Beyond Consent-based Privacy Protection*

Eloïse Gratton**

Executive Summary

At the time that the FIPPs were initially drafted in the early 1970s, their main purpose was to address specific concerns pertaining to computerized databases. The best way to deal with these data protection issues was deemed to be having individuals keep control of their personal information. Forty years later, that self-concept is still one of the most predominant theories of privacy and the basis for data protection laws around the world, including PIPEDA. The "notice and choice" approach is no longer realistic: Individuals are overloaded with information in quantities that they cannot realistically be expected to process or comprehend. Moreover, providing notice and choice in the context of new technologies can be challenging due to the ubiquity of devices, persistence of collection, and practical obstacles for providing information, if devices lack displays or explicit user interfaces. Before amending PIPEDA on consent, one should be careful to make sure that the amendment will not be detrimental or problematic as soon as new technologies emerge**.** The wording pertaining to obtaining consent under PIPEDA is flexible enough to accommodate new types of technologies and business models. Another argument against amending PIPEDA pertains to the fact that social norms in connection with any new technology or business practice may not yet to be established. The downside of the flexibility surrounding the notion of consent is that it creates uncertainty. Policy guidance on enhancing transparency and obtaining valid consent will therefore be increasingly necessary to address some of this uncertainty and allow organizations to innovate without taking major legal risks. It is always less disturbing to provide a solution which will be incorporated within the current legal framework, such as a proposed interpretation, than to propose a new amendment to the law. The notion of "consent" under PIPEDA is already quite flexible and is technology-neutral, allowing for this notion to be interpreted with the proper balance between the protection of privacy and the need or organizations to collect, use or disclose personal information for the purposes that the reasonable person would consider appropriate in the circumstances. Any interpretation of the notion of consent should consider any impact on innovation, as well as certain new ethical issues that may, to a certain extent, go beyond the current application of PIPEDA. An interpretation which includes a risk-based approach may also allow organizations to streamline their communications with individuals, reducing the burden and confusion on individual consumers. Although this new approach would imply rethinking, to some extent, PIPEDA's current consent model, this approach should be further explored in the near future.

* This paper dated July 11, 2016, is submitted to the Office of the Privacy Commissioner of Canada, as part of its Consultation and Call for Submissions on consent and privacy, exploring potential enhancements to consent under PIPEDA. An earlier version of this paper was submitted to Innovation, Science and Economic Development Canada in March 2016. The views expressed in this paper are not necessarily those of Innovation, Science and Economic Development Canada or of the Government of Canada. Les opinions exprimées dans ce document ne sont pas nécessairement celles d'Innovation, Sciences et Développement économique Canada ou du gouvernement du Canada.

** Partner and National Co-Leader, Privacy and Data Security. The content from this white paper should not be understood or considered as providing legal advice. The views expressed herein are solely those of the author in her private capacity and do not in any way represent the views of the law firm Borden Ladner Gervais LLP.

TABLE OF CONTENTS

INTRODUCTION

Privacy is no doubt essential for individuals as well as for society in general and protecting privacy has always been seen as an important, even as a fundamental right. Privacy is also indispensable for the protection of other rights, including freedom of speech and freedom of information. The concern for the protection of privacy is relatively recent, in the sense that it has been stimulated by the growing pressures exerted by modern industrial society upon daily life.[1]

Various definitions of *privacy* have been adopted since the late nineteenth century, illustrating an evolving concept. After privacy was first conceptualize as "the right to be let alone" following the landmark 1890 article by Warren and Brandeis,[2] and then conceptualized as "the respect for one's private and family life, his home and his correspondence"[3] in the late forties, the most recent step in theorizing privacy came in the late 1960s and early 1970s, motivated by technological threats to privacy. With the development of automated data banks and the growing use of computers in the private and public sectors, privacy was at that point conceptualized as having individuals "in control over their personal information". The Fair Information Practices Principles ("FIPPs") were elaborated during this period and have been incorporated in data protection laws adopted in various jurisdictions around the world ever since, including, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") in Canada. Under these FIPPs, individuals have certain rights, including the right to be informed of what personal information is collected about them and concerning the use and the disclosure that will be made of their information, and the right to consent to such data handling activities. PIPEDA was built on the FIPPs and provides for a consent-based model.

The circumstances have changed fundamentally since privacy was conceptualized as "individuals in control of their personal information" over forty years ago. Individuals constantly provide personal information. The Internet now reaches billions of people around the world and serves as a virtual marketplace for products, information, and ideas. The fluidity of personal information collections has increased as the scope and goals of such data continuously evolve. Business models are increasingly based on the notion of greater customization and various products and services are offered for free, as they may be partially supported by advertising revenue. Companies also wish to use analytic solutions in order to better understand their customers, as well as to improve or develop new products and services. The second generation of the Internet made possible greater interaction and connectedness among online users, and individuals are becoming increasingly involved in managing their own data through online social networks. There are also recent technological developments triggering the emergence of new identification tools, which allow for easier identification of individuals.

Recent technologies are presenting additional challenges to consent-based privacy protection frameworks. With the Internet of Things (IoT), seemingly mundane everyday devices are fitted with

---

[1] See Home Office, Lord Chancellor's Office, Scottish Office (Chairman The Rt. Hon, Kenneth Younger), *Report of the Committee on Privacy*, presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by Command of Her Majesty, July 1972, at 6, para. 20.

