators regarding children's use of their networks. Mr. Colin McKay, testifying on behalf of Google Canada noted that his company has built some extra protection into its social networking product, Google+, specifically for youth and which encourages safe online behaviour. As he told the Committee:

---

135 Ibid., 1530.

136 Ibid.

137 Ibid., 1535.

138 Ibid., 1635 (Matthew Johnson, HabiloMédias).

139 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1155 (Valerie Steeves, University of Ottawa).

> Posting something for everyone to see on a social network is an especially big deal for young people, so when teens try to share outside their circles we put in an extra confirmation step that encourages them to think before they post. We have also built default protections that block strangers from directly contacting or even saying hello to teens without a teen's express permission.[140]

For his part, Mr. Robert Sherman of Facebook noted that his company provides resources on security awareness and online safety, including a "family safety centre" with specific content for parents, teens, educators, and law enforcement, as well as a "safety advisory board" that provides expertise on products and policy.[141]

The Committee also heard of the youth-specific resources that the OPC has produced, including the Youth Privacy Web site youthprivacy.ca, and the extensive research studies it has funded, including the *Young Canadians in a Wired World* series and the *eGirls Project* (in which both Ms. Jane Tallim and Professor Valerie Steeves participate as researchers).

Recommendation 6

The Committee recommends that the Government of Canada and social media companies continue to provide support to organizations dedicated to educating and promoting awareness to children, their parents and teachers to protect their personal information and privacy online.

140 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1535 (Colin McKay, Google Canada).

141 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1535 (Robert Sherman, Facebook).

D. The Importance of Digital Literacy

> *Generally speaking, a person's ability to determine their own privacy parameters on a social media site calls for a high level of information literacy.*[142]
>
> *- Professor Normand Landry, TELUQ and Professor Leslie Regan Shade, University of Toronto*

Related to the issue of children and social media networks is the matter of digital literacy. "Digital literacy" describes the range of skills needed by individuals to make wise, informed and ethical online decisions.[143] Privacy management is one of the core skills necessary for digital literacy. Digital literacy is considered a central component of a larger digital economy strategy.[144]

According to Mr. Brendan Wicks of the MRIA, the experience of social media research practitioners indicates that most Canadians who publish information online "have a good understanding of the impact of their actions and they know what steps to take to protect their information."[145] Consequently, the MRIA finds that high standards-based ethical business practices, combined with the informed, deliberate actions of Canadians when they post information online are a "golden mean" that ought to be maintained.[146]

However, the Committee heard other witnesses that were less convinced about the levels of understanding of Canadian social media users and who insisted on the need to develop digital literacy tools with which to educate Canadians on the use of online services and eventually maximize the opportunities inherent to this nascent industry. Mr. Colin McKay of Google Canada advocated for Canada, as a society, to

> take the steps to make sure, as we evolve into a society that communicates online, that not only young people, but every generation has access to educational tools that allow them to work through how they should be sharing on social media sites, how they should be using online services, and the context within which they want to share information or make information public or restricted.[147]

The Committee also heard from researchers and academics that strongly insisted on the need to "take digital literacy education seriously" and to "support public-interest organizations so they can provide people with the information they need to make intelligent

---

142 ETHI, Brief submitted by Normand Landry and Leslie Regan Shade, "Privacy and Social Media: Privacy Issues," November 15, 2012, page 9.

143 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1530 (Jane Tallim, MediaSmarts).

144 See, for example, the submissions to the 2010 Public Consultations on Canada's Digital Economy by Bell Canada, the Ontario Literacy Coalition, ABC Life Literacy Canada, Prof. Catherine Middleton and the Media Awareness Network, amongst others.

145 ETHI, *Evidence*, 1st Session, 41st Parliament, June 5, 2012, 1115 (Brendan Wycks, MRIA).

146 Ibid.

147 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1605 (Colin McKay, Google Canada).

choices and informed decisions on the Internet."[148] According to Ms. Jane Tallim, as part of a wider digital strategy, such assistance should also be extended to teachers so they can have some guidance and consistency when teaching the core competencies related to privacy education and other digital literacy skills.[149]

Ms. Tallim went on to note the different roles that different stakeholders, such as government, industry and communities can play, stating that:

> The federal role can provide leadership in supporting gatherings, events, facilitating opportunities for multiple stakeholders to come together and conceptualize what this framework might look like, what the needs are. What really is apparent in countries where they have digital literacy as a pillar in their national strategy is this notion that it's not just government led, it's not industry led, it's not just community led, that you really do have to bring multiple stakeholders together to work together.[150]

Mr. Gupta of the Information and Technology Association of Canada (ITAC) also honed in on the different actors that need to be involved in developing a digital strategy and believes that:

> To create those conditions, we need to have the framework that supports all of the pieces. Privacy and the social media is only one aspect of it. The other aspects are equally important. We need to have the appropriate intellectual property regime. We need to have appropriate taxation policies. We need to have proper education standards. All of these dots need to be connected.[151]

The Privacy Commissioner echoed these sentiments, stating that she believes:

> … that the moment has come for government, for educators, and for our communities to seriously focus attention on the digital education of all Canadians of all ages. (…) People need to understand that information on the Internet can live on forever and that they should be careful about what they post about themselves and others.[152]

In her opinion, even if digital literacy rates do increase, it is but one piece of the privacy and social media issue, one that "does not absolve companies of their obligations under privacy law."[153] The Committee agrees that Canadians need to have better access to privacy education tools.

---

148 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1130 (Valerie Steeves, University of Ottawa).

149 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1600 (Jane Tallim, MediaSmarts).

150 Ibid., 1605.

151 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1640 (Karna Gupta, ITAC).

152 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1625 (Jennifer Stoddart, Privacy Commissioner of Canada).

153 Ibid.

Recommendation 7

The Committee recommends that the Government of Canada continue to provide support to digital literacy programs.

CANADA'S LEGISLATIVE FRAMEWORK IN AN EVOLVING LANDSCAPE

The Committee heard witnesses praise Canada's privacy legislation for its promotion of self-regulation, and for being flexible and technology-neutral. Nevertheless, the Committee also heard wide-ranging testimony questioning whether Canada's privacy legislation, and PIPEDA in particular, is up to the task of handling the challenges brought about by changing technology; the evidence heard ranged from maintaining the status quo, to making tweaks to PIPEDA, to wholesale reconsideration of the law. The discussion below highlights how Canada's current legislation and main federal regulator, the Privacy Commissioner of Canada, have been able to adapt to the challenges and opportunities brought about by social media, and aims to inform future discussions on how to adapt the law and the powers of the Privacy Commissioner to these developments.

Those mainly favourable to maintaining PIPEDA's status quo were witnesses representing the private sector or industry associations. These witnesses argued that, as presently written and applied, PIPEDA is a good law that meets the demands of industry and privacy rights, and facilitates self-regulation. They said that changing it is not necessary or advisable.

Mr. Colin McKay lauded Canada's "particularly interesting and useful privacy framework" that facilitates open dialogue and consultations with the Privacy Commissioner about upcoming products and services.[154] Similarly, Mr. David Elder of the CMA, noted the "delicate legislative balance between individual interests and business needs [that] produces significant benefits for both consumers and for information-based marketers, who comprise an increasingly significant sector of the Canadian economy."[155]

Mr. Warren Everson of the Canadian Chamber of Commerce drew attention to the fact that, as presently drafted, PIPEDA already bans the collection of personal information for reselling without the individual's consent, making self-regulation in this regard a moot point.[156] In the opinion of the Canadian Chamber of Commerce "there is nothing in social media that stretches PIPEDA to the breaking point."[157] Further, Mr. Everson noted that

---

154 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1545 (Colin McKay, Google Canada).

155 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1540 (David Elder, CMA).

156 ETHI, *Evidence*, 1st Session, 41st Parliament, June 5, 2012, 1140 (Warren Everson, Canadian Chamber of Commerce).

157 Ibid., 1100.

"the rules for privacy in Canada are well known, they are well understood, and in my estimation they work. They have adapted remarkably well in the digital world, and they provide quite strong protections for Canadians."[158]

Mr. Adam Kardash of Heenan Blaikie was also positive about PIPEDA's applicability in the social media context:

> In my view, PIPEDA has worked and continues to work particularly well in addressing privacy challenges raised by new technologies… One of the reasons the statute remains effective today is because it was drafted in a technologically neutral fashion. PIPEDA's core rules are mainly set out in plain language as broad principles, and therefore can be applied to any new technology, new application, or new system that involves the processing of personal information, including social media platforms.[159]

He went on to add that "under PIPEDA, a self-regulatory framework developed by way of a meaningful consultation process would have legal value under the statute. Self-regulatory frameworks establish industry standards, and well-developed industry standards inform the meaning of PIPEDA's overarching reasonable person test."[160]

Other witnesses, while also generally positive about PIPEDA, focused on the dangers and risks inherent in changing Canada's privacy framework. Mr. Kevin Bartus, owner of Nexopia.com, a social networking site for youth, noted the important role that Canadian privacy regulations play "in protecting Canadians and in levelling the playing field among digital corporations," yet cautioned the Committee to "tread carefully when making this any more challenging than it needs to be."[161] Ms. Annie Pettit of the MRIA warned that "if [Canadian marketing research companies] are unable to compete in the social media research space because our privacy standards restrict us rather than let us self-regulate, our clients will have to use social media research conducted in places with less-than-high ethical standards."[162]

Lastly, Mr. Alan Chapell of BlueKai cautioned that legislative change may both have unintended consequences and prove unable to keep pace with rapidly evolving technologies, while noting that "the beauty of self-regulation, if there's an adequate enforcement mechanism, is that it can continue to grow and morph around the innovation that's going on in the marketplace."[163]

However, the Privacy Commissioner, as well as other witnesses from academia and public interest groups, were less inclined to leave Canada's privacy legislation untouched, arguing that the law needs to be strengthened in order to respond to

---

158 Ibid.

159 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1120 (Adam Kardash, Heenan Blaikie).

160 Ibid.

161 ETHI, *Evidence*, 1st Session, 41st Parliament, November 6, 2012, 1530 (Kevin Bartus, Nexopia).

162 ETHI, *Evidence*, 1st Session, 41st Parliament, June 5, 2012 (Annie Pettit, MRIA).

163 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1610 (Alan Chapell, BlueKai).

the privacy challenges presented by new technologies, including social media. Tamir Israel of CIPPIC noted that "PIPEDA has largely withstood the test of time [but] the privacy landscape has changed substantially since its enactment, and a decade of experience has exposed a number of shortcomings that should be addressed if the statute is to continue to meet its objectives."[164]

The opinions expressed by this group of witnesses ranged from recognizing how the privacy landscape has changed and Canada's need to adapt to these changes through specific, privacy-related reforms, to larger reviews of a wider spectrum of data and consumer protection laws.

Mr. John Lawford of PIAC was of the opinion that PIPEDA "really just needs tweaks" that focus on providing "teeth in the enforcement."[165] Mr. Jason Zushman of the Merchant Law Group also suggested that privacy laws become "more robust" by way of stronger enforcement mechanisms, asserting that:

> Effective consequences should be brought to bear in relation to damages in tort, common law, or other breaches of statute. Consequences should be strictly enforced to effect deterrence and to protect the privacy rights of all Canadians.[166]

Professor Colin Bennett of the University of Victoria particularly addressed the question of changes to privacy legislation in light of the rise of social media and the changes in why and how personal information is collected and used:

> … it is true that our privacy protection rules need to be considered and updated in relation to social media, and particularly with respect to this issue. Our laws, such as the Privacy Act and PIPEDA, were developed with the notion of a distinction in mind between an organization and a subject, or between a controller of data and an individual. Now that distinction has broken down as social media sites are producing and selling data that is actually generated by users. It's that notion of user-generated data that really does challenge some of the existing principles within our privacy protection laws.[167]

For her part, Professor Teresa Scassa of the University of Ottawa told the Committee that "the collection, use, and disclosure of personal information is no longer simply an issue of privacy, but also raises issues of consumer protection, competition law, and human rights, among others."[168] As such, "data protection law reform is overdue and may now require a reconsideration or modification of the consent-based approach, particularly in contexts where personal data is treated as a resource and personal data collection extends to movements, activities, and interests."[169] In her opinion, there is a

---

164 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1110 (Tamir Israel, CIPPIC).

165 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1550 (John Lawford, PIAC).

166 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1555 (Jason Zushman, Merchant Law Group).

167 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1625 (Colin Bennett, University of Victoria).

168 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1110 (Teresa Scassa, University of Ottawa).

169 Ibid.

"need for a more multidisciplinary, multi-faceted approach to some of these issues," one that includes other disciplines, such as competition law or human rights law.[170]

Ms. Janet Goulding of Industry Canada suggested that the second five-year parliamentary review of PIPEDA, which is now due, would be a good opportunity to take another look at the legislative issues raised by the Committee's study.[171]

Lastly, summarizing what the Committee had heard and providing her own perspective, Commissioner Stoddart argued for changes to strengthen PIPEDA and, in particular, its enforcement model:

> The most important question put forward throughout the study was whether PIPEDA is up to the task of handling the challenges brought about by changing technology. Most witnesses felt that PIPEDA needs to be modernized. Others took the position that PIPEDA does not need to be changed, that its enforcement model works, and that its technology-neutral character is its strength.
>
> In my view, with the emergence of Internet giants, the balance intended by the spirit and letter of PIPEDA is at risk. The quasi-monopoly of these multinationals has made PIPEDA's soft approach, based on non-binding recommendations and the threat of reputation loss, largely ineffective, I believe. We have seen organizations ignore our recommendations until the matter goes to court. We have seen large corporations, in the name of consultation with my office, pay lip service to our concerns and then ignore our advice. Moreover, with vast amounts of personal information held by organizations on increasingly complex platforms, the risk of significant breaches and of unexpected, unwanted, or even intrusive uses of that information calls for commensurate safeguards and financial consequences not currently provided for in PIPEDA.
>
> New incentives, including changes to the enforcement model, are required to encourage organizations to be proactive, to build upfront protections, and to ensure secure treatment of individuals' personal information. I agree with the witnesses who stated that PIPEDA's strength is that it is technology-neutral and principles-based. These are characteristics that must remain.[172]

The Committee heard wide-ranging evidence regarding Canada's legislative framework and, more particularly, PIPEDA. 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.

---

170 Ibid., 1150 (Teresa Scassa, University of Ottawa).

171 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1235 (Janet Goulding, Industry Canada).

172 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1615 (Jennifer Stoddart, Privacy Commissioner).

A. Current Amendments before the House of Commons (Bill C-12)

> *Bill C-12 will create a powerful tool to protect and empower consumers online.*[173]
>
> *- Janet Goulding, Department of Industry*

The Committee heard from several witnesses with respect to Bill C-12, An Act to amend the Personal Information Protection and Electronic Documents Act,[174] which is currently at first reading before the House of Commons. The Bill is the result of the first five-year review of PIPEDA, conducted by this Committee between November 20, 2006 and February 22, 2007, with the final report issued on May 2, 2007.