[2] Samuel Warren & Louis Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193 [Samuel Warren & Louis Brandeis]; these authors were defending privacy against the threat of instantaneous photography in the popular press.

[3] *Universal Declaration of Human Rights*, G.A. res. 217(III), U.N.G.A.O.R., 3d Sess., Supp. No. 13, U.N. Doc A/810, (1948) 71, at preamble, para.2; Soon afterwards, the Council of Europe, founded in 1949 and based in Strasbourg, adopted its own Convention for the Protection of Human Rights and Fundamental Freedoms. The *European Convention for the Protection of Human Rights and Fundamental Freedoms,* 4 November 1950, 213 U.N.T.S. 221, Eur TS 5, at Introductory section, para.2.

microchips, sensors, and wireless communication capabilities. All of these devices are networked together to provide a seamless user experience. They are intended to collect data, aggregate them, communicate them to other devices in the network (*machine-to-machine* communication or M2M) and respond according to predetermined outcomes.[4] Every device, of course, has its own producer and therefore its own privacy policy dictating who owns and gets access to the data and how it may be used – including data that comes from M2M communication. A study by Cisco shows that by 2020, 37 billion intelligent devices will be connected and communicating – three times the number of such devices being used in 2015.[5] Wearable technologies collect data about all of the user's daily activities and communicate them automatically to an online data management system, aggregating the data and ensuring feedback to the user.[6] The more data the user allows the device to accumulate, the more useful it may become.[7] Moreover, more and more devices record, stream or upload a constant feed of images or movies. CCTV is one example; Google Glass is another. Almost everyone nowadays owns a smartphone with which we constantly take pictures, share them on social networks, and comment on them.[8]

At the time that the FIPPs were initially elaborated in the early 1970s, their main purpose was to address specific concerns pertaining to computerized databases. The best way to deal with these data protection issues was deemed to be having individuals in control of their information.[9] Forty years later, that selfsame concept is still one of the most predominant theories of privacy and the basis for data protection laws around the world, including PIPEDA. In light of the recent technologies, it is reasonable to wonder if the current consent-based approach from PIPEDA is still the best way forward.

The Office of the Privacy Commissioner ("OPC") has recently published a discussion paper entitled "Consent and privacy" exploring potential enhancements to consent under PIPEDA.[10] The OPC also launched a Consultation and Call for Submissions requesting input on its consent paper and on solutions which would be helpful in addressing consent challenges and on whether legislative changes are required. This paper is meant to provide guidance on some of the issues raised, such as whether legislative

[4] For a brief overview, see Article 29 Data Protection Working Party, "Opinion 8/2014 on the recent developments on the internet of things", 14/EN WP 223, available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> [Article 29 Data Protection Working Party (2014)].

[5] White paper, "The Internet of Everything and the connected athlete. This changes… everything", available at: Cisco <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.html>.

[6] Thierer, A.D., "The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation", 21 Rich. J. L. & Tech. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>; Martin, G., "Wearable intelligence: Establishing protocols to socialize wearable devices" (April 1, 2014), available at: O'Reilly Media Company <http://radar.oreilly.com/print?print_bc=60033>.

[7] For instance, a microchip that automatically alarms the hospital and provides the location of an individual when it senses that, based on the individual's body temperature, weight, sex, muscle tenseness etc., he/she is having a heart attack, may be very useful indeed.

[8] Hargreaves, S., "*Jones*-ing" for a Solution: Commercial Street Surveillance and Privacy Torts in Canada" (2014) 3 Laws 388.

[9] Eloïse Gratton, *Understanding Personal Information, Managing Privacy Risks* (Markham: LexisNexis, 2013), at 1-17 [Eloïse Gratton (2013)].

[10] Office of the Privacy Commissioner, *Consent and privacy, A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act,* Prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada, May 2016, available at https://www.priv.gc.ca/information/research-recherche/2016/consent_201605_e.pdf,

changes are required as well as on potential solutions which would be helpful in addressing consent challenges.

In the first section, this paper will illustrate how, in the context of new Internet technologies, the "notice and choice" approach is challenged. This is in part due to the current volume of data collections and vagueness of privacy policies, the increase in the numbers of players involved, the dynamic aspect of privacy policies and business models and the ubiquity of data collections and exchanges. It is also due to the fact that with technology becoming increasingly sophisticated, individuals may have a hard time understanding what kind of information is being collected about them and how their information will in fact be used. The fact that seeking consent may not always be practical to obtain, and is sometimes even impossible with recent business models and innovative technologies, will also be discussed.

In the second section, a few considerations which may be useful when addressing the challenges with PIPEDA's consent-based model will be discussed. More specifically, this section will elaborate on the fact that we should be careful before amending the law, that research and policy development will play an increasingly important role, and that the interpretation that will be adopted of the notion of meaningful consent may also be part of the solution. That interpretation should take into account its impact on innovation and ethical issues. Moreover, this section will discuss considering the adoption of a risk-based approach and the benefits of such an approach.