According to Ms. Janet Goulding, from Industry Canada:

> Bill C-12 requires organizations to notify individuals in cases where a breach poses a real risk of significant harm, such as identity theft or fraud or damage to reputation. The Privacy Commissioner will also be informed of any material breach, thus allowing her to exercise oversight of compliance with the new requirements. Consistent with her current compliance powers, the Commissioner will be able to publicly name organizations that fail to meet their obligations if she feels this is in the public interest. This is a powerful inducement for organizations to act in good faith.[175]

In terms of reaction to the proposed legislation, some witnesses, including Tamir Israel, told the Committee that Bill C-12 was a positive first legislative step in addressing privacy-related concerns, but cautioned that other steps may need to be taken. 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."[176]

One of the highlights of Bill C-12 is a new proposed provision with respect to data breach notification, which allows the company suffering a breach to make the determination of whether the breach is material enough to report to the Privacy Commissioner. However, Mr. John Lawford suggests that such a provision will not succeed as "it's extremely unlikely, in our view, that any company, but particularly a social network that trades in data, will declare that it has a systemic problem with data breaches and data handling that leads to breaches."[177] Speaking for the PIAC, Mr. Lawford went on to "confidently predict that under Bill C-12 a social network or other online company will almost never notify the Privacy Commissioner of a breach that has not otherwise been made public."[178]

---

173 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1225 (Janet Goulding, Industry Canada).

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

175 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1225 (Janet Goulding, Industry Canada).

176 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1115 (Tamir Israel, CIPPIC).

177 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1530 (John Lawford, PIAC).

178 Ibid.

Commissioner Stoddart is largely of the same view as Mr. Lawford, expressing her 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."[179] She went on to suggest the need to establish a penalty system that would 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. According to the Commissioner, Bill C-12 may already be outdated.

B. The Enforcement Powers of the Privacy Commissioner

> *What others like about our law is that it does not single out sectors and is non-prescriptive. Yet, given that many of my international counterparts either have stronger enforcement tools or are requesting them, it is not our enforcement model they are admiring.*[180]
>
> *- Jennifer Stoddart, Privacy Commissioner*

Under PIPEDA, the Privacy Commissioner currently has the power to receive or initiate, investigate, and attempt to resolve complaints about any aspect of an organization's compliance with the law's data protection provisions. The Commissioner does not have the power to enforce any recommendation emanating from her investigations, and will usually attempt to resolve any contraventions through persuasion and negotiation. However, where this ombudsman approach fails and matters remain unresolved, the Commissioner has the power to file suit before the Federal Court, which will conduct its hearings *de novo* and can issue any judicial remedy, including ordering compliance and awarding damages.

The Committee heard evidence both praising and criticizing the ombudsman model and role that the OPC has under PIPEDA. Those praising the model, such as Mr. Adam Kardash of Heenan Blaikie, noted how well it is received by private sector organizations, as it "facilitates flexible and collaborative interaction" between them and the OPC.[181] Mr. Mark Hayes of Nexopia praised the fact that the Privacy Commissioner's current role prevents her from being "judge and jury," as the Privacy Commissioner does not do any adjudication. He warned that, should this role change, "it's entirely possible that the balance that now exists in terms of the ability to be able to advocate, the ability to be able to work with privacy commissioners around the world, as this commissioner has done extremely well, may in fact be somewhat compromised. It just changes the nature of the balance."[182] Mr. David Elder made a similar argument, also adding that changes to the ombudsman model would "fundamentally" change the relationship between the OPC and the business community, leading to "an awful lot less" communication and cooperation

---

179 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1625 (Jennifer Stoddart, Privacy Commissioner).

180 Ibid., 1620 (Jennifer Stoddart, Privacy Commissioner).

181 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1125 (Adam Kardash, Heenan Blaikie).

182 ETHI, *Evidence*, 1st Session, 41st Parliament, November 6, 2012, 1545 (Mark Hayes, Nexopia).

between the two.[183] For his part, Mr. Adam Kardash added that a move away from the ombudsman model would be costly and require structural changes to the OPC.[184]

Mr. Colin McKay of Google Canada added his voice to those cautioning against change, warning the Committee that "a move to a system that is more enforcement-based would prompt some caution on the part of companies" and noted that it would force companies such as his to "consider the possible repercussions of having that open a discussion of how our products roll out and how the Privacy Commissioner interprets our actions."[185] In a similar vein, Mr. Karna Gupta from ITAC stated that the general consensus in the IT sector is that "we do not need to create different. The Privacy Commissioner has the trust of the industry today and they work extremely well together on an on-going basis. The industry's view is that they would like to see it stay that way."[186]

However, the Information and Privacy Commissioners of British Columbia and Ontario, who both have order-making powers, "a very powerful tool", were amongst those who expressed concern over the federal Privacy Commissioner's enforcement powers.[187] They argued that the lack of enforcement power resulted in corporations ignoring the Privacy Commissioner's recommendations and continuing practices that run counter to Canadian privacy law.[188] As Mr. John Lawford noted:

> … the Privacy Commissioner has no order-making power. She has no fining power. Social networks that judge privacy findings too inconvenient or expensive, it appears, can continue to operate in a privacy-violating manner. (…) the refusal reveals the real nature of social networks: they are financed by personal information. Asking a social network to destroy data appears to them like removing an asset from the balance sheet.[189]

The MRIA, unlike other private sector witnesses that appeared before the Committee, was also "supportive of stronger enforcement powers for the Privacy Commissioner of Canada."[190] For his part, Tamir Israel characterized enforcement as "critical" for two reasons: to provide incentives for compliance and to assist in interactions with large multinational corporations when seeking to protect the privacy of Canadians.[191]

In discussing enforcement powers that would allow the Privacy Commissioner to react to privacy breaches, witnesses specifically referred to the power to make orders,

---

183 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1635 (David Elder, CMA).

184 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1130 (Adam Kardash, Heenan Blaikie).

185 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1605 (Colin McKay, Google Canada).

186 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1600 (Karna Gupta, ITAC).

187 ETHI, *Evidence*, 1st Session, 41st Parliament, June 7, 2012, 1250 (Elizabeth Denham, Information and Privacy Commissioner of British Columbia) and 1145 (Ann Cavoukian, Information and Privacy Commissioner of Ontario).

188 See Privacy Commissioner's quote above in footnote 172.

189 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1530 (John Lawford, PIAC).

190 ETHI, *Evidence*, 1st Session, 41st Parliament, June 5, 2012, 1120 (Brendan Wycks, MRIA).

191 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1115 (Tamir Israel, CIPPIC).

award damages and issue penalties. Professor Teresa Scassa suggested that the power to levy fines or impose penalties should be given to the Commissioner and used "in the case of egregious or repeated transgressions."[192] She added:

> As for administrative penalties, I think that would be an important weapon in the arsenal of the Privacy Commissioner. Not only does the administrative penalty impose a sanction on companies, which can be important in signalling that there has been a lapse in behaviour that is problematic and needs to be addressed, but it also has a more public shaming dimension as well. I think one of the concerns that's frequently been expressed about PIPEDA is that the commissioner has taken a very soft approach to dealing with corporations and doesn't name names, particularly in the context of most complaints, and so on, so that there's not enough information provided.[193]

While less inclined to allow for "heavy-handed fines," Tamir Israel suggested that the threat of a penalty would prove "very necessary to get both proactive and reactive compliance" since "without the possibility of a penalty, there's often little incentive to practicably figure out what these principles are and really integrate them into your business model."[194]

For his part, Mr. Jason Zushman of the Merchant Law Group raised the possibility of considering laws that provide for quantification of damages that are in direct relation to the profit, or multiples of profit, of companies that have misused user information. According to Mr. Zushman, one option would be to look at a hybrid model that promoted the cooperation of businesses and global social media organizations with whom Parliament could work on developing relevant laws and regulations to protect the privacy of all Canadians.[195]

Professor Colin Bennett also argued that broader enforcement powers are necessary "in light of these rapid changes in technology" and suggested that they "would create a greater certainty for consumers and indeed for business."[196] He went on to note that broader enforcement powers:

> … would establish a clearer jurisprudence where the rules and the investigation reports would have a clearer legal standing than they perhaps do at the moment. It's also a little odd that some of our provincial commissioners, such as in Quebec, British Columbia, and Alberta, do in fact have enforcement powers under their respective privacy laws, when the Privacy Commissioner does not.[197]

---

192 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1110 (Teresa Scassa, University of Ottawa).

193 Ibid., 1130 (Teresa Scassa, University of Ottawa).

194 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1135 (Tamir Israel, CIPPIC).

195 ETHI, *Evidence*, 1st Session, 41st Parliament, October 16, 2012, 1555 and 1615 (Jason Zushman, Merchant Law Group).

196 ETHI, *Evidence*, 1st Session, 41st Parliament, November 1, 2012, 1625 (Colin Bennett, University of Victoria).

197 Ibid.

The question of what is done in other jurisdictions, discussed in greater detail further below, was often raised as a matter of comparison. The Privacy Commissioner discussed this issue at length in her second appearance before the Committee, noting that Canada's federal law needs to provide enforcement powers comparable to those in other jurisdictions. That would be the best way to have the greatest impact on privacy protection and to improve Canadians' confidence in their online environment.[198]

> A law that dates back to a time before social networks and smart technologies were created cannot remain static. The ways in which personal information in this environment can be collected and used by many players makes a formal study of the effectiveness of our privacy framework even more pressing.[199]

In responding to concerns raised by those who feared that she would become "judge, jury and executioner," Commissioner Stoddart noted the experiences in other jurisdictions, including other Canadian provinces where commissioners have stronger enforcement powers, signalling that it had not prevented them from "doing education work, from working with chief privacy officers [or] from having collegial meetings with the private sector."[200]

> The reality of what we call multifunctional administrative organizations is a concept that is very well known in Canadian law — and, I believe, in British law and arguably in Australian law, to take laws that resemble our public law the most. Both my Australian and U.K. colleagues have different functions: they do education, they do arbitration, they do mediation, they do public outreach, and they also can either impose fines themselves — that's my U.K. colleague — or can go to the court and ask for fines of over $1 million Australian — that's my Australian colleague, so this is a model that's well known internationally.
>
> It's also well known here. Again, my B.C. and Alberta colleagues do education work with us. We've issued several guidance documents together with them. They have a public outreach office and so on, and they are tribunals. They make binding conclusions. Therefore, I don't know why all of a sudden it would be impossible for us, when it has been possible in Alberta, B.C., and Quebec for the last 15 years and it's the rule abroad.[201]

The evidence presented to the Committee demonstrates the competing views regarding the enforcement powers of the Privacy Commissioner. On the one hand, the current model facilitates the constant flow of information and good will between the private sector and the Privacy Commissioner, and has proven effective in ensuring that this relationship remains cordial and non-adversarial. On the other hand, much can and has been said regarding how the current model favours self-regulation and is not adequately

---

198 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1625 (Jennifer Stoddart, Privacy Commissioner).

199 Ibid.

200 Ibid., 1635 (Jennifer Stoddart, Privacy Commissioner).

201 Ibid.

prepared to ensure compliance when self-regulation fails. The Committee hopes that this valuable discussion will be of benefit to any future legislative review in this regard.

PRIVACY-ENHANCING MEASURES AND BEST PRACTICES

The Committee heard various important suggestions from witnesses regarding privacy-enhancing measures and best practices for the consideration of social media companies, regulators, policy makers and social media users in general.

While the Committee does not seek to make specific recommendations on legislative change in this Report, it does take note of the concerns raised regarding privacy-enhancing measures and encourages social media companies to continue to endeavour to promote privacy as a key principle in their operations and product design.

A. Privacy as the Default Setting

> *The architecture of every technology includes a number of design choices. Some of those design choices create default positions…The devil is in the defaults.*[202]
>
> *- Professor Ian Kerr, University of Ottawa*

Ann Cavoukian, Commissioner of the Office of the Information and Privacy Commissioner of Ontario, presented the concept of privacy by design to the Committee. According to Dr. Cavoukian:

> The essence of privacy by design is to embed privacy into the design of not only information technologies but accountable business practices, policies, and procedures in a proactive way, in an effort to prevent the privacy harm from arising as opposed to reactively offering a system of redress after the fact.[203]

She explained that privacy by design is "all about ensuring that the user has control of their data."[204] In a brief Dr. Cavoukian submitted to the Committee, she explained that privacy by design is based on seven foundational principles — it is proactive not reactive; privacy is a default setting; privacy is embedded into the design; full functionality is maintained; there is end-to-end security; there is visibility and transparency; and it is user-centric, maintaining respect for user privacy.[205]

These principles emphasize respect for user privacy and place privacy as a default condition, allowing the user, as data subject, to be assured of privacy — which, as it is

---

202 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1210 (Ian Kerr, University of Ottawa).

203 ETHI, *Evidence*, 1st Session, 41st Parliament, June 7, 2012, 1150 (Ann Cavoukian, Information and Privacy Commissioner of Ontario).

204 Ibid., 1145.

205 ETHI, *Brief submitted by the Information and Privacy Commissioner of Ontario*, "Privacy by Design: The Gold Standard," June 7, 2012.

embedded in the system, is both automatic and guaranteed.[206] In a paper Dr. Cavoukian published with Jeff Jonas, Chief Scientist at IBM Entity Analytics, and which she referenced in her testimony, it is argued that privacy protections are best achieved when privacy principles are introduced early; that is, during architecture planning, system design and operational procedures. As such, they are interwoven into business process and practices from the beginning and do not represent a later cost to companies.[207]

In its appearance before the Committee, Facebook acknowledged its implementation of a comprehensive privacy program that incorporates privacy by design. According to Mr. Robert Sherman, "this program involves a broad cross-functional privacy review of products at all stages of development and before they're released."[208]

Similarly, Mr. Alan Chapell of BlueKai noted that since its founding in 2007, his company has embraced privacy by design in recognition of the importance of incorporating privacy into [BlueKai's] products and services."[209] The result has been what he describes as a culture of protecting consumer privacy interests since day one.

Also highlighting the importance of the front-end privacy choices that companies make when designing their Web sites or programs, Professor Michael Geist of the University of Ottawa explained that

> […] the choices made by leading social media companies with respect to default privacy settings are the de facto privacy choice for millions of users. Given the increasing pressure to generate revenues, we can expect that those default choices are going to change in more aggressive ways to make use of user data.[210]

Tamir Israel of CIPPIC pointed out a recent consultation process on online privacy that noted that many online services are public by default and privacy by effort. As such:

> New users will rarely know how to configure the complex web of the often conflicting privacy control services that are offered when first signing on. Settings constantly shift and change, as new ones are introduced and old ones replaced, or when new features are added to existing services. Simply maintaining a constant level of privacy is a never-ending effort.[211]

While education and enhanced digital literacy may account for part of the solution to this issue, Professor Geist believes there needs to be continued work on these defaults

---

206 ETHI, *Evidence*, 1st Session, 41st Parliament, June 7, 2012, 1150 (Ann Cavoukian, Information and Privacy Commissioner of Ontario).