1. NOTICE AND CHOICE APPROACH CHALLENGED

Many have, for quite some time, criticized the notion of meaningful consent which is central in any legislation based on the FIPPs, as it allegedly no longer provides a realistic approach. Solove reports that "people will be given consent forms with vague fine-print discussions of the contractual default privacy rules that they are waiving, and they will sign them without thought."[11] Schwartz questions whether individuals are in fact able to exercise meaningful choices with regard to the handling of their personal information, given disparities in knowledge and power when bargaining over the transfer of their information.[12] Nissenbaum has articulated the view that it is no longer clear whether individuals are always capable of making informed choices and therefore, meaningful privacy notices and valid consent may be considered as illusory.[13] In this section, the inadequacy of privacy policies as a means to communicate choices, as well as the fact that consent is now challenged by technological changes, will be discussed.

1.1 Transparency: Inadequacy of Privacy Policies as a Means of Communicating Choices

Privacy policies play a central role in determining whether consent can be said to be meaningful. PIPEDA aims to ensure that the privacy policies of organizations clearly and directly inform individuals about the ramifications of sharing personal information with these organizations. Under PIPEDA, organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.[14] To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Following the recent amendments provided in the *Digital Privacy Act* (S-4),[15] PIPEDA was amended to include a revised "valid consent" provision, by shifting from a subjective standard to a more objective one. Under PIPEDA's new section 6.1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which he or she is consenting.[16]

This section will discuss how, in practice, most privacy notices are ineffective in properly informing users of data handling practices.[17] This ineffectiveness stems from challenges that can be attributed not only to general shortcomings of the notice and choice concept, but also to the challenges in designing

[11] Daniel J. Solove, *"*Privacy and Power: Computer Databases and Metaphors for Information Privacy*"* (2001) 53 Stan. L. Rev. 1393, at 1454 [Daniel J. Solove].

[12] Paul M. Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 Vand. L. Rev. 1609, at 1661.

[13] Solon Barocas & Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent" (Lecture delivered at the Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information, October 2009), at 1.

[14] *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c. 5, Schedule 1, s. 4.3.2.

[15] *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*, R.S.C . 2015, c.32.

[16] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, s. 6.1.

[17] L. F. Cranor, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice" (2012) 10:2 J. On Telecomm. & High Tech. L 273 [L.F. Cranor (2012)]; A. M. McDonald & L. F. Cranor, "The Cost of Reading Privacy Policies" (2008) 4:3 I/S -A Journal of Law and Policy for the Information Society 540 [A.M. McDonald & L.F. Cranor].

effective privacy notices.[18] More specifically, the fact is that privacy policies are inadequate as a means of communicating choices to individuals, for the simple reason that they are vague and complex documents that users no longer bother to read, and that organizations may, in some cases, have an incentive to collect as much information as possible.

1.1.1 Vagueness and Complexity of Privacy Policies

There are several reasons why privacy policies are ineffective. It is reported that it is difficult for individuals to understand such policies, because they are often complex and use specialized terms.[19] Policies are often written by specialized professionals, without considering the audience that may include users who are "below basic" literacy. Privacy policies, for instance, tend to be written at a college level; whereas the average reading level of an individual may typically be somewhere between that of eighth and ninth grade pupils.[20] Similarly, privacy policies are often written in English, which is not everyone's first language. Privacy policies may also be very long, discouraging users from reading them.[21] Users are not generally capable of processing all the information they contain.[22]

Privacy policies may not always include sufficient or complete information to allow for a truly informed decision on the part of the consumer.[23] Privacy policies may also often be vague about what information is collected, how the information will be used and how it will be disclosed.[24]

Organizations managing personal information may capitalize on the ambiguity of new types of data which may or may not qualify as personal information, either by omitting to disclose the collection of new types of data (such as IP addresses, UDIDs, metadata, MAC addresses, profile or location

---

[18] Florian Schaub et al., "A Design Space for Effective Privacy Notices" (Paper delivered at the USENIX Association Symposium on Usable Privacy and Security, 2015), 2 [Florian Schaub et al.].

[19] Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", 01197/11/EN WP187, available at: European commission <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>, at 35; Florian Schaub et al., *supra* note 18, at 2,9; Fred Cate, "The Limits of Notice and Choice" (2010) 8(2) IEEE Security Privacy 59 [Fred Cate (2010)]; Joshua Gomez, Travis Pinnick & Ashkan Soltani, "KnowPrivacy", School of Information, UC Berkeley, Berkeley, California, 2009-037, June 2009, at 11-12, available at: <http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf> [Joshua Gomez et al.]; US, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Preliminary Staff Report, December 2010) [Federal Trade Commission (2010)].

[20] *Ibid,* at 1053 referring to Patrick Gage Kelley et al., "Standardizing Privacy Notices" (2010) available at: Carnegie Mellon University <http://repository. cmu.edu/cgi/viewcontent.cgi?article=1002&context=cylab>, at 1.

[21] Florian Schaub et al., *supra* note 18, at 2; See also Fred H. Cate, "The Failure of Fair Information Practice Principles" in Jane K. Winn, ed, *Consumer Protection in the Age of "Information Economy"* (Ashgate, 2006) 341, at 359.

[22] Ryan Calo, "Against Notice Skepticism In Privacy (And Elsewhere)", (2012) 87 Notre Dame Law Review 1027, at 1054 [Ryan Calo (2012)].

[23] Joel R. Reidenberg et al., *Automated Comparisons of Ambiguity in Privacy Policies and the Impact of Regulation* (January 9, 2016), Fordham Law Legal Studies Research Paper No. 2715164, available at: <http://ssrn.com/abstract=2715164> [Joel R. Reidenberg et al.].

[24] Irène Pollach, "A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent" (2005) 62:3 Journal of Business Ethics 221, at 228, 230-231.

information), or by disclosing the collection but mentioning that the data in question is not *personal information* (i.e. "Non-PII").[25]

Privacy policies may also be purposefully vague as to the uses which will eventually be made of the data to avoid limiting future uses. For example, organizations may claim to use the data collected for broad purposes, such as improving their products and services, developing new ones or enhancing the customer's experience. Organizations do not necessarily have bad intentions when they use broad language in their policy; they may simply wish to be flexible so as to accommodate future actions without changing their policy,[26] but the implication is that potential future uses of the information are too vast to enable individuals to make an adequate evaluation.

Finally, these privacy policies may also be nebulous when it comes to those with whom the data will be shared. Businesses often share this information with their marketing partners (as well as corporate affiliates and subsidiaries), in order to build more complete profiles about individual consumers; and often do so quietly.[27] Many privacy policies will use terms like "partners" or "affiliates" to describe potential recipients of user data. According to some, these terms are "elastic", because they can encompass different meanings in different contexts.[28] The KnowPrivacy report analysis of privacy policies found that while many businesses mention that they do not share data with third parties, what they mean by "third parties" is not clear.[29] They may share customer data with "subsidiaries" or "affiliated businesses"[30], but rarely do they ever clarify who these parties are, and what kind of privacy business practices they follow.[31] Without providing a definitive distinction between the types of parties with whom data may be shared, individuals often do not know the extent to which their personal information has been outsourced or shared. [32]

In many instances, consent to data collection activities is granted, despite the possibility -- completely unbeknownst to the particular user in question -- that personal information already on file may be correlated or aggregated with new data, in order to form a more complete user profile. Cohen notes that "a comprehensive collection of data about an individual is vastly more than the sum of its parts."[33]

---

[25] Eloïse Gratton, "Top five mistakes when drafting website privacy policies" (July 6, 2015) available at: <http://www.eloisegratton.com/blog/2015/07/06/top-five-mistakes-when-drafting-website-privacy-policies/> [Éloïse Gratton, July 6, 2015]; See also Joel R. Reidenberg et al., *supra* note 23 , at p. 28.

[26] Joel R. Reidenberg et al., *supra* note 23, at 4.

[27] See Stephanie Clifford, "*Your Online Clicks Have Value, for Someone Who Has Something to Sell*" (25 March 2009), available at: *The New York Times* <http://www.nytimes.com/2009/03/26/business/media/26adco.html>.

[28] Joel R. Reidenberg et al., *supra* note 23, at p. 7.

[29] The CPO of an organization operating a website claimed that they consider the advertising service company DoubleClick to be a "marketing partner," and not a "third party"; Joshua Gomez, Travis Pinnick & Ashkan Soltani, *KnowPrivacy* (1 June 2009), available at: <http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf>.

[30] See Amazon.ca Privacy Notice, available at: Amazon <http://www.amazon.ca/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=918814> [Amazon.ca Privacy Notice]: "We share customer information only as described below and with subsidiaries (…) We work closely with our affiliated businesses."

[31] Joshua Gomez et al., *supra* note 19, at 9.

[32] Janet Lo, *A "Do Not Track List" for Canada?* (Ottawa: Public Interest Advocacy Centre, 2009) at 48, available at: Public Interest Advocacy Centre, available at: <http://www.piac.ca/wp-content/uploads/2014/11/dntl_final_website.pdf> [Janet Lo].

[33] Julie E. Cohen, "*Examined Lives: Informational Privacy and the Subject as Object*" (2000) 52 Stan. L. Rev. 1373, at 1398 [Julie E. Cohen].

Certain business models focus on the aggregation and sale of personal information by acquiring information from public records.[34] The initial collection of information and the consent provided may therefore not always reflect the extent to which a given individual is "informed" about a given data collection practice, as further discussed in section 1.2. This issue is also linked to the fact that technologies are increasingly complex.

1.1.2 Privacy Policies Fatigue

The issue with a consent or choice-based approach is the fact that, with the volume of data exchanges and collections taking place in modern society, individuals would be faced with the prospect of constantly reviewing privacy policies and consenting to them throughout any given day.[35] It has been recently estimated that to read the privacy policies for all the websites an Internet user visits annually would take about 244 hours per year.[36] Researchers at Carnegie Mellon once calculated that it would cost $781 billion in worker productivity, if everyone were to read all of the privacy policies they encountered online in one year.[37] It is not reasonable to expect average individuals to devote large portions of their time in order to process and provide meaningful responses to consent requests.

Most users do not read privacy policies:[38] A recent White House report stated, "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[39] To further illustrate the fact businesses know that users do not read privacy policies, it was reported a few years ago that a videogame company from the United Kingdom included a provision in its statement that, unless the user opted out, the company would retain rights to the user's eternal soul.[40]

Privacy notices may also often be shown at inopportune times when they conflict with the user's primary task; therefore they are dismissed or accepted without scrutiny. Last but not least, authors have articulated the view that even if individuals could understand and had the time to read privacy policies, there is not enough market differentiation for them to make informed choices.[41] Ostensibly, users are

---

[34] See Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2009-004* : *No Consent Required for Using Publicly Available Personal Information Matched with Geographically Specific Demographic Statistics*, available at: <https://www.priv.gc.ca/cf-dc/2009/2009_004_0109_e.asp> [PIPEDA Case Summary #2009-004].