207 Ann Cavoukian and Jeff Jonas, "Privacy by Design in the Age of Big Data," June 8, 2012.

208 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1535 (Robert Sherman, Facebook).

209 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1530 (Alan Chapell, BlueKai).

210 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1110 (Michael Geist, University of Ottawa).

211 ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1115 (Tamir Israel, CIPPIC).

and noted the importance of initiatives to provide users with greater information and transparency and steps to ensure companies live by their privacy commitments.[212]

Nevertheless, while agreeing with these comments, his colleague, Professor Ian Kerr, suggested that ensuring privacy as the default would only be achieved through legislation.[213] In the context of e-commerce, social media and children's sites, Professor Kerr thinks that:

> … the way we would design defaults in those situations would still be focused on the fair practice principles for information collection, use, and disclosure. So the defaults would be dependent upon whether and to what extent information is being collected. I do think that we will be able to study and to think carefully to define defaults that would work across a general array of technologies, the purposes of which are information collection, use, and disclosure, which are the three buzz phrases attached to PIPEDA.[214]

B. Do Not Track

> *More realistic is to set in place some of the mechanisms, such as "do not track", to ensure that with the choices people would make, the reasonable person would likely say, "I'm quite comfortable providing you with a certain amount of information".*[215]
>
> *- Professor Michael Geist, University of Ottawa*

The Committee also heard interesting testimony on the do-not-track option for Internet browsing. "Do not track" is a feature available to users on certain Internet browsers and sites, which allows individuals to opt out of having their online behaviour tracked. It is modelled on the National Do Not Call List that gives consumers a choice about whether to receive telemarketing calls. In this vein, Mr. John Lawford of PIAC suggested to the Committee the creation of a "national do-not-track list."[216]

Mr. Warren Everson of the Canadian Chamber of Commerce explained that the do-not-track option is available in certain browsers, which prevent the lodging of cookies in a computer.[217] As he noted, since a whole series of tracking features are pre-approved because of computer cookies; do not track would serve to block these cookies from tracking an individual user; so the individual would then become a "fresh face" every time he or she accessed a Web site or service. Mr. Everson further explained that:

> Currently, when you identify yourself and you indicate your language of choice, and other things that you want the service to know, it will register that and lodge a cookie in your

---

212 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1110 (Michael Geist, University of Ottawa).

213 ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1210 (Ian Kerr, University of Ottawa).

214 Ibid., 1245.

215 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1140 (Michael Geist, University of Ottawa).

216 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1535 (John Lawford, PIAC).

217 ETHI, *Evidence*, 1st Session, 41st Parliament, June 5, 2012, 1220 (Warren Everson, Canadian Chamber of Commerce).

> computer so that every time it comes to you, it says, "Oh yes, this is algorithm such-and-such, and these are the preferences."[218]

Professor Michael Geist noted that many sites have been slow to adopt the do-not-track option. He cited the example of Facebook, which has thus far declined to adopt a do-not-track option.[219] He believes that, given the industry's failure to self-regulate, it would be appropriate for government to step in with stronger measures to ensure the user's choice is implemented and respected.[220]

Mr. Colin McKay, appearing on behalf of Google Canada, noted that his company has developed a function in its Web browser that includes something called "the incognito mode." This function, according to Mr. McKay, allows a user to browse the Internet in a stealth mode; that is, without being tracked or having Google or other companies be able to collect information on the searches or sites visited by the user.[221]

Similarly, Ms. Laura Pirri of Twitter noted that her company is "very proud to be one of the first major Internet services to implement 'do not track'."[222] According to Ms Pirri, Twitter implemented this feature "as a way for users to let us know, by setting 'do not track' in their browser, that they do not want this information collected."[223] Twitter's support for "do not track" is a development the company hopes will encourage its "wider adoption… as a privacy preference for users."[224]

Lastly, Mr. Alan Chapell noted that the BlueKai Registry allows users to see what preferences are being stored via the BlueKai cookies on their computer and opt out of having the company continue to use these cookies to track online behaviours. According to Mr. Chapell, having such an option "brings transparency to consumers" even though "relatively few consumers who visit the BlueKai registry actually opt out from further use of their preference data."[225] This suggests to him that "consumers who understand BlueKai's practices are generally less concerned by them."[226] It was not clear what level of sophistication or digital literacy is expected from users to use this or other available opt-out options.

---

218 Ibid.

219 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1115 (Michael Geist, University of Ottawa).

220 Ibid.

221 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1530 and 1630 (Colin McKay, Google Canada).

222 ETHI, *Evidence*, 1st Session, 41st Parliament, December 6, 2012, 1545 (Laura Pirri, Twitter).

223 Ibid.

224 Ibid.

225 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1530 (Alan Chapell, BlueKai).

226 Ibid.

C. Privacy Charter

Finally, the Committee heard a novel proposal from Professor Normand Landry of TELUQ, who recommended the creation of a "social media privacy charter." According to Professor Landry, such a charter could be drafted by privacy regulators in partnership with Canadian civil society, with the aim of creating a set of consistent standards "that would serve as a framework and would very clearly require the various players, regardless of their business model, to respect the standards across the country."[227] All social media that have activities in Canada would then be expected to comply with the charter.[228] He recommended that any such effort include non-judicial processes that would lead to increased accountability of social media companies in relation to the Canadian public. As he put it:

> We also need some non-judicial processes — and I stress the word "non-judicial"— to resolve conflicts between users and managers of social media sites. The lines of communication between the people who manage the sites and the people who use them must be improved. The lack of productive and non-judicial conflict management mechanisms create the tensions we are currently seeing.[229]

Professor Landry noted that Canadians are very concerned about their right to privacy.[230] He said that surveys show that Canadians are particularly concerned about the current trend in the digital world and that they have very little trust in the confidentiality policies of major social media sites.[231] He notes:

> The rules do not currently work adequately. What we are seeing when there are solutions that go before the courts is that a very heavy burden rests on the shoulders of a few individuals who have the skills, resources or desire to set a precedent. That's not how you manage a large-scale problem.[232]

EVIDENCE SPECIFIC TO CERTAIN PRIVATE COMPANIES

A. Google

Founded in 1998, Google is a publicly-traded company offering Internet-related products and services, including Web search and cloud computing services, and software and advertising technologies. Its social networking and identification service, Google+,

---

227 ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1605 (Normand Landry, TELUQ).

228 Ibid., 1540.

229 Ibid., 1605.

230 Ibid., 1615.

231 Ibid.

232 Ibid. A brief presented to the Committee at the moment of Mr Landry's testimony, which he has written with Professor Leslie Regan Shade of the University of Toronto ("Privacy and Social Media: Privacy Issues", November 15, 2012), contains the same recommendation.

was launched in June 2011 and already has 400 million registered users, 100 million of whom are active every month.[233]

Google has drawn considerable criticism for its privacy practices. In August 2012, it was fined $22.5 million by the United States Federal Trade Commission (FTC) for bypassing the privacy settings in Apple's Safari browser in order to track the browser's users and show them advertisements, thereby violating a prior agreement with the FTC.[234]

Furthermore, in September 2012, the European Union (EU) asked Google to amend its privacy policy, imposing a four-month ultimatum for it to make the recommended changes in order to "give people more detailed control over personal data."[235]

This demand, submitted by the French data protection commissioner on behalf of the 27 national data protection authorities, came in the wake of changes made by Google in March 2012.[236] It raises several concerns, including Google's practice of combining anonymous data from users' browsing histories across its services in order to better target advertising.[237]

Canada's Privacy Commissioner, Jennifer Stoddart, indicated that she could not endorse the recommendations made by the EU, because Canada had adopted a different approach in this matter.[238] However, the Commissioner shared the concerns of the data protection authorities "with respect to Google's policy of combining data, as well as its data retention and transparency practices generally."[239]

In Canada, Google has been the subject of a number of privacy-related investigations. On May 31, 2010, the OPC filed three complaints against Google, alleging it had reasonable cause to believe that the company had collected personal information

---

233 Statistics from September 2012, posted to the Google+ page of Vic Gundotra, Senior Vice-President, Engineering of Google.

234 Claire Cain Miller, "F.T.C. Fines Google $22.5 Million for Safari Privacy Violations," *The New York Times*, August 9, 2012.

235 Charles Arthur, "Google privacy policy slammed by EU data protection chiefs," *The Guardian*, October 16, 2012.

236 The changes made by Google consisted of combining separate "silos" of data from its various services, particularly its search engine, YouTube and Google Maps, into a single database in order to better target its advertising and content.

237 Dan Lalor, "EU gives Google four months to amend privacy policy," *Reuters*, October 16, 2012.

238 The Privacy Commissioner explained that her approach was "to examine the privacy implications of the changes in the policy, namely, the lack of specific information relating to data retention, the implications of linking personal information of account holders across services, and the implications for Android users. We did not conduct a formal investigation under the *Personal Information Protection and Electronic Documents Act* into these practices, but rather raised our concerns in an exchange of correspondence with the company." Office of the Privacy Commissioner, Letter to the French Data Protection Authority Regarding its Review of Google's Privacy Policy, *Announcement,* October 16, 2012.

239 Ibid. See also Rick Mitchell, "Article 29 Working Party Urges Google to Reconsider Privacy Policies by Year's End," *Bloomberg*, October 22, 2012.

from payload data found in unencrypted Canadian Wi-Fi networks.[240] In June 2011, the OPC published the findings of its investigation, declaring that Google had violated PIPEDA. It recommended that Google re-examine and improve the privacy training it provides to all its employees, that it adopt a privacy governance model, and that it delete the Canadian payload data collected, to the extent permitted under Canadian and U.S. laws. However, the OPC positively acknowledged the manner in which Google responded to this incident. Even though Google agreed to implement the OPC's recommendations, Commissioner Stoddart asked it to undergo an independent third-party audit of its privacy programs and to forward the results to the OPC no later than June 2012. Those audit findings have yet to be sent.

The Privacy Commissioner and Google also exchanged correspondence regarding various concerns raised by the company's changes to its privacy policies. In letters sent in February and March 2012,[241] the Commissioner noted that the policy which came into effect on March 1, 2012 is less specific about retention and disposal of personal information, and asked Google for a clearer explanation of its policies and practices in this area. After reviewing Google's explanations, the Commissioner expressed her concern regarding possible future changes that the company might make to its data retention and disposal policies.[242]

Mr. Colin McKay, of Google Canada, said that two-step verification for Google accounts provides all users with extra protection against unauthorized access to their information. According to Mr. McKay, Google guarantees the security of the users' information and strives to create user-focused controls and experiences that make it easy to make informed choices about what information to share with Google and others, and how to share it.[243]

He described Google Dashboard as "a tool that can help answer the question: what does Google know about me? Dashboard shows each user the information stored in their Google account. From one central location, you can easily change the settings for any Google services you may use, such as Blogger, Calendar, Docs, Gmail, Google+, and more."[244]

Mr. McKay also described the role of Google Takeout, an application which makes it easy to export data from many of Google's most popular services, to which new services

---

240 OPC, Report of Findings: Google Inc. WiFi Data Collection, *PIPEDA Report of Findings # 2011-001*, June 2011.

241 OPC, "Reply to Google regarding privacy policy changes," *Announcement*, March 8, 2012; OPC, "Letter from Google," *Announcement*, February 29, 2012; and OPC, "Letter to Google regarding privacy policy changes," February 24, 2012.

242 Ibid., Letter of March 8, 2012.

243 ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1530 and 1535 (Colin McKay, Google Canada).

244 Ibid., 1535.

are regularly added.[245] According to Mr. McKay, "We make it easy for users to leave and choose another service, which keeps us honest. Our users are safe and secure with us, but they also don't have to feel locked in."[246] Mr. McKay mentioned a tool called Ads Preferences Manager, which allows one to go and look at, correct or delete the "buckets" that Google has identified as applying to a user's particular interests.[247]

Mr. McKay also told the Committee that Google does not sell data to third parties.[248] He explained:

> … there's a substantial amount of what could be classified "transactional" or "network" data. This is about how traffic is being communicated through the network and how we see attacks on customers' accounts. That isn't necessarily user data but it is relevant to a user. We find that data very valuable, and that's what allows us to provide security services not only to the individual but to our whole company and the Internet as a whole.[249]

Mr. McKay considers Google to be very specific about the information it collects from users and why it is collecting it.[250] He says that Google is just as specific about the information it does not use in creating its data "buckets" and providing services to advertisers.[251]

> Some of the information that you would consider the most sensitive, whether it's political views or whether it's health issues, we don't consider at all. Then in other instances, when you're using our products, like Google+, it's very explicit to you why you're providing this information and why we're using it.[252]

When giving her evidence before the Committee, the Assistant Privacy Commissioner, Chantal Bernier, mentioned that the OPC's 2011 report on Google Wi-Fi gave Google a period of one year to provide the Office with a third-party audit.[253] According to Ms. Bernier, the Office wanted to be sure that Google was applying all of its recommendations.[254] Ms. Bernier said:

> That timeline was May 20. At the beginning of May we had a meeting with Google, and our request for a third party audit, which was clearly stated in our letter, did not even

---

245 Ibid., 1540.

246 Ibid.

247 Ibid., 1555.

248 Ibid., 1550.

249 Ibid., 1555.

250 Ibid., 1625.

251 Ibid.

252 Ibid.

253 OPC, "*Report of Findings: Google Inc. WiFi Data Collection*," *PIPEDA Report of Findings # 2011-001*, June 2011.

254 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1640 (Chantal Bernier, Assistant Privacy Commissioner).