[35] Lawrence Lessig notes that our existing system of posting privacy policies and enabling consumers to opt in or out has high transaction costs because people do not have "the time or patience to read through cumbersome documents describing obscure rules for controlling data." See Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 160; See also Chris Jay Hoofnagle & Jennifer King, "*What Californians Understand about Privacy Online*" (3 September 2008), available at: <http://ssrn.com/abstract=1262130 or http://dx.doi.org/10.2139/ssrn>.

[36] A.M. McDonald & L.F. Cranor, *supra* note 17.

[37] *Ibid*.

[38] Florian Schaub et al., *supra* note 18; See also discussed in US, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), at 2 [Federal Trade Commission, March 2012].

[39] President's Council of Advisors on Science and Technology, *Big data and privacy: A technological perspective* (Report to the President, Executive Office of the President, May 2014).

[40] See *7,500 Online Shoppers Unknowingly Sold Their Souls*, FoxNews (Apr. 15, 2010), available at: <http://www.foxnews.com/scitech/2010/04/15/online-shoppers-unknowinglysold-souls/>.

[41] A.M. McDonald & L.F. Cranor, *supra* note 17.

being flooded with privacy policies and are becoming increasingly complacent when faced with consent requests.

1.1.3 Incentive for Data Collection and Retention

Business models are increasingly based on the notion of greater customization of services and products. Due to the global dimension of its potential audience, the Internet has become an increasingly attractive forum for advertisers, who can target their campaigns more precisely and effectively than by advertising in other media. Technology now makes it possible to gather a lot of information to profile individuals and track their conduct, in order to send personalised advertising or tailored websites, products or services accordingly. Behavioural advertising provides benefits to consumers in the form of free web content and personalized advertisements.[42] Many online service providers are offering services, information, and entertainment free of charge to online users, as long as they agree to receive advertising and allow their online behaviour to be tracked.[43] Various services are offered for free online, as they may be partially supported by advertising revenue, including online social services such as Facebook and Google's web service Gmail.[44] Additionally, more individuals are able to access newspaper content on the Internet for free, because it is subsidized by online advertising.[45] Certain studies even show that individuals do not want and do not expect to be paying for web services.[46]

In the Canadian Internet Policy and Public Interest Clinic complaint against Facebook,[47] one of the issues raised was the fact that since users were not allowed to opt out of Facebook ads, Facebook was unnecessarily requiring users to agree to such ads as a condition of service, in violation of principle 4.3.3 of PIPEDA. The finding of the OPC on this issue took into account the fact that the site is free to users and that since advertising is essential to the provision of the service, individuals who wish to use the service must be willing to receive a certain amount of advertising.[48] This case may illustrate a change in mentality as to what is acceptable from a privacy and business perspective, where a certain trade-off is necessary.

---

[42] Office of the Privacy Commissioner of Canada, *Privacy and Online Behavioural Advertising*, Guidelines, December 2011.

[43] Google, *Response to the Article 29 Working Party Opinion On Data Protection Issues Related to Search Engines* (8 September 2008) at 3.

[44] See Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud* (26 June 2008), U of Chicago Law & Economics, Olin Working Paper No. 414, at 7, available at: <http://ssrn.com/abstract=1151985>. See also Options Consommateurs, "How Free is "Free", Setting limits on the collection of personal information for online behavioural advertising', Research Report, 2015, available at: <http://www.option-consommateurs.org/documents/principal/en/File/option_consommateurs_2015_gratuite_english.pdf>.

[45] Janet Lo, *supra* note 32, at 48.

[46] Internet Advertising Bureau, "PIPEDA & IAB Canada's Industry Self-Regulation Initiatives: A Win-Win For Canadian Consumers, Web Publishers + Web Innovators Going Forward", Submission for the 2010 Privacy Commissioner Consultation, 15 March 2010, at 5.

[47] Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2009-008*: *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.* (16 July 2009) [PIPEDA Case Summary #2009-008].

[48] *Ibid*, at Section 3, Finding 131.

With new business models based on "sponsored" services or greater customization, personal information is often viewed as a commodity.[49] This appetite for information can lead to very nebulous privacy policies attempting to entice individuals to release information. Expanding on the idea of personal information as a commodity, Schneier states:

> "Here's the problem: The very companies whose CEOs eulogize privacy make their money by controlling vast amounts of their users' information. Whether through targeted advertising, cross-selling or simply convincing their users to spend more time on their site and sign up their friends, more information shared in more ways, more publicly means more profits. This means these companies are motivated to continually ratchet down the privacy of their services, while at the same time pronouncing privacy erosions as inevitable and giving users the illusion of control. (…)"[50]

By default, privacy settings will usually be set to allow the sharing of personal information. For example, it was reported that over the years, Facebook has changed its default privacy settings in order to make profiles more public.[51] While users can, in theory, keep their previous settings, that takes an effort, and many individuals will simply accept the new defaults settings.[52]

Certain companies design apps that seek to access all of a user's contacts in order to encourage the user to draw others to the service.[53] Other companies press users to share information in ways that may exceed initial expectations.[54] It has been reported that certain social video-sharing apps saw their user base grow by 10 million users per week, after being integrated with Facebook, thus becoming the top Facebook and iOS apps in record time.[55] Many of these new users failed to realize that by clicking to see videos shared by friends, they were also sharing those videos with their entire network.[56]

---

[49] Facebook is one example of a business model which has an economic incentive to gather as much information as possible about its users to help advertisers promote their goods and services. It was reported to have posted more banner ads than any other website in 2010; L. Gordon Crovitz, "Privacy Isn't Everything on the Web", Editorial, *The Wall Street Journal* (24 May 2010).

[50] Bruce Schneier, "Google and Facebook's Privacy Illusion", Editorial, *Forbes* (6 April 2010), available at: <http://www.forbes.com/2010/04/05/google-facebook-twitter-technology-security-10-privacy.html>.

[51] Kevin Bankston, "Facebook's New Privacy Changes: The Good, The Bad, and The Ugly", *The Electronic Frontier Foundation* (9 December 2009), available at: <https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>.

[52] Ian Kerr, "The devil is in the defaults" (May 29, 2010), available at: <http://iankerr.ca/content/2010/05/29/the-devil-is-in-the-defaults/>; Michael Richter, "Another Step in Open Site Governance", *The Facebook Blog* (26 March 2010), available at: <http://blog.facebook.com/blog.php?post=376904492130>; Hamish Barwick, "Facebook facial recognition should be opt in, not opt out", *Computerworld* (10 June 2011), available at: <http://www.computerworld.com.au/article/389810/facebook_facial_recognition_should_opt_opt/>.

[53] Megan Rose Dickey, *It Turns Out Path, Considered a Threat to Facebook, May Just be Really Good at Spamming*, BUSINESS INSIDER, May 1, 2013, available at: <http://www.businessinsider.com/pathspamming-users-2013-5>.

[54] See Fred Stutzman, Ralph Gross & Alessandro Acquisti, "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook", 4(2) J. PRIV. & CONFID. 7 (2012) [Fred Stutzman, Ralph Gross & Alessandro Acquisti].

[55] *Viddy* and *Socialcam*. See Om Malik, "Facebook giveth, Facebook taketh: A curious case of video apps", *GIGAOM* (May 14, 2012), available at: <http://gigaom.com/2012/05/14/facebook-giveth-facebook-taketh-a-curious-case-ofvideo-apps>.

[56] Elinor Mills, "Socialcam closes hole that enabled accidental sharing", *CNET* (May 17, 2012), available at: <http://news.cnet.com/8301-1009_3-57436777-83/socialcam-closes-hole-that-enabledaccidental-sharing>; Wendy Davis, "Socialcam Beefs Up Privacy Features", *MEDIAPOST* (May 17, 2012), available at: <http://www.mediapost.com/publications/article/174877/#axzz2SAgpHAX9>.

With Big Data, organizations have an incentive to collect more personal information and keep such information for longer. These examples simply illustrate the shared incentive for businesses to collect a large quantity of personal information and to remain vague in framing their privacy policies. Froomkin suggests that: "In theory, the parties to a transaction can always contract for confidentiality. This is unrealistic due because consumers suffer from privacy myopia: they will sell their data too often and too cheaply".[57]

1.2 Consent Challenged by Technological Changes

The previous section illustrates how ineffective current privacy policies are a means to communicate choices, as these statements are rarely ever read, are often confusing and are incapable of capturing the complexity of modern data-handling practices. As a result, individuals typically have little meaningful choice about the use of their personal information.

As Cohen correctly notes, "freedom of choice in markets requires accurate information about choices and other consequences, and enough power—in terms of wealth, numbers, or control over resources—to have choices."[58] Due to lack of understanding about the collection, use and disclosure of their personal information, individuals are then incapable of making informed choices.[59] According to some, although data protection laws around the globe generally require consent prior to the collection, use, or disclosure of most personal information, privacy laws such as PIPEDA (based on the FIPPs) must be understood as setting higher thresholds for obtaining consent.[60]

Many are recently questioning whether the notice and consent model still makes sense. As a matter of fact, although individuals are aware that there are some risks involved with data collection when they are active on the web or using new technologies, these risks are only potential to them, not very visible, and not quite quantifiable. A particular concern flows from the fact that the consequences of information circulation are often unbeknownst to stakeholders when information is initially put into circulation, especially since it is often the agglomeration of information that may be viewed as problematic. Solove believes that it is difficult for a given individual to attribute a meaningful value to specific pieces of personal information.[61]

This section will discuss how the notion of consent is being challenged, in light of the increase in the number of players providing new products and services, the dynamic aspect of privacy policies and business models, the ubiquity of data collection and sharing practices, as well as because technology is becoming increasingly sophisticated, so as to enable individuals to properly evaluate the risks related to their consent to a given data-handling activity.

---

[57] A. Michael Froomkin, "The Death of Privacy?" , (2000) 52 Stan. L. Rev. 1461, at 1469, 1502: "Once created or collected, data is (…) hard to eradicate; the data genie does not go willingly, if ever, back into the bottle".

[58] Julie E. Cohen, *supra* note 33.

[59] Federal Trade Commission (March 2012), *supra* note 38, at 2.