> seem to be on their radar screen. They were rather apologetic, and said "Oh, my God, can we have an extension?" In July, they sent us the third party audit that in fact had been written for the FTC [U.S. Federal Trade Commission].[255]

B. Nexopia

Nexopia.com is a social networking site created in 2003 by a teenager. Based in Edmonton, it describes itself as Canada's largest networking sight specifically addressed to youth.[256] It has more than 1.7 million registered users, the great majority of whom (about 80%) live in Canada and nearly half in Alberta and British Columbia. According to Nexopia, its users are particularly interested in meeting people, expressing themselves and getting to know each other. To do so, they create profiles, interact in free-form blogs and forums, create photo galleries, and publish articles, works of art, music, poems and videos.[257]

It is company policy that young people who want to register on Nexopia be at least 13 years old.[258] Those self-reporting as being between 13 and 18 years of age make up more than 34% of the site's active users. The second largest demographic is those aged 19 to 22. According to one commentator, the site is "an online utopia for teens" because it "flies far under the parental radar."[259] As basic subscription is free of charge, the site generates revenue from advertising and offers users a "plus" service which gives them more options and extra privileges. Nexopia has confirmed that 7% of its users have signed up for this service.[260]

Mr. Kevin Bartus, Chief Executive Officer of Nexopia, told the Committee that Nexopia is one of the smaller sites that focus on a particular niche. The niche for Nexopia is young Canadians between the ages of 16 and 24.[261]

On January 18, 2010, representatives of the PIAC filed a complaint against Nexopia with the OPC.[262] The PIAC complaint concerned the privacy of young people in the online world. It maintained that Nexopia was not protecting the privacy of the users of its youth-oriented online networking site, in violation of its obligations under PIPEDA.[263]

On March 1, 2012, the OPC released its findings from the investigation into this complaint and, in an unusual step, named the company at issue. The OPC investigation

---

255 Ibid.

256 Nexopia.com, *About*.

257 Ibid.

258 Ibid.

259 Scaachi Koul, "Nexopia is an online utopia for teens," *Maclean's*, August 14, 2012.

260 Nexopia.com, *About*.

261 ETHI, *Evidence*, 1st Session, 41st Parliament, November 6, 2012, 1530 (Kevin Bartus, Nexopia).

262 PIAC, "PIAC Files Privacy Complaint Against Nexopia," January 19, 2010.

263 Ibid.

concluded that Nexopia was violating PIPEDA in the areas of disclosure of users' profiles to the public; default privacy settings; collection, use and disclosure of personal information collected at registration; sharing of personal information with advertisers and other third parties; and retention of personal information of non-users.[264] The OPC therefore addressed 24 recommendations to Nexopia so that it could comply with the various provisions of PIPEDA. Nexopia agreed to implement 20 recommendations in the prescribed timeframes, including to provide the OPC with periodic progress reports, documentation and proof that it has made the requested changes to its site. To date, Nexopia has yet to publish a report demonstrating that it is following the OPC's recommendations.[265]

The four other recommendations concerned the retention of users' personal information. At the time of publication of the findings, Nexopia had refused to implement the OPC's recommendations in this regard and had not proposed any alternative measures. On April 13, 2012, the Privacy Commissioner filed an application for judicial review with the Federal Court regarding Nexopia.com, with the aim of compelling the company to implement its conclusions concerning the archiving of personal information of users.[266]

In September 2012, Nexopia was sold to a new group of investors, headed by Mr. Bartus. In his evidence, Mr. Bartus explained that he had met with the OPC in the course of the buyout process. Although he was unable to speak of the decisions made by the previous ownership group, he told the Committee that Nexopia's new administration intends to act upon all of the OPC's recommendations.

C. Facebook

Facebook is a social media company founded in 2004. It made its initial public offering on May 18, 2012.[267] At the end of September 2012, Facebook had 4,331 employees.[268] According to its Web site, in the fall of 2012, Facebook had one billion active users, an average of 584 million active users per day, and 604 million active users of Facebook mobile products per month.[269]

In 2011, the OPC conducted investigations into privacy-related complaints against Facebook, mainly as a result of new features added by the company to its social

---

264 OPC, PIPEDA Report of Findings #2012-001, "Report of Findings: Social networking site for youth breached Canadian privacy law."

265 ETHI, *Evidence*, 1st Session, 41st Parliament, October 18, 2012, 1615 (John Lawford, PIAC).

266 *Privacy Commissioner of Canada* v. *Nexopia.com Inc.*, Federal Court, File No. T-764-12.

267 Facebook, Newsroom, *Facebook Announces Pricing of Initial Public Offering*.

268 Facebook, Newsroom, Key facts.

269 Ibid.

networking platform.[270] The OPC report suggests that Facebook seemed to ascribe more importance to privacy than in the past.

However, the OPC said it was disappointed that the company had not provided for protective measures in its new "friend suggestion" features at the design stage.[271] One complaint about the friend suggestion features mentioned that Facebook might have inappropriate access to the electronic address books of certain individuals.[272] The company agreed to make changes to the features, such as removing the friend suggestion from initial invitations and sending it only in subsequent reminders, and allowing certain non-users to opt out of receiving Facebook messages.[273]

Another Facebook feature that came in for complaint was the social plug-ins, which allow users to see content drawn from their user profile on third-party Web sites.[274] The OPC investigation found that no personal information was shared by Facebook with third-party Web sites, but did suggest that Facebook make improvements in educating the public and its users on how to use this feature and its privacy consequences.[275]

A third complaint alleged that Facebook collected more personal information than necessary in verifying its users' identity.[276] The OPC considered that asking users to upload mobile phone numbers or government-issued ID numbers in order to identify themselves did not contravene PIPEDA. The OPC found that Facebook's procedure for filing a privacy complaint was accessible and easy to use.[277]

On November 21, 2012, Facebook made changes to its Data Use Policy, which explains how the company collects and uses data when people use Facebook, and to its Statement of Rights and Responsibilities, which explains the conditions governing the use of its services.[278] Among the changes announced, Facebook will now combine user data with that of the recently acquired Instagram photo-sharing service, and will loosen restrictions on emails between members of the social network. In addition, Facebook is proposing to scrap the process permitting its users to vote on changes to its policies and

---

270 OPC, PIPEDA Report of Findings #2012-002, "Report of Findings: Facebook didn't get non-members' consent to use email addresses to suggest friends, investigation finds."

271 Ibid.

272 OPC, Backgrounder, "Facebook Investigations Finding Details.".

273 Ibid.

274 OPC, PIPEDA Report of Findings #2011-006, "Report of Findings: No evidence Facebook shares personal information with other sites via social plug-ins, investigation finds."

275 Ibid.

276 OPC, PIPEDA Report of Findings #2011-005,"Facebook authentication practices reasonable, investigation finds."

277 Ibid.

278 Alexei Oreskovic, "Privacy in spotlight again with Facebook's latest changes," *Globe and Mail*, November 22, 2012.

terms of services, and replace it with other channels of engagement, including a function for submitting privacy-related questions to the company's chief privacy officer.[279]

Mr. Robert Sherman, the Facebook representative who appeared before the Committee, said that the company is committed to providing privacy tools that enable people to control the information they share and the connections they make through its platform.[280] According to Mr. Sherman, the trust of its users is fundamentally important to Facebook.[281]

Mr. Sherman commented that "Canada, with 18 million monthly active users, is among the most engaged Facebook populations in the world. Four of five Internet users in Canada are on Facebook."[282] Mr. Sherman explained the approach that Facebook takes with its privacy policy as being "layered," in that it summarizes its practices on the front page and then allows users to click through the policy for more details.[283]

> Content is organized by topic, which lets people find exactly what they're looking for quickly and easily. People who want to read the entire policy on one page can do that as well. If they have questions about specific issues, they can find an answer by conducting a search within our help centre.[284]

Mr. Sherman also explained that the "download your information" tool allows people to download an archive of information associated with a Facebook account, including photos, posts and messages. He said that this tool allows people to have a copy of their information if they want to use it elsewhere. He also explained that Facebook offers an application "dashboard" so that users can review the specific kinds of information that each application can access on Facebook and make choices about what access applications will have to their Facebook accounts going forward.[285]

Mr. Sherman said that the main Facebook business model is to offer the service free of charge to anyone who wants to use it, in exchange for which Facebook shows advertising on its site. One page called "Ads on Facebook" further explains how this works.[286] He added that:

---

279 Facebook, "Proposed Updates to our Governing Documents."

280 ETHI, *Evidence*, 1st Session, 41st Parliament, November 27, 2012, 1530 (Robert Sherman, Facebook).

281 Ibid.

282 Ibid.

283 Ibid.

284 Ibid.

285 Ibid., 1535.

286 Ibid., 1550.

> In general, when you post information on Facebook, for example, information about your interests, you like a page that is relating to a particular topic, that's information we might use to decide which ads to show you.[287]

Mr. Sherman explained that advertisers will ask Facebook to show certain ads to people who are interested in a particular topic. Facebook then shows the advertising to the users, without providing the advertisers with personal information on the people who are viewing the ad. Facebook instead provides general information on the number of people who have seen a certain advertisement.[288]

Mr. Sherman said that Facebook tries to operate its service in a way that is consistent globally, so that everyone on Facebook has the same experience.[289] The decisions on privacy that are made by Facebook are made in a way that applies to all users in all countries where the company has relationships.[290]

> In general, when we receive feedback from [a] regulator, we take that feedback seriously. There may be instances where we make a decision that certain features will work differently in some jurisdictions, but we prefer to avoid that where possible and maintain a consistent experience for everybody.[291]

Mr. Sherman regards Facebook's relationship with the OPC as being very productive and positive. He feels that Facebook is able to discuss with the Commissioner the decisions that it makes about privacy and get her feedback. This helps Facebook make a better product and better protect the privacy of Canadians. Mr. Sherman considers Facebook a good example of the fact that the existing regime works well.[292]

> We've had consultations with the Privacy Commissioner on an ongoing basis and we've made changes to our product, in fact, in response to her feedback. We've made those judgments based on the fact that the Privacy Commissioner has suggested ways that we can better protect the privacy of Canadians.[293]

D. Twitter

Twitter is an online social networking and microblogging network which allows users to send and receive messages containing up to 140 characters, known as "tweets." The San Francisco–based company was founded in 2006, and has since seen strong and steady growth. In 2012, Twitter had more than 500 million users, producing more than

---

287 Ibid.

288 Ibid.

289 Ibid., 1555.

290 Ibid.

291 Ibid.

292 Ibid., 1610.

293 Ibid.

340 million tweets every day. In addition, over 1.6 billion searches are made every day.[294] With 11 million subscribers, Canada ranks eighth among countries with the most Twitter users.[295]

Tweets can be public or private. Persons without a Twitter account can read public tweets, while Twitter subscribers can post both public and private messages, and send private messages to other subscribers. In its privacy policy, Twitter says that it collects personal information about its users and relays it to third parties offering client services and applications.[296] Some of this information, including name and username, is publicly posted. Although a good many of its services do not require it, Twitter utilizes "cookie" technology "to collect additional Web site usage data and to improve [its] Services."[297]

According to its privacy policy, Twitter does not disclose "personal private information" without its users' consent, but reserves the right to share or disclose "your non-private, aggregated or otherwise non-personal information, such as your public user profile information, public Tweets, the people you follow or that follow you, or the number of users who clicked on a particular link" without first requesting users' consent.[298]

Ms. Laura Pirri, the Twitter representative who appeared before the Committee, said that Twitter has certain company values, one of which is to defend and respect the user's voice, and that includes respect for the user's personal information.[299] She says:

> Our service doesn't require a whole lot of personal information in order to use it. As I mentioned, you can use the service without actually having an account. If you have an account, you don't need to provide a real name or a street address. You don't need to provide age. You don't need to provide gender.[300]

Ms. Pirri said that, when designing or launching a new product feature, Twitter does so with privacy in mind.[301] "For example, one of our privacy philosophies is to provide contextual notices or disclosures to users in the product at the time that they provide us with information, in order to supplement our privacy policies."[302]

---

294 Lauren Dugan, "Unofficial Reports Suggest Twitter Surpassed 500M Registered Users In June," *All Twitter*, July 31, 2012.

295 Shea Bennett, "The Top 20 Countries and Cities on Twitter," *All Twitter*, August 13, 2012.

296 Twitter, *Twitter Privacy Policy*.

297 Ibid.

298 Ibid.

299 ETHI, *Evidence*, 1st Session, 41st Parliament, December 6, 2012, 1535 (Laura Pirri, Twitter).

300 Ibid.

301 Ibid., 1540 (Laura Pirri, Twitter).

302 Ibid.

Ms. Pirri commented that Twitter contacted the OPC when it launched its do-not-track feature, to let the Commissioner know what its plans were.[303]

Ms. Pirri mentioned that law-enforcement guidelines are available on the Twitter site. She explained that, to protect the privacy of its subscribers, Twitter requires that a request for personal information about a user follow the normal legal process, i.e. a court order or subpoena. She added that Twitter is also committed to transparency when it comes to requests from law enforcement, and that it always notifies users when someone has requested their information in this way. This is the process that Twitter asks parties to follow when they are looking to receive information.[304]

On the subject of anonymity on Twitter, Ms. Pirri had this to say:

> It's part of our goal to be the platform to represent the stories and the voices of so many different users. We think it's important to allow those voices to be heard and for them to speak without providing identifying information that may have consequences where they may live.[305]

Ms. Pirri commented that many of the privacy principles being advocated in the United States do not just concern notices, disclosure, security, information access, and the right to delete or modify information:[306]

> Our privacy policy attempts to disclose to users all the different controls and tools that we give them around the information we collect, how it can be modified, and how it can be deleted. We give users those kinds of controls and that kind of access to the information we're providing […].[307]

Ms. Pirri stressed the importance of being clear with users about why the company collects the information and how it gets used, and of giving them the ability to delete information in a way that is more piecemeal than simply deleting their whole account.[308]

> We try to do things that are a little more fine-tuned, such as how you can delete the location from your tweet without actually deleting the tweet itself.[309]

E. Acxiom

Founded in 1969, Acxiom Corporation is a global marketing technology and services company with offices in the United States, Europe, Asia and South America.[310]

---

303 Ibid., 1545.

304 Ibid.

305 Ibid., 1600.

306 Ibid., 1610.

307 Ibid.

308 Ibid., 1620.

309 Ibid.

310 Acxiom, About.

Its services enable marketers to manage target audiences, personalize consumer experiences and create customer relationships. Its online and offline activities include collection and analysis of consumer data, databases, data integration and consulting solutions for personalized multichannel marketing strategies.[311]

In 2005, Acxiom took over Digital Impact and set up Acxiom Digital, allowing it to integrate its digital and online services, thereby creating one of the world's largest commercial data banks on consumers. Recent analyses indicate that Acxiom servers process more than 50 trillion data "transactions" per year. The company's executives have said that their data bank contains information on some 500 million active consumers worldwide, with about 1,500 data points per person.[312] The annual value of Acxiom is estimated at $1.15 billion, which is more than 12% of the $11 billion represented by annual sales in direct marketing services.[313]

Ms. Jennifer Barrett Glasgow, the Acxiom representative who appeared before the Committee, said that "… we as a company pride ourselves on following all the legal obligations in each country where we source data. I also want to point out that when consumer data is properly used it can make significant contributions to the economy, and the growth and stability of an economy."[314]

Ms. Barrett Glasgow explained that elsewhere in the world Acxiom offers a wider range of products and services, but in Canada it offers only business and consumer telephone directory products, amounting to just under $1.5 million in annual revenue. She said that Acxiom does business in Canada without having a physical presence there, preferring to provide support from its headquarters in Little Rock, Arkansas, in the United States.[315]

Ms. Barrett Glasgow explained the nature of the company's Canadian activities:

> Acxiom's Canadian business and consumer directories are licensed to companies and non-profit organizations for their internal use as an automated and inexpensive form of directory assistance or for direct mail and telemarketing purposes. Our directories are also licensed to companies that host directory search engines on the Internet for both consumer and commercial use. In these instances Acxiom's listings may be merged with telephone listings from other sources by our client.[316]