[60] See Ian Kerr et al., *"*Soft Surveillance, Hard Consent*"*, (2006) 6 Personally Yours 1, at p. 4.

[61] Daniel J. Solove, *supra* note 11, at 1452.

1.2.1 Ever-increasing Number of Players Involved

Information and communication technologies and globalization have created structural and organizational changes, which have influenced data protection laws such as PIPEDA; including greater diversification within business groups, the growth of joint ventures, as well as loyalty programs. These developments are blurring the traditional boundaries between legal entities, such that it is becoming increasingly difficult to conclusively identify the owner or custodian of any particular piece of information.

In Europe, the interaction between data controllers and data processors is essential in the application of certain data protection laws such as Directive 95/46/EC, since they influence who will be responsible for compliance with data protection rules and how individuals can exercise their rights. The increasing complexity of the environment in which these concepts are used has given rise to new and difficult issues, such that the Article 29 Working Party recently issued an opinion emphasizing the need to allocate responsibility between data controllers and data processors, so that compliance with data protection laws can be enforced sufficiently.[62]

The number of players in the ad network and exchange space is ever-increasing, resulting in flows of user data that are opaque to users.[63] More recently, the implementation of the IoT casually implies the combined intervention of multiple stakeholders, including device manufacturers, social platforms, third-party applications, device lenders or renters, data brokers or data platforms. The implies the necessity of a precise allocation of legal responsibilities among these multiple stakeholders with regard to the processing of personal information based on the specificities of their respective interventions.[64] The increasing adoption of wearable devices, (i.e. smart watches or fitness trackers) as well as smart home devices (i.e. smart thermostats or connected light bulbs) represents a trend towards smaller devices that are even more constrained in terms of interaction capabilities, but are also highly connected with each other and the cloud. While providing notice and choice is still considered essential in the IoT,[65] finding appropriate and usable notice and choice mechanisms can be challenging.

1.2.2 Dynamic Aspect of Privacy Policies and Business Models

Many organizations and industry players may change their privacy policies, making it even more difficult to keep track (i.e. "control") of data handling practices.[66] Privacy policies often reserve the right to change their terms and conditions unilaterally, so if users want to know the precise nature of any such modification, it is often up to them to refer back to the new version, which is unrealistic.[67] This practice of unilaterally modifying privacy policies makes it even more difficult for individuals to keep control over their information and provide meaningful consent.

---

[62] Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor"", 00264/10/EN WP 169, available at: European commission, available at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf>

[63] Solon Barocas & Helen Nissenbaum, *supra* note 13, at 1.

[64] Article 29 Data Protection Working Party (2014), *supra* note 4, at 11.

[65] US, Federal Trade Commission, *Internet of things: Privacy & security in a connected world* (FTC staff report, Jan. 2015) [Federal Trade Commission (2015)].

[66] Solon Barocas & Helen Nissenbaum, *supra* note 13, at p. 1.

[67] Éloïse Gratton (July 6, 2015), *supra* note 25.

Not only do privacy policies change, business models often do as well. For instance, Facebook and Google have changed their products over time, and users are not likely to perceive the change.[68] It is even more difficult for users to keep track of their personal information with recent technologies, since such technologies either involve invisible data sharing practices or they are increasingly complex, as further discussed in the next sections.

1.2.3 Ubiquity of Data Collection and Sharing

In many cases, information is collected online and offline instantaneously and invisibly, which further challenges the validity of consent. For instance, when the consumer browses for products and services online, advertisers may choose to collect and share information about the consumer's activity, search history, websites visited, etc. When participating in an OSN, third-party applications are likely to have access to the user's information pertaining to his posts. When using location-enabled devices, various third party application providers and entities may thus ascertain the consumer's precise whereabouts. If a consumer uses loyalty cards at a grocery store or sends in a product warranty card, his name, address, and information about his purchase may be shared with data brokers and combined with other data.[69]

More recently, certain wearable things are likely to be adopted quickly, as they extend the usefulness of everyday objects familiar to the individual. They may be embedded in cameras, microphones and sensors that can record and transfer data to the device manufacturer.[70] The Article 29 Working Party has raised the concern that such wearable things, kept in close proximity to users, result in the availability of a range of other identifiers, such as the MAC addresses of other devices, which could be useful to generate a fingerprint allowing location tracking:

> "The collection of multiple MAC addresses of multiple sensor devices will help create unique fingerprints and more stable identifiers which IoT stakeholders will be able to attribute to specific individuals. These fingerprints and identifiers could be used for a range of purposes, including location analytics[71] or the analysis of movement patterns of crowds and individuals."[72]

The FTC has also noted that providing notice and choice in the context of the IoT can be challenging due to the ubiquity of devices, persistence of collection, and practical obstacles to providing information if devices lack displays or explicit user interfaces.[73] The OPC, which recently issued its research paper on the IoT, also raises the point that data collection by devices in the IoT context may often be invisible to

[68] Chris Jay Hoofnagle, "The privacy Machiavellis" *San Francisco Chronicle* (25 May 2010), available at: <http://www.sfgate.com/cgi-bin/article.cgi?f=%2Fc%2Fa%2F2010%2F05%2F24%2FED101DJPE1.DTL> [Chris Jay Hoofnagle].

[69] Federal Trade Commission (2010), *supra* note 19, at i.