---

311 Ibid.

312 Natasha Singer, "Acxiom, The Quiet Giant of Consumer Database Marketing," *The New York Times*, June 16, 2012.

313 Ibid.

314 ETHI, *Evidence*, 1st Session, 41st Parliament, December 6, 2012, 1635 (Jennifer Barrett Glasgow, Acxiom).

315 Ibid.

316 Ibid.

According to Ms. Barrett Glasgow, Acxiom does not sell data to individuals, but only to qualified businesses.[317] Screening is done "to make sure that they are a legitimate business and that they have a legitimate name for the data they're specifically requesting."[318]

Ms. Barrett Glasgow explained that "In the U.S. we have products that identify heavy users of social media and what types of social media, such as Twitter or Facebook, an individual might use, but we do not offer those kinds of products in Canada."[319] "In Canada," she continued, "we match name and address and telephone number, because these are telephone directory listings and we have a phone number for every record."[320]

Ms. Barrett Glasgow explained that Acxiom could deliver data to its clients in two ways.[321] The first is to buy from Acxiom a list drawn up according to certain criteria specified by the client.[322] The second is called "list enhancement," where the company's database is matched with information provided by the client, which is thereby complemented and completed.[323]

F. BlueKai

Founded in 2008, BlueKai is one of the leading online data aggregation companies. It describes itself as the most interconnected media-independent data management platform, data exchange and analytics system in the industry.[324] It is a private corporation headquartered in Cupertino, California, with offices in New York and Seattle.[325]

BlueKai's software enables its customers to sort consumers into some 30,000 market segments, such as "light spenders" or "midscale thrift spenders."[326] The categorization of Internet users makes real-time bidding easier for advertising that is targeting a particular user category. The company's extensive partnership network allows it to follow more than 160 million people every month who are looking to buy things like cars, financial services, retail and consumer goods or travel accommodations. By sorting users into categories based on their interests and purchasing power, BlueKai's software

---

317 Ibid., 1645.

318 Ibid.

319 Ibid., 1655.

320 Ibid.

321 Ibid., 1705.

322 Ibid.

323 Ibid.

324 BlueKai, About Us.

325 Ibid.

326 Jeffrey Rosen, "Who Do Online Advertisers Think You Are?" *The New York Times Magazine*, November 30, 2012.

helps advertisers determine to what extent each person is worth following, and at what price. Although BlueKai itself does not collect or sort data about consumers, it provides the software that enables Web sites to track users and put them into market segments.[327]

According to the company's CEO, Mr. Omar Tawakol, BlueKai and other companies in data-driven marketing serve two purposes: they ensure that consumers are offered an accurate set of content and opportunities that may be of interest to them, and they maintain efficiency for businesses that want to reach out to those consumers. The by-product of this relationship is simply a free Internet.[328]

Mr. Alan Chapell, the representative of BlueKai who appeared before the Committee, described the company's mission as being "to build the world's first complete enterprise platform for data-driven marketing with the utmost attention and diligence to ensuring consumer privacy."[329] He described what his company does as follows:

> We offer a data management platform that enables advertisers to collect, store, and utilize anonymous consumer preference data. [330]

Mr. Chapell explained that BlueKai's platform enables marketing businesses to use pseudonymous data for online behavioural advertising and analytics purposes.[331] This platform:

> … allows businesses to create target audiences based on a combination of their own data and third party data in order to reach their target audiences across third party advertising networks and exchanges. The platform also helps those businesses to measure with accuracy which campaigns performed in order to refine media buys and advertise creatively over time.[332]

Giving the example of Ghostery,[333] Mr. Chapell noted that more and more Internet users are downloading their own transparency tools.[334] He explained how these tools work:

> They're browser-based plug-ins that tell an Internet user which cookies are being dropped by which companies on the websites that they visit. Certainly, users can be provided with that mechanism with some additional transparency. We're seeing more and more Internet users utilize those exact types of tools.[335]

---

327 Ibid.

328 Omar Tawakol, "Statement Correcting Recent NY Times' Story Assertions," December 1, 2012.

329 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1530 (Alan Chapell, BlueKai).

330 Ibid.

331 Ibid.

332 Ibid.

333 Ghostery, About.

334 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1600 (Alan Chapell, BlueKai).

335 Ibid.

Mr. Chapell noted the growing presence in the United States of forward-looking little icons on digital advertisements that are being targeted with online behavioural advertising data.[336]

> From the user's perspective, looking at that little dot on the advertisement may not let that person know exactly which company is targeting them, but it does provide a mechanism for them to understand a little bit more about the practice of online behavioural advertising and then let them go to the opt-out page.[337]

INTERNATIONAL EXAMPLES

As Commissioner Stoddart reminded the Committee,[338] the privacy laws in different countries are not all that different, as they are all based on the fair information principles adopted by the Organisation for Economic Co-operation and Development (OECD) in 1980. She said that Canada chose to follow the European standard for privacy law, and therefore our system for transferring data is adequate.[339] Commissioner Stoddart noted that:

> More recently there have been very positive developments in the United States, led by the Department of Commerce and the Federal Trade Commission, to make the privacy standards in the United States more explicit. There is very little difference now between the various countries.
>
> Secondly, I'd like to add that privacy enforcement authorities are increasingly working together.[340]

Ms. Janet Goulding, from Industry Canada, mentioned that the OECD was currently reviewing its privacy guidelines, which were agreed upon internationally and which influenced the development of the Standards Council of Canada's model privacy code, upon which PIPEDA is based.[341]

A. The European Union and Enforcement Powers

On January 25, 2012, the European Commission proposed a comprehensive reform of the data protection rules adopted by the European Union in 1995 in order to strengthen online privacy rights and help boost Europe's digital economy.[342] At present, the 27 member states of the EU are implementing the 1995 rules differently, resulting in

---

336 Ibid.

337 Ibid.

338 ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1210 (Jennifer Stoddart, Privacy Commissioner of Canada).

339 Ibid.

340 Ibid.

341 Ibid., 1225 (Janet Goulding, Industry Canada).

342 European Commission, "Press Release: Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses," January 25, 2012.

divergences in enforcement. The Commission is seeking to provide the EU with a single set of rules for all the member states.

In addition to standardizing the rules, the new system is aiming to improve data protection. For example, businesses have to obtain the explicit consent of persons concerned before using and processing data about them. They cannot collect more information than is strictly necessary, and can retain it only as long as it is needed. The new rules also create a "right to be forgotten," which will permit citizens to delete their data or request its deletion if there is no legitimate reason to retain it.[343]

The new rules will apply to all member states and any company doing business with a member state, even if its head office is outside the EU. The Commission's proposals have been forwarded to the European Parliament and the member states for discussion purposes. They will come into effect two years after their adoption, which is expected in 2016.[344]

With regard to the European situation, professor Valerie Steeves of the University of Ottawa told the Committee:

> I would suggest that the jurisdictions that have approached these issues from a broader perspective and come up with solutions that better capture these broader human rights interests are places in Europe, for example, which have a human rights approach to privacy and where there are strong human rights protections for privacy, for the inviolability of the personality.[345]

Commissioner Stoddart noted that the United Kingdom commissioner and a number of international data protection authorities have the power to impose fines.[346]

> In the United Kingdom, my counterparts have stronger enforcement powers, but that has not precluded an ombudsman approach. Fines are issued where a softer touch has failed. Our counterparts tell us that businesses that invest in adopting good privacy practices from the start feel it is only fair to impose a financial burden on those who do not, in order to even the playing field.[347]

Commissioner Stoddart drew a parallel in this regard with the commissioners in Quebec, Alberta and British Columbia, who have order-making powers and jurisdiction over the private sector. As she went on to explain:

> They also have other duties — prescribed by law — that enable them to perform multiple roles, such as educator, adjudicator, enforcer, advocate, and so on. I have noted that witnesses before this committee had only good things to say about their relationship with

---

343 Ibid.

344 Ibid.

345 ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1150 (Valerie Steeves, University of Ottawa).

346 ETHI, *Evidence*, 1st Session, 41st Parliament, December 11, 2012, 1620 (Jennifer Stoddart, Privacy Commissioner).

347 Ibid.

> the commissioners. Witnesses have said that the Canadian model was the envy of many countries around the world.[348]

Commissioner Stoddart reminded the Committee that when PIPEDA was passed, the objective was to meet European Union standards. She added that, to date, 80 countries in the world have adopted the European model, and about 15 countries outside the EU explicitly meet the European standards.[349] Canada was the first one to do so. In her opinion:

> We should continue to look at the European model and have these different levels of fines that start at perhaps a few thousand euros and go up to something major. That's because you may be dealing with a small, local family business that just doesn't want to pay attention, or you may be dealing with a big multinational player.[350]

Commissioner Stoddart provided the Committee with a document entitled "Enforcement Powers under International Privacy Laws," which compares powers to enforce privacy laws in a number of countries. This document can be found in Appendix B.

B. The United States of America and the Federal Trade Commission

In the United States, where the general rule is to let companies regulate themselves, there is no particular framework governing the use of personal data. The Federal Trade Commission (FTC)[351] intervenes only when a company is obviously negligent in regulating itself. The FTC has wide-ranging powers to investigate unfair and deceptive business practices, powers it has invoked to render decisions concerning Facebook[352] and Google.[353]

In March 2012, the FTC published a report in which it asks Congress on the one hand to consider enacting baseline privacy legislation to protect consumers, and industry on the other to implement a privacy framework, inviting businesses to take individual initiatives and adopt rigorous, enforceable self-regulatory measures.[354]

With regard to the proposed privacy framework, the FTC has made recommendations in three key sectors. First, it recommends that companies adopt an approach that builds in respect for privacy from the design stage, making privacy a fundamental criterion of their business practices. Second, companies should offer

---

348 Ibid.

349 Ibid., 1645.

350 Ibid.

351 Federal Trade Commission (FTC), About the Federal Trade Commission.

352 FTC, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises ," November 29, 2011.

353 FTC, "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network," March 30, 2012.

354 FTC, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012.

consumers simpler and better structured choices concerning their information practices. Third, companies should adopt measures to make those practices more transparent. More specifically, companies that do not do business with consumers directly, such as data brokers, should offer consumers reasonable access to the data they have about them. The report encourages individual businesses and self-regulating organizations to accelerate adoption of the principles contained in the privacy framework.[355]

The FTC report also recommends continued implementation of a feature which allows consumers to opt out of collection by advertisers and third parties of information about their Internet activities. The report mentions the important initiatives taken by a number of companies in response to the Commission's do-not-track recommendation: Microsoft, Mozilla, Apple, Google, the online advertising industry through the Digital Advertising Alliance, and the World Wide Web Consortium, an international standard-setting organization.[356] The FTC appeared before the U.S. Senate Committee on Commerce, Science and Transportation to discuss its report.[357]

THE COMMITTEE'S TRIP TO WASHINGTON, D.C.

Six members of the Committee went to Washington from October 3 to 5, 2012 to meet with different stakeholders and learn more about the issue of privacy and social media in the United States.

A. U.S. Legal System

1. Definition of Privacy

Chuck Curran, Executive Director at the Center for Data Innovation,[358] presented social media as a form of digital citizenship.[359] Professor Howard Beales, of the Department of Strategic Management and Public Policy at George Washington University, answered the question of how to define privacy by relating the concept to the following six principles: individual control over personal information; fair information handling processes; the right to personal solitude, or the right to withdraw; the right to security of the person; the right to liberty of the person; and the right to dignity.[360]

---

355 Ibid.

356 Ibid.

357 For the FTC's testimony, see: FTC, Testimony.

358 The Center for Data Innovation is a Washington D.C.-based non-profit company with the objective of advancing data innovation by showcasing its societal economic benefits. For information on Mr. Curran, see: Security, Privacy and the Law, Chuck Curran.

358 Chuck Curran, Center for Data Innovation, October 4, 2012.

359 Howard Beales, George Washington University, October 4, 2012.

2. Legislative Framework

Eric Miller, Senior Policy Advisor for Industry Canada at the Embassy of Canada, reminded Committee members that the U.S. legal regime regarding privacy protection dates from the 1980s and that its rules and standards do not address issues such as geolocation and mobile devices. He noted that the Obama Administration had tried to update the regime by issuing a "Privacy Bill of Rights" in the form of a document entitled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*.[361] According to Mr. Miller, this document shows just how much a new privacy approach is needed in light of the activities of Internet giants such as Google and Facebook. According to Mr. Miller, the FTC is currently acting in its regulatory authority in the absence of a comprehensive legal privacy regime.[362]

The FTC has recommended that Congress enact baseline privacy legislation, but has not proposed specific language to do so.[363] FTC representatives pointed out that 47 states currently have legislation on breach notifications.[364]

Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC), reminded the Committee that the U.S. does not have comprehensive privacy legislation similar to PIPEDA; the main U.S. legislative tool is section 5 of the *Federal Trade Commission Act.*[365] Christopher Soghoian, Principal Technologist and Senior Policy Analyst with the American Civil Liberties Union's (ACLU) Speech, Privacy and Technology Project,[366] noted that the word "privacy" doesn't appear in the FTC Act and that it would be beneficial to specifically give privacy authority to the FTC.[367]

Taking a different perspective, Mr. Curran believes that the gaps to be filled should be identified before the adoption of a privacy law can be considered. He believes that existing laws are too easily discarded, and he noted that non-statutory tools also exist. In Mr. Curran's view, we must start by asking ourselves if there is a legal remedy for the reprehensible actions in question, and what the basis is for the specific harm. Mr. Curran considers that lawmakers must be precise in providing a remedy.[368]

---

361 See: White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy".

362 Eric T. Miller, Senior Policy Advisor, Industry Canada, Embassy of Canada, October 3, 2012.

363 FTC, Markus B. Heyder, Christopher N. Olsen, Mark Eich, October 4, 2012.

364 Ibid.

365 Marc Rotenberg, EPIC, October 4, 2012. Cornell University Law School, Legal Information Institute, 15 USC § 45.

366 The ACLU is a non-partisan, non-profit organization whose mission is to defend the rights and liberties of all individuals. The ACLU engages in court actions, lobbying and community education activities.

367 Christopher Soghoian, ACLU, October 4, 2012.

367 Chuck Curran, Center for Data Innovation, October 4, 2012.

3. Federal Trade Commission

The FTC's primary authority comes from section 5 of the *Federal Trade Commission Act*. Among other things, this provision declares to be illegal any "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce".[369] Under this provision, the FTC is also "empowered and directed to prevent persons, partnerships, or corporations, with certain exceptions, from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce".[370]

According to FTC representatives, this provision imposes the need for proof of a substantial injury and includes a cost-benefit test.[371] They explained that companies must take reasonable security measures to meet this obligation. In the context of social media, in the Facebook and Google cases, the FTC recognized that consumers had a reasonable expectation under this provision that their information would not be shared.[372]

Under section 5 of the *Federal Trade Commission Act*, the FTC cannot levy fines, but it can impose penalties by order: a civil penalty amounts to $16,000 for each violation. FTC representatives also stressed the importance of the role of their enforcement branch in this process.[373]

FTC representatives reminded Committee members that the FTC has no rulemaking or legislative authority. They explained that the report published by the FTC in March 2012 lays out what it considers to be best practices. In publishing this report, the FTC hoped to give consumers the opportunity to make appropriate choices. The do-not-track option and the concept of privacy by design are in keeping with that idea.[374]

According to FTC representatives, one of the 2012 report's primary messages is this: based on the technology available today, one should ensure that data is protected. They emphasized that this message is intentionally vague to facilitate adaptability.[375]

One of the features of the U.S. regime is that the FTC can make public its investigations of certain companies and any settlements negotiated with those companies following such investigations. According to Christopher Soghoian, only investigations

369 15 USC § 45(a)(1).

370 15 USC § 45(a)(2).

371 FTC, Markus B. Heyder, Christopher N. Olsen, Mark Eich, October 4, 2012.

372 Ibid.

373 Ibid.

374 Ibid.

375 Ibid.

made public by the FTC ended in settlement.[376] FTC representatives expressed the hope that these settlements will serve as examples for other companies.[377]

FTC representatives reminded Committee members that the FTC's various investigations into Facebook, Google and MySpace led to settlements.[378] Regarding the Facebook case, they explained that the FTC had alleged that Facebook violated section 5 of the *Federal Trade Commission Act*. The FTC negotiated a consent order requiring Facebook to obtain express consent from users, to set up a privacy program assessing risk with a privacy specialist, and to have that privacy program audited.

In light of an agreement between Facebook and the FTC in August 2012, Eric Miller speculated that Facebook would henceforth try to monetize all the data it handles.[379] Similarly, Marc Rotenberg told the Committee that Facebook knows perfectly well that the only way for it to make money is through its users' information.[380] Representatives of the National Network to End Domestic Violence (NNEDV),[381] meanwhile, expect Facebook to look for ways to make even more money with its data now that it has become a public company.[382]

In Mr. Rotenberg's view, moreover, recent settlements show that Facebook has not changed its behaviour. He pointed to facial recognition as one of the most important issues to be dealt with and reminded the Committee of the issues raised by Facebook's association with Datalogix.[383]

Mr. Rotenberg noted that when Facebook changed its privacy setting features in 2009, the FTC agreed with EPIC's contention that this was an unfair and deceptive practice under section 5 of the FTC Act, and the subsequent settlement between Facebook and the FTC flowed from the FTC's authority to investigate such practices.[384]

---

376 Christopher Soghoian, ACLU, October 4, 2012.

377 FTC, Markus B. Heyder, Christopher N. Olsen, Mark Eich, October 4, 2012.

378 Ibid.

379 Eric T. Miller, Industry Canada, Embassy of Canada, October 3, 2012.

380 Marc Rotenberg, EPIC, October 4, 2012.

381 NNEDV serves as the leading voice for victims of domestic violence and their advocates. This umbrella organization provides support and training for special projects and collaborates with the U.S. Department of Justice. NNEDV takes a particular interest in technology issues.

382 Cindy Southworth and Cynthia Fraser, NNEDV, October 4, 2012.

383 Marc Rotenberg, EPIC, October 4, 2012. Facebook signed an agreement with Datalogix, a data management company, to provide statistics to advertisers in order to reassure them of the effectiveness of their Facebook advertising campaigns. See: Alexei Oreskovic, Reuters, "Facebook's new pitch to brand advertisers: forget about clicks," October 1, 2012.

384 Marc Rotenberg, EPIC, October 4, 2012.

In short, Mr. Rotenberg asserted that the role of the FTC has become critical, since it has taken responsibility for consumer protection. However, the moment the FTC stops enforcing its orders, he noted, companies resume their earlier practices.[385]

B. Balancing Innovation and Regulation

Jim Harper, Director of Information Policy Studies with the Cato Institute,[386] noted that important changes in technology have affected social networks; he cited as examples the growing use of sensors, which transform an analog signal into a digital signal, as well as the storage, processing and transfer of information.[387] The impact of technological change on social media leads us to consider another issue: balancing technological innovation and privacy regulation.

According to Eric Miller of the Canadian Embassy, the current debate in the U.S. on the roles of the government and the market is based on the idea that robust privacy measures will result in new technologies not being available to consumers. On the subject of whether or not it is more profitable for companies to have a predictable legal privacy regime, he suggested exploring the creation of an international standard and analyzing the impact of this system on cloud computing and employment.[388]

Michael Mandel, Chief Economic Strategist with the Progressive Policy Institute (PPI),[389] believes the central issue is how to strike a balance between privacy and economic growth. His main argument is that privacy regulation and economic growth together yield better results than privacy regulation alone.[390]

The real issue, according to Mr. Mandel, is that there are economic problems in developed countries, and data-driven industries remain the most dynamic. The legislator should not try to guess in advance what the regulations should be: it would get in the way of growth. Accordingly, Mr. Mandel believes that the narrower the regulations, the better. The difficulty is that by the time the regulations come into effect, technology has moved on, and there is the possibility that the government could stamp on innovation accidentally. According to Mr. Mandel, the success of data-driven industries is precisely due to the fact that they were not regulated in a decade that saw regulation and a slowing down of the economy.[391]

---

385 Ibid.

386 The Cato Institute is an independent non-partisan public policy research organization dedicated to the principles of individual liberty, limited government, free markets and peace.

387 Jim Harper, Cato Institute, October 4, 2012.

388 Eric T. Miller, Industry Canada, Embassy of Canada, October 3, 2012.

389 The PPI is an independent non-profit organization that promotes economic growth, national security and performance-based government.

390 Michael Mandel, PPI, October 3, 2012.

391 Ibid.

Ross Schulman, Public Policy and Regulatory Counsel with the Computer and Communication Industry Association (CCIA),[392] believes that regulation is not a bad thing in itself, as long as it allows for sound competition between companies. He asserted that legislating technology is a delicate task because technology always moves faster than legislation.[393]

According to Chuck Curran, we should not try to regulate the geolocation aspect of new applications in order to impose a limit on them; we should instead focus on the beneficial aspects of technology. He suggested that the Committee contemplate solutions other than regulation in order to retain the advantages brought by technological innovations.[394]

Christopher Soghoian of the ACLU believes that while regulation can hurt certain sectors of the economy, it can help others: it can kick-start a new sector of the economy.[395]

Meanwhile, Ross Schulman believes that it is possible for a company with good privacy practices to have a comparative advantage and that privacy-friendly products are being developed in that regard. In his view, people must give a small amount of personal information as a trade-off for free services. The problem is that people do not like to learn they are being tracked by strangers and they do not know how that tracking is done.[396]

Michael Mandel explained that he is more worried about the data the government collects than the data companies collect. According to him, companies are vulnerable: they will have to pay for their errors. As for the government, it has coercive power, and coercive power coupled with data is dangerous. Mr. Mandel used the example of credit bureaus, which have the obligation to give consumers access to their credit report for free once a year. He suggested that it would be useful to have self-regulation of that sort among data-driven industries in order to provide access to data reports.[397]

Professor James Cooper, Director, Research and Policy with the Law & Economics Center at George Mason University,[398] believes that privacy policy should focus on the harm caused and be based on empirical evidence. The first step in a sound regulatory regime should be to determine what unfair practices have occurred and what material

---

392 CCIA is a non-profit membership organization for a wide range of companies in the computer, Internet, information technology, and telecommunications industries. It seeks to promote and protect the interests of the industries it represents.

393 Ross Schulman, CCIA, October 4, 2012.

394 Chuck Curran, Center for Data Innovation, October 4, 2012.

395 Christopher Soghoian, ACLU, October 4, 2012.

396 Ross Schulman, CCIA, October 4, 2012.

397 Michael Mandel, PPI, October 3, 2012.

398 The Law & Economics Center (LEC) at the George Mason University School of Law is a national centre for research and education that focuses primarily on the economic analysis of legal and public policy issues.

harm has been done. The second step, the need for empirical evidence, should be to ask what is actionable. In his view, the magnitude of expected harm helps determine what constitutes a reasonable practice.[399]

Similarly, Jim Harper of the Cato Institute thinks that we should let the public decide what value comes first in terms of protecting privacy. In the trade-off between privacy and new technology, he believes we should focus on the harm actually done.[400]

C. Collection, Use and Disclosure of Information

According to Marc Rotenberg, companies prefer to believe that they can do whatever they want with the information they use, since it has been made public. In his view, however, the fact that information is public does not mean that the person concerned has lost interest in it.[401]

Professor Howard Beales of George Washington University explained that the information collected in a transaction between a consumer and a company creates a concern, with regard to privacy, as to how this information is used. In his view, broad rules are easier for consumers to understand and provide an incentive for companies to comply with them. Professor Beales thinks that regulations should not get in the way of industry, because competition between social networks will discipline companies. He emphasized the fact that the information handled by companies is what consumers have chosen to make public.[402]

With respect to privacy policies, Mr. Rotenberg noted that, while there has been much discussion of “short notices”, he remains sceptical about the idea because we are not dealing with fixed metrics and companies are constantly changing their policies. He believes that the best strategy is the idea of privacy by design.[403]

NNEDV representatives also stressed the importance of privacy by default; they noted that the absence of such privacy means that abuse survivors lose their civil rights, which would also have an impact on their children. They believe that the issue of informed consent must be addressed, as well as the increased risk represented by geolocation and biometric encryption. They asserted that the *Children’s Online Privacy Protection Act* (COPPA) needs to be updated to take these elements into account.[404]

---

399 James C. Cooper, George Mason University, October 4, 2012.

400 Jim Harper, Cato Institute, October 4, 2012.

401 Marc Rotenberg, EPIC, October 4, 2012.

402 Howard Beales, George Washington University, October 4, 2012.

403 Marc Rotenberg, EPIC, October 4, 2012.

404 Cindy Southworth and Cynthia Fraser, NNEDV, October 4, 2012.

D. Accountability and Transparency

FTC representatives explained that the FTC had made a legislative recommendation regarding data brokers and the creation of a centralized Web site. The recommendation was intended to improve transparency and shed more light on data brokers, because many of these companies are not known to the public. The idea would be to create a list of these companies so that consumers would be able to make a more informed choice, given the increasing amount of data gathering that is going on.[405]

Christopher Soghoian, for his part, believes that data brokers are not being held accountable because consumers are not aware of them. These companies say that their activities are harmless because the information is anonymous. According to Mr. Soghoian, that statement is increasingly untrue. He explained that when someone visits a Web site, an auction takes place at the same time (in microseconds) for advertising networks, and the highest bidder immediately gets the opportunity to place an ad. Mr. Soghoian believes that consumers should have products that are safe outside of their use and that long-term collection of data will have effects that no one can really foresee.[406]

According to Howard Beales, the primary business model for social networks today is financing through advertising. He considers that advertising, such as behaviorally targeted advertising, is financing a free good, and that it is important for regulation not to make it a less valuable product. He believes that targeted advertising is innocuous.[407]

In the same vein, Michael Mandel drew a link between the way advertisers used to pay for television and newspapers ads, and the way they are now advertising online.[408] Chuck Curran, for his part, voiced the opinion that advertisers buy an audience and they do not care about the personal information itself.[409]

According to Jim Harper, there are no huge lists of personal information being traded by companies. He reminded Committee members that there are levels of control available and that it is possible to deny cookies to Web sites in order to avoid receiving targeted ads.[410] Professor Beales, meanwhile, considers that complete transparency regarding data aggregators cannot work, and he does not think that consumers need to know that some companies are aggregating information.[411]

---

405 FTC, Markus B. Heyder, Christopher N. Olsen, Mark Eich, October 4, 2012.

406 Christopher Soghoian, ACLU, October 4, 2012.

407 Howard Beales, George Washington University, October 4, 2012.

408 Michael Mandel, PPI, October 3, 2012.

409 Chuck Curran, Center for Data Innovation, October 4, 2012.

410 Jim Harper, Cato Institute, October 4, 2012.

411 Howard Beales, George Washington University, October 4, 2012.

E. Consent

On the issue of contracts binding consumers to companies, the FTC has been pushing companies to disclose information to consumers in a clearer way and encouraging them to be innovative in this regard. Privacy policy regarding mobile privacy disclosure is a bigger problem. The FTC promoted the idea of icons accompanied by short text and it has been working in that direction with platform developers, such as Apple.[412]

Ross Schulman of CCIA thinks that privacy policies should be more user-friendly. He noted that companies understood 10 years ago that they needed a privacy policy and that they are now developing their products in line with the privacy by design concept.[413]

Jim Harper believes that consumer education is important, but he considers this a difficult task. He noted that nobody reads privacy policies; consumers want to get where they want to go quickly.[414]

Christopher Soghoian raised the issue that mobile device users had a lack of choice regarding privacy settings, with "take it or leave it" as the only option.[415] NNEDV representatives stated that users should not have only one choice — to turn privacy controls on or off. Privacy control mechanisms should be built in. Big companies such as Google and Facebook have their reputation to consider in their activities, whereas small companies are largely unknown to the public and therefore have no reputation to lose. The biggest challenge is to control the impact of the development of apps by small companies.[416]

F. Security

Christopher Soghoian pointed out that U.S. politicians seem to feel that they have to choose between security and privacy. This is a false choice in Mr. Soghoian's view and more a question of national security (since the security of personal information is not assured and access to such information consequently cannot be controlled).[417]

Marc Rotenberg of EPIC explained that the only area in the U.S. where there is comprehensive privacy legislation is child protection, through COPPA, and that the private sector is not happy with all the restrictions imposed on industry in that regard. According to Mr. Rotenberg, privacy regulation should make data collectors more responsible.[418]

---

412 FTC, Markus B. Heyder, Christopher N. Olsen, Mark Eich, October 4, 2012.

413 Ross Schulman, CCIA, October 4, 2012.

414 Jim Harper, Cato Institute, October 4, 2012.

415 Christopher Soghoian, ACLU, October 4, 2012.

416 Cindy Southworth and Cynthia Fraser, NNEDV, October 4, 2012.

417 Christopher Soghoian, ACLU, October 4, 2012.

418 Marc Rotenberg, EPIC, October 4, 2012.

Regarding COPPA, Eric Miller of the Canadian Embassy mentioned that the FTC requires parental consent to geolocate children and protects children from targeted advertising.[419]

Michael Mandel, for his part, believes there are two ways of seeing the new class of "apps" such as those using geolocation: either as a dangerous innovation, or a way to obtain interesting information about oneself. Starting from the premise that stopping innovation equals stopping economic growth, he asserted that a country with a very strong privacy framework hinders innovation and could therefore fall behind economically. Asked what the role of the legislator should be in that regard, he answered by asking another question: what is the worst that could happen? He mentioned the issue of the protection of children, noting that it is easy to turn off tracking features on mobile devices, to disable cookies, etc.[420]