[70] Article 29 Data Protection Working Party (2014), *supra* note 4, at p. 5. Furthermore, the availability of an API for wearable devices (e.g. Android Wear) also supports the creation of applications by third parties who can thus get access to the data collected by those things.

[71] Location analytics refers to the analysis of how many people are in a certain place at a certain time and for how long they remain there.

[72] Article 29 Data Protection Working Party (2014), *supra* note 4, at p. 8.

[73] Federal Trade Commission (2015), *supra* note 65.

users and, because they may not be aware of it, they are unlikely to be in a position to understand it or weigh in on the manner in which it is done. [74]

These new trends and technologies must be combined with the fact that the data collected can later be combined with other data issued from other systems (e.g. CCTV or internet logs), in most cases without the knowledge of the individuals concerned. The OPC has demonstrated the powerful insights that can be obtained about individuals from IP addresses, as well as from metadata.[75] This has obvious implications for achieving meaningful consent.

1.2.4 Technology Becoming Increasingly Sophisticated

Recent technologies and new types of business models are becoming more complex, creating additional challenges and (regarding recent technologies) potential risks, especially if they are not known or understood by most users. In his article "*The Myth of the Superuser: Fear, Risk, and Harm Online*", Ohm cautions against laws and regulations that are addressed at risks created by a legendary, omnipotent, malevolent "superuser", who seldom exists in practice.[76] In the recent case of *Richard v. Time Inc.*[77], the Supreme Court of Canada rendered judgment on the rules governing false and misleading representations under Quebec's *Consumer Protection Act*. The Court held that the test to use to determine if the advertising was misleading was not what a consumer of average intelligence, scepticism and curiosity would understand from the commercial representation, but rather what a credulous and inexperienced consumer would comprehend. If a consumer of average intelligence has a difficult time understanding recent technologies, whether consent obtained under PIPEDA can be considered meaningful seems clearly debatable.

Tene and Polonetsky have voiced their concern with the fact that typically, individuals (i.e. users of average intelligence) get privacy defaults wrong;[78] disseminate content more broadly than they intended or is advisable for their own good;[79] forget passwords or keep them listed on unencrypted files

[74] Policy and Research Group of the Office of the Privacy Commissioner of Canada, *The Internet of Things An introduction to privacy issues with a focus on the retail and home environments*, (Ottawa: Office of the Privacy Commissioner of Canada, February 2016) [Policy and Research Group of the Office of the Privacy Commissioner of Canada (2016)].

[75] Technology Analysis Branch of the Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You: A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada*, (Ottawa: Office of the Privacy Commissioner of Canada, May 2013); See also Office of the Privacy Commissioner of Canada, *Metadata and Privacy: A technical and legal overview,* (Ottawa: Office of the Privacy Commissioner of Canada, October 2014).

[76] Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, (2008) 41 UC DAVIS L. REV. 1327.

[77] 2012 SCC 8.

[78] Maritza Johnson, Serge Egelman & Steven Bellovin, "Facebook and Privacy: it's complicated" (Paper delivered at the SOUPS '12: Proceedings of the Eight Symposium on Usable Privacy and Security, 2012), available at: <http://www.cs.columbia.edu/~maritzaj/publications/soups12-johnson-facebook-privacy.pdf>; Fred Stutzman, Ralph Gross & Alessandro Acquisti, *supra* note 54.

[79] Kashmir Hill, "Either Mark Zuckerberg got a whole lot less private or Facebook's CEO doesn't understand the company's new privacy settings", *Forbes* (December 10, 2009), available at: <http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-lessprivate-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings>.

on their laptop;[80] and generally struggle to keep up with the astounding surge in digital economy and culture. [81]

In a survey pertaining to whether Canadian consumers believe a "Do Not Track List" would be desirable, the first question asked respondents to identify their level of familiarity with the existence of tracking devices and techniques such as persistent cookies and web beacons. Overall, half of the respondents were not very familiar or not at all familiar with these technologies.[82] More recently, researchers at Carnegie Mellon University investigated the usability of tools to limit OBA. They observed participants' behaviour as they installed and used various privacy tools, including opt-out tools, browser settings and cookie blockers, and recorded their perceptions and attitudes about those tools, finding serious usability flaws in all nine tools examined.[83] The researchers concluded, "There are significant challenges in providing easy-to-use tools that give users meaningful control without interfering with their use of the web. Even with additional education and better user interfaces, it is not clear whether users are capable of making meaningful choices about trackers."[84]

In a recent complaint filed with the FTC in the U.S. by three advocacy organizations, demanding that it investigate and impose drastic requirements on entities involved in online data analytics and behavioural advertising, it was argued that the "compilation and analysis of data on users in real time involve highly sophisticated data mining technologies that few users—and likely regulators!—understand."[85]

A main concern is that these issues are even more challenging with recent technologies, such as wearable computing, which refers to everyday objects and clothes, such as watches and glasses, in which sensors may be included to extend their functionalities.[86] As a matter of fact, smartphones and mobile apps introduce additional privacy challenges, and some have noted that comparatively smaller screens and other device restrictions constrain how users can be given notice about and control over data practices.[87] The FTC has also recently articulated a similar concern:

> "Privacy notices are not only relevant for websites, mobile apps, or surveillance cameras, but for the whole gamut of systems and devices that process user information. Designing and providing appropriate notices for novel systems, such as

[80] Cormac Herley