NNEDV representatives explained that some companies consult with them regarding the development of their products. For example, Google consulted with NNEDV to ensure that no shelters appeared on Google Street View or Google Maps, and Twitter consulted with them to ensure that communications on its network were protected.[421]

The NNEDV representatives emphasized that technology can be used as a form of violence not only against women, but also against children and people with disabilities. They mentioned that technology offers both increased opportunities and increased risks.[422] Innovations in social media, such as geolocation on mobile phones, can be a threat to victims of domestic violence. However, social media is also a useful tool that isolated victims can use to reconnect with other people. That is why NNEDV believes that women should take precautions when using social media, but it does not suggest avoiding the Internet altogether, as that would isolate them even more.[423]

NNEDV representatives explained that it is possible to locate a spouse by email or using spyware (an application that records everything). They spoke about the Safety Net project, which focuses on how technology affects domestic violence. Safety Net is partnered with the CIPPIC in Ottawa, and it also received a grant from the OPC. This project shows how abuse can happen in the digital world and how technology is involved at various stages of the violence.[424]

---

419 Eric T. Miller, Industry Canada, Embassy of Canada, October 3, 2012.

420 Michael Mandel, PPI, October 3, 2012.

421 Cindy Southworth and Cynthia Fraser, NNEDV, October 4, 2012.

422 Ibid.

423 Ibid.

424 Ibid.

Christopher Soghoian shared another point of view: he explained that the police can now track people using geolocation or by asking Google, for example, to provide a copy of a person's inbox.[425]

The NNEDV representatives also raised the issue of anonymity and pseudonymity, which can be powerful tools.[426] Mr. Marc Rotenberg, of EPIC, explained that, while consumers are not opposed to innovation, they are most concerned about identity theft. He pointed out the important role that legislators have in protecting fundamental rights, including the right to privacy. He believes that users cannot address these issues by themselves; even careful users cannot trust companies' claims. Mr. Rotenberg suggested the possibility of creating legislation to force companies to self-regulate.[427]

Regarding the medical sector, which also must be very careful about how it uses personal information, Michael Mandel believes that medical innovation in the U.S. has been hampered because the regulatory framework is too strict. In answer to the Committee's questions regarding which sector he believed would benefit most from legal intervention, Mr. Mandel identified the medical sector.[428]

G. Right To Be Forgotten

Eric Miller explained that, while Europeans are concerned with the "right to be forgotten",[429] the current rules in the United States do not address both privacy issues and issues involving freedom of speech and other rights.[430]

Marc Rotenberg said that EPIC works closely with privacy organizations around the world, and that they all share the same concerns. He noted that the process to standardize privacy regulations in the European Union has been ongoing for about 20 years, and that the upcoming adoption of the Directive and the Regulation[431] will mean a single set of applicable set of rules instead of 27. He also mentioned that cloud computing in the United States makes it harder to control access to information, as data is being stored in other countries.[432]

Underlining the importance of the "right to be forgotten" for victims of domestic violence, NNEDV suggested that regulations regarding privacy and technology should

---

425 Christopher Soghoian, ACLU, October 4, 2012.

426 Cindy Southworth and Cynthia Fraser, NNEDV, October 4, 2012.

427 Marc Rotenberg, EPIC, October 4, 2012.

428 Michael Mandel, PPI, October 3, 2012.

429 See: European Commission, Press Release, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses," January 25, 2012.

430 Eric T. Miller, Industry Canada, Embassy of Canada, October 3, 2012.

431 See: European Commission, Press Release, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses," January 25, 2012.

432 Marc Rotenberg, EPIC, October 4, 2012.

remain general to ensure that they will continue to apply as technology progresses. They noted that Facebook is building a huge database of tagged photos with facial recognition.[433]

Jim Harper explained that, once someone has put information in the system, it is very hard to get it back, to get it out of the system. According to Mr. Harper, the European "right to be forgotten" is like swimming upstream.[434]

H. Do Not Track

Eric Miller noted that the FTC has been pushing hard to have companies add a do-not-track option to their products, and it is doing the same on the child protection front.[435]

Privacy issues are increasingly visible, but James Cooper, of the Law & Economics Center at George Mason University, believes that there is no evidence that it is a crisis that justifies the government's intervention. He also considers the do-not-track concept to be premature, as he believes the market can manage itself.[436]

Christopher Soghoian considers that do not track sends a clear signal about consent; it gives a tool to the FTC and forces companies to react, without requiring legislation.[437]

I. Powers of the Privacy Commissioner of Canada

NNEDV representatives mentioned that, even though Google and Facebook have responded positively to the Privacy Commissioner of Canada's inquiries, small companies must be held accountable as well. NNEDV pointed out the difficulties in obtaining information from companies outside of Canada. The representatives also suggested that the Committee consider the scope of the Privacy Commissioner's influence and proposed that the Commissioner be given the power to fine companies.[438]

Marc Rotenberg, of EPIC, emphasized the quality of the work done by Jennifer Stoddart, the Privacy Commissioner of Canada, and suggested that she be granted order-making powers.[439] Christopher Soghoian, of the ACLU, also asserted that the quality of Ms. Stoddart's work makes her the envy of the world. He recommended that

---

433 Cindy Southworth and Cynthia Fraser, NNEDV, October 4, 2012.

434 Jim Harper, Cato Institute, October 4, 2012.

435 Eric T. Miller, Industry Canada, Embassy of Canada, October 3, 2012.

436 James C. Cooper, George Mason University, October 4, 2012.

437 Christopher Soghoian, ACLU, October 4, 2012.

438 Cindy Southworth and Cynthia Fraser, NNEDV, October 4, 2012.

439 Marc Rotenberg, EPIC, October 4, 2012.

the Privacy Commissioner of Canada be given the power to impose monetary sanctions.[440]

440 Christopher Soghoian, ACLU, October 4, 2012.

APPENDIX A — COMPARING DEFINITIONS IN SOCIAL MEDIA PRIVACY POLICIES AND TERMS OF SERVICE*

	Definition of "personal information" or equivalent
PIPEDA	"means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." s.2(1)
Facebook	By "**information**" we mean facts and other information about you, including actions taken by users and non-users who interact with Facebook. By "**content**" we mean anything you or other users post on Facebook that would not be included in the definition of information. By "**data**" or "**user data**" or "**user's data**" we mean any data, including a user's content or information that you or third parties can retrieve from Facebook or provide to Facebook through Platform. (Statement of Rights and Responsibilities, s.18, accessed June 15, 2012)
Google+	"**Personal Information:** This is information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google. **Sensitive personal information:** This is a particular category of personal information relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality. **Non-personally identifiable information:** This is information that is recorded about users so that it no longer reflects or references an individually identifiable user." (Privacy Policy, Key Terms, accessed June 15, 2012)
LinkedIn	"Please note that certain information, statements, data, and content (such as photographs) which you may submit to LinkedIn, or groups you choose to join might, or are likely to, reveal your **gender, ethnic origin, nationality, age, and/or other personal information about you."** (Terms of Service, 2.K, accessed June 15, 2012)

* Source: Public Interest Advocacy Centre (PIAC), October 18, 2012.

Nexopia	"When opening an account, Nexopia.com collects **identifiable information** submitted by you (Personal Information), including but not limited to: name, email address, username (that you create), sex (gender), location and age. In addition, to help members find and communicate with each other, you may submit and post additional profile data ("**Profile Data**"), including but not limited to the following: weight, height, sexuality (i.e. sexual orientation), dating and living situation and information regarding your interests through the "Profile" tab. In addition, you have the ability to post photographs. **Profile Data is not Personal Information** collected by Nexopia." (Privacy Policy, accessed June 15, 2012)
Twitter	"**personal information**: When you create or reconfigure a Twitter account, you provide some personal information, such as your name, username, password, and email address." **"Non-Private or Non-Personal Information:** We may share or disclose your non-private, aggregated or otherwise non-personal information, such as your public user profile information, public Tweets, the people you follow or that follow you, or the number of users who clicked on a particular link (even if only one did)." (Privacy Policy, accessed June 15, 2012)

APPENDIX B —ENFORCEMENT POWERS GRANTED BY PRIVACY LEGISLATION AROUND THE WORLD*

Privacy organization and privacy protection legislation	Most recent year in which the organization was granted enforcement powers by statute or amendment	Power to issue orders and ensure accountability	Statutory damages and sanctions
Canada OPCC *PIPEDA*	2000	No power to issue orders. Can launch an investigation further to a complaint or initiate an audit if there are reasonable grounds to believe an organization is contravening the Act. Has the power to collect evidence and visit the premises.	No power to impose fines or statutory damages. Must appear before the Federal Court to act on findings.
France French Data Protection Agency (CNIL) *Act on Information Technology, Data Files and Civil Liberties* (LIL)	2004	Can issue a decision.[441] Must inform the company before entering the premises and beginning its investigation. Must obtain authorization from the court to proceed if the company objects to the investigation at the start.	Can impose a fine from €10,000 to €50,000 if a security lapse is noted after a compliance assessment. Under the criminal code, the penalty for insufficient privacy protection cannot exceed a fine of €300,000 and a jail sentence of five years in the case of an individual, or a fine of €1,500,000 in the case of a corporation.

* Unless otherwise indicated, the content from this table has been taken from Baker and McKenzie, "Global Privacy Handbook 2011," IAPP, 2011, 389 pages.

441 Official Web site of the CNIL.

Privacy organization and privacy protection legislation	Most recent year in which the organization was granted enforcement powers by statute or amendment	Power to issue orders and ensure accountability	Statutory damages and sanctions
Germany Federal Commissioner for Data Protection and Freedom of Information *Federal Data Protection Act* (BDSG)	2009	Commissioner oversees telecommunications companies and postal services. Data protection monitoring falls to the states for other areas of the private sector. Mandatory data breach notification. Can order organizations to fix problems that have been identified.	Can fine organizations up to €300,000 for non-compliance with data protection provisions. Heavier fines can be imposed if the infraction resulted in commercial gain.
Ireland Data Protection Commissioner *Data Protection Act*	2003	Has the power to obtain information. Has the power to ensure compliance. Can appoint an "Authorised Officer" to enter and examine premises. Can initiate proceedings and file a lawsuit (summary proceedings).	Can impose a maximum fine of €3,000 on summary conviction. On convictions of indictment, the maximum penalty is a fine of €100,000.[442]
Spain Spanish Data Protection Agency *Spanish Data Protection Act*	2011	Has the power to issue orders, including ordering the destruction of data and data storage equipment. No obligation to notify of data breach.	Has the power to impose penalties for three categories of infringements (minor, serious and very serious), with penalties ranging from €600 to €600,000.

442 Official Web site of the Data Protection Commissioner of Ireland.

Privacy organization and privacy protection legislation	Most recent year in which the organization was granted enforcement powers by statute or amendment	Power to issue orders and ensure accountability	Statutory damages and sanctions
United Kingdom Information Commissioner's Office *Data Protection Act*	2010	Has the power to impose fines and prepare assessment notices. Can investigate private-sector companies, but only with the organization's consent. As part of certain investigations, has the power to enter the premises without giving notice and with a warrant, if needed. Can bring a case before the criminal court in England, Wales and Northern Ireland.	Can fine organizations up to £500,000 for serious data breaches.
United States of America Federal Trade Commission *Federal Trade Commission Act*	1938 (the *Federal Trade Commission Act* of 1914 was amended to provide for administrative fines for non-compliance with orders issued under section 5).[443]	Has the power to summon witnesses and compel the production of documents. Can require that annual or special reports be submitted in order to obtain information about an organization, its practices and management. Can initiate administrative proceedings or bring the case before the courts. Can prescribe rules defining deceitful or unfair practices. Can ask for compensation for harm suffered by the consumer.	Can impose administrative fines, with support from the courts, if an order to cease and desist is not respected after an administrative proceeding.

443 Official Web site of the United States Federal Trade Commission.

Privacy organization and privacy protection legislation	Most recent year in which the organization was granted enforcement powers by statute or amendment	Power to issue orders and ensure accountability	Statutory damages and sanctions
Australia Office of the Australian Information Commissioner (PASSED, BUT WILL NOT COME INTO FORCE UNTIL MARCH 2014) *Enhancing Privacy Protection*	The bill amends the *Privacy Act of 1988*.	The Commissioner will have the power to conduct assessments of privacy performance for both private-sector businesses and government agencies. The Commissioner will be able to make a binding decision further to an investigation initiated by the Commissioner. The Commissioner will be able to accept a written statement from a company committing either to take certain measures or to abstain from certain measures.	The Commissioner will be able to impose administrative fines of up to $1,100,000 for serious or repetitive breaches of privacy. If the Commissioner believes that an organization has not respected a commitment, he or she can ask the court to order the organization to respect its commitment.[444]

444 Official Web site of the Office of the Australian Information Commissioner.

Privacy organization and privacy protection legislation	Most recent year in which the organization was granted enforcement powers by statute or amendment	Power to issue orders and ensure accountability	Statutory damages and sanctions
European Union European Commission (PROPOSED) *General Data Protection Regulation*	Currently under consideration	The authorities in charge of data protection would all have the power to issue orders to cease certain activities, correct data, delete data or destroy data, and to give individuals access to their personal data. They would be able to carry out an investigation to obtain from the controllers and institutions: (a) access to all personal data and all information necessary for their inquiries; (b) access to any premises, including equipment and data processing methods, if there are reasonable grounds to assume that the Regulation is being contravened.	The Regulation states that each supervisory body is able to impose administrative sanctions, including a warning for a first, unintentional offence and then up to three levels of fines: A maximum fine of €250,000 (for government agencies or non-profit organizations) or up to 0.5% of a company's annual global revenue (for businesses); A maximum fine of €500,000 (for government agencies or non-profit organizations) or up to 1% of a company's annual global revenue (for businesses); A maximum fine of €1,000,000 (for government agencies or non-profit organizations) or up to 2% of a company's annual global revenue (for businesses).[445]

445 Official Web site of the European Commission.

LIST OF RECOMMENDATIONS

APPENDIX C
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
Department of Industry	2012/05/29	41
Janet Goulding, Director General Governance, Policy Coordination and Planning		
Jill Paterson, Policy Analyst Security and Privacy Policy, Digital Policy		
Bruce Wallace, Director Security and Privacy Policy, Digital Policy		
Office of the Privacy Commissioner of Canada		
Barbara Bucknell, Strategic Policy Analyst Legal Services, Policy and Research Branch		
Daniel Caron, Legal Counsel Legal Services, Policy and Parliamentary Affairs Branch		
Jennifer Stoddart, Privacy Commissioner of Canada		
University of Ottawa	2012/05/31	42
Michael Geist, Canada Research Chair of Internet and E-commerce Law		
Teresa Scassa, Canada Research Chair Information Law Faculty of Law, Common Law Section		
Valerie Steeves, Associate Professor Department of Criminology		
Canadian Chamber of Commerce	2012/06/05	43
Warren Everson, Senior Vice-President Policy		
Marketing Research and Intelligence Association		
Annie Pettit, Vice-President		
Brendan Wycks, Executive Director		
Office of the Information and Privacy Commissioner of British Columbia	2012/06/07	44
Elizabeth Denham, Commissioner		
Caitlin Lemiski, Policy Analyst		
Helen Morrison, Senior Policy Analyst		
Office of the Information and Privacy Commissioner of Ontario		
Ann Cavoukian, Commissioner		
Michelle Chibba, Director of Policy		
David Goodis, Director of Legal Services		

Organizations and Individuals	Date	Meeting
Ryerson University	2012/06/12	45
Avner Levin, Associate Professor and Director Privacy and Cyber Crime Institute		
Université de Montréal		
Vincent Gautrais, Full Professor		
University of Ottawa		
Ian Kerr, Canada Research Chair in Ethics, Law and Technology		
Canadian Internet Policy and Public Interest Clinic	2012/06/19	46
Tamir Israel, Staff Lawyer		
Heenan Blaikie		
Adam Kardash, Managing Director and Head Access Privacy		
University of Toronto		
Sara Grimes, Assistant Professor Faculty of Information		
As an individual	2012/10/16	50
Pierrôt Péladeau, Researcher and Consultant Social Assessment of Information Systems		
Canadian Marketing Association		
David Elder, Special Digital Privacy Counsel		
Merchant Law Group		
Jason Zushman, Attorney		
Public Interest Advocacy Centre	2012/10/18	51
John Lawford, Executive Director and General Counsel		
Google Inc.	2012/10/30	53
Colin McKay, Policy Manager Google Canada		
MediaSmarts	2012/11/01	54
Matthew Johnson, Director of Education		
Jane Tallim, Co-Executive Director		
University of Victoria		
Colin J. Bennett, Professor		
Nexopia.com Inc.	2012/11/06	55
Kevin Bartus, Chief Executive Officer		
Mark Hayes, Managing Director Heydary Hayes PC		

Organizations and Individuals	Date	Meeting
Information Technology Association of Canada	2012/11/20	56
Karna Gupta, President and Chief Executive Officer		
TÉLUQ		
Normand Landry, Professor		
Facebook, Inc.	2012/11/27	57
Robert Sherman, Manager Privacy and Public Policy		
Acxiom	2012/12/06	58
Jennifer Barrett Glasgow, Global Privacy and Public Policy Executive		
Twitter Inc.		
Laura Pirri, Legal Counsel		
BlueKai Inc.	2012/12/11	59
Alan Chapell, Outside Counsel, Privacy Officer		
Office of the Privacy Commissioner of Canada		
Chantal Bernier, Assistant Privacy Commissioner		
Barbara Bucknell, Strategic Policy Analyst Legal Services, Policy and Research Branch		
Jennifer Stoddart, Privacy Commissioner of Canada		

APPENDIX D
LIST OF BRIEFS

Organizations and Individuals

BC Freedom of Information and Privacy Association

Facebook, Inc.

Landry, Normand and Leslie Regan Shade

Levin, Avner (Ryerson University)

Marketing Research and Intelligence Association

Office of the Information and Privacy Commissioner of Ontario

Parsons, Christopher

Public Interest Advocacy Centre

APPENDIX E
MEETINGS WITH INDIVIDUALS AND ORGANIZATIONS IN WASHINGTON OCTOBER 3 TO 5, 2012

Organizations and Individuals	Date
Industry Canada	2012/10/03
Eric Miller, Senior Policy Advisor	
Progressive Policy Institute (PPI)	
Michael Mandel Chief Economic Strategist	
American Civil Liberties Union (ACLU)	2012/10/04
Christopher Soghoian, Principal Technologist and Senior Policy Analyst	
Computer and Communication Industry Association (CCIA)	
Ross Schulman, Public Policy and Regulatory Counsel	
Electronic Privacy Information Center (EPIC)	
Marc Rotenberg, Executive Director	
Federal Trade Commission (FTC)	
Markus B. Heyder Christopher N. Olsen Mark Eich	
George Mason University	
James Cooper, Director, Research and Policy, Law & Economics Center	
Google Inc.	
National Network to End Domestic Violence (NNEDV)	
Cynthia Fraser Cindy Southworth Vice President of Development & Innovation	
Cato Institute	2012/10/05
Jim Harper, Director of Information Policy Studies	
Center for Data Innovation	
Chuck Curran, Executive Director	
	2012/10/05

Organizations and Individuals	Date
George Washington University	
Howard Beales, Professor, Department of Strategic Management and Public Policy	

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. 39 to 46, 49 to 51 and 53 to 60, 67 and 71*)* is tabled.

Respectfully submitted,

Pierre-Luc Dusseault, M.P.

Chair

Supplementary Report of the New Democratic Party of Canada

New Democrat Members of the Standing Committee on Ethics, Privacy and Access to Information are pleased that the Committee chose to proceed with the NDP motion to study social media and its relationship to the privacy of Canadians. As social media and the commoditization of personal information reshape the privacy landscape world-wide, the *Privacy and Social Media* study offered a timely opportunity for Members to investigate the implications of these changes through a uniquely Canadian lens.

However, New Democrat Members are concerned that the recommendations in this report fall short in key areas. While guidelines issued by the Privacy Commissioner are important tools, they are not sufficiently strong to secure the privacy of social media users in the world of big data. In an effort to do justice to the testimonies heard, New Democrats propose nine additional recommendations that establish a balanced vision for the role of government in privacy protection.

Recommendations

Testimony from Privacy Commissioner Stoddart and others suggests that the Privacy Commissioner's Office wrestles regularly with incidents of noncompliance[i]. On the whole, committee testimony suggested that the *Personal Information Protection and Electronic Documents Act* (PIPEDA) provided a good framework for data protection. However, the soft enforcement powers currently held by the Commissioner are no longer sufficient as personal information is increasingly commoditized and shared across borders in the form of data. It is little wonder that data protection authorities in countries such as the UK, Germany, Australia and France are equipped with enforcement powers (see Appendix B). Consequently, New Democrats believe that enforcement powers must be the first step in reforming PIPEDA. Without them, organizations that want to can continue to disregard the privacy rights of Canadians.

> *"The current law is particularly weak with respect to enforcement. The commissioner has no order-making powers and lacks the ability to impose fines or other penalties in the case of particularly egregious conduct*" – Professor Teresa Scassa, University of Ottawa [ii]

> **Recommendation 1: New Democrats recommend that the government grant enforcement powers to the Privacy Commissioner such as order making powers and the authority to impose administrative monetary penalties.**

As witnesses reported, even diligent and privacy-respecting organizations can fall victim to breaches to the personal data they hold[iii]. New Democrats believe that Canadians deserve to know when they are in harm's way following a breach. Lost personal information can result in identity theft and fraud, heavily costing the victims. Data breach reporting requirements would encourage organizations to invest in better security measures that will also reflect well on the trustworthiness of their brand. The result is both greater security for the public and improved confidence in the online marketplace.

> *"Canada is in dire need of a breach notification obligation. Such an obligation will improve incentives to build stronger technical safeguards and provide users with opportunities to redress harm…"* – Tamir Israel, CIPPIC[iv]

Recommendation 2: New Democrats recommend that the government require all organizations to report data breaches or losses to the Privacy Commissioner where a reasonable person would find that the breach or loss presents any risk of harm to the individuals affected.

The current review of PIPEDA is two years late and Canada's personal information protection law is no longer the envy of the world. Canadians deserve a world-class personal information protection law. Yet, committee testimony repeatedly revealed that Canada lags behind many comparable jurisdictions in data and privacy protection. While New Democrats support a PIPEDA model that is flexible to the demands of new and changing technologies, we do not believe this should eclipse the need for periodic review. Indeed, PIPEDA is required to undergo a statutory review every 5 years.

> "*My office has been conducting extensive research and analysis in preparation for the second mandatory five-year review of PIPEDA by Parliament, which is now past due. We're giving serious thought to how the current regime, which predates all these novel technological developments, should be modernized to keep up with the times."* – Jennifer Stoddart, Privacy Commissioner[v]

Recommendation 3: New Democrats recommend that the government modernize Canadian privacy laws to measure up to privacy protections in comparable democracies and to ensure that the personal information of Canadians is well protected in the digital age.

As online services and applications continue to multiply, so too does the quantity of license agreements and privacy policies requiring the consent of Canadians. These license agreements are generally long, jargon-filled and incomprehensible, yet they can have a staggering impact on an individual's control over their personal information. Indeed, Professor Valerie Steeves stated that license agreements and privacy policies

are often designed to reduce the liability of the service-provider rather than to better inform the user[vi]. The result undermines the effectiveness of the consent principle in PIPEDA. New Democrats believe that as surveillance capacity grows, through mechanisms such as geo-location and facial recognition, Canadians deserve transparency when they give consent for the use of their personal information.

> *"One of the main issues with the protection of personal information on social media sites is the proliferation of standards and protection policies in relation to privacy. We are concerned about the lack of an exhaustive, clear and consistent framework that provides social media users with a set of clear standards on the protection of personal information."* – Professor Normand Landry, TélUQ[vii]

Recommendation 4: New Democrats recommend that the government review Schedule 1 of PIPEDA to clarify that express consent should generally be sought for disclosure of personal information to third parties and that this is especially necessary where such disclosure is a requirement of an end-user license agreement.

In addition to dragging their feet on the privacy file, this government has shown a reluctance to articulate a comprehensive digital economy strategy despite years of promises. Examples of such strategies abound in countries as diverse as Australia and Estonia. New Democrats agree with testimony suggesting that the lack of leadership and ambition by this government on the digital file will prove to be a costly error. Further, our party believes that a digital strategy of any kind, should it materialize, must tackle head-on the challenges that the digital world presents to the privacy of individuals in Canada.

> *"I believe that the failure to articulate and implement a national digital economy strategy comes back to haunt us in these circumstances"* – Michael Geist, University of Ottawa[viii]

Recommendation 5: New Democrats recommend that privacy issues constitute an essential part of a comprehensive digital economy strategy for Canada.

Consumers and users deserve control, choice and transparency in how they manage their personal information. During the study, the Committee heard testimony acknowledging the positive initiatives of some social media organizations to improve the accessibility of their privacy framework and defaults to their users[ix]. However, these practices are not universal. Increasing commoditization of personal information provides incentive for organizations to set very weak default privacy settings. What's more,

tracking mechanisms such as cookies are widespread. New Democrats believe that government should partner with industry to promote the integration of privacy-by-design into default settings and develop do-not-track functions for users.

> *"We always say privacy is good for business. There should be a privacy payoff to business that follow good privacy practices."* – Anne Cavoukian, Ontario Privacy Commissioner[x]

> *""The Devil is in the Defaults". In short, the architecture of every technology includes a number of design choices"* – Professor Ian Kerr, University of Ottawa[xi]

Recommendation 6: New Democrats recommend that the government consider reviewing PIPEDA and corresponding regulations to encourage organizations to implement the practice of privacy by design.

Recommendation 7: New Democrats recommend that PIPEDA, corresponding regulations, and any relevant statutes be amended to encourage organizations to implement Do Not Track functions.

New Democrats believe that, in today's world, a study like this demands further recommendations regarding the protection of children. The Committee heard witnesses emphasize the growth in online advertising targeting children,[xii] and in her testimony Commissioner Stoddart questioned whether children could indeed provide meaningful and informed consent as defined under PIPEDA[xiii]. Numerous experts at committee testified to the challenges of legislatively protecting the personal information of children. University of Toronto professor Sara Grimes spoke of the need for child-specific regulations in Canada and University of Ottawa professor Valerie Steeves raised the tiered consent options based on age studied during the last PIPEDA review. New Democrats believe that in order to fully benefit from the social, cultural and democratic opportunities in social media, children must also benefit from the security that only strong privacy protections can provide.

> *"There is a clear and growing need for child-specific regulation on the collection, management, and use of children's data."* – Professor Sara Grimes, University of Toronto[xiv]

Recommendation 8: New Democrats recommend that the government continue to study ways in which to best protect the personal information of children online while encouraging that they too benefit from the social, cultural, and democratic benefits of the online world.

Digital footprints are left every time an individual surfs the Internet or uses social media. Under PIPEDA, data should only be retained as long as it is necessary to fulfill a specific purpose. Commissioner Stoddart, however, indicated in her testimony that

compliance with this principle under PIPEDA is not always achieved and many social media organizations still maintain vague retention schedules[xv]. Furthermore, much of this data is stored internationally and has become more difficult to track down. Some committee testimony referred to recent European studies seeking to codify a right to be forgotten[xvi]. As the digital footprints of internet users multiply, New Democrats believe that Canadians should be empowered to control their online histories.

> *"It's almost a human right. You should have a chance to ask a company to remove the information. It's clear in the act that you are supposed to delete it if it's no longer used, so we don't see why you shouldn't have the right to remove it."* – John Lawford, PIAC[xvii]

Recommendation 9: New Democrats recommend that the government conduct a study on the privacy policy known as the "right to be forgotten" and report back to Parliament.

******

These nine recommendations reflect a balanced New Democratic vision for privacy reform in the age of social media, big data and instant digital connectivity. The flourishing of social media has afforded us unprecedented opportunity to connect, to share knowledge, to democratically engage and to open up new markets for goods and services. New Democrats believe that the future success of Canada's digital economy and society demands recognition of the new challenges facing privacy protection. Government must adapt and update its policies on and approach to privacy in order to preserve this fundamental civil liberty in the digital realm.

---

[i] ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1155 (Jennifer Stoddart, Privacy Commissioner).
[ii] ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1100.
[iii] ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1225 (Janet Goulding, Industry Canada).
[iv] ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1115.
[v] ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1150.
[vi] ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1125.
[vii] ETHI, *Evidence*, 1st Session, 41st Parliament, November 20, 2012, 1540.
[viii] ETHI, *Evidence*, 1st Session, 41st Parliament, May 31, 2012, 1110.
[ix] ETHI, *Evidence*, 1st Session, 41st Parliament, October 30, 2012, 1535(Colin MacKay, Google).
[x] ETHI, *Evidence*, 1st Session, 41st Parliament, June 7, 2012, 1200.
[xi] ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1210.
[xii] ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1200 (Sara Grimes, University of Toronto)
[xiii] ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1150.
[xiv] ETHI, *Evidence*, 1st Session, 41st Parliament, June 19, 2012, 1105.
[xv] ETHI, *Evidence*, 1st Session, 41st Parliament, May 29, 2012, 1150.
[xvi] ETHI, *Evidence*, 1st Session, 41st Parliament, June 12, 2012, 1225 (Vincent Gautrais, Université de Montréal).
[xvii] ETHI, *Evidence*, 1st Session, 41st Parliament, Octobre 18, 2012, 1545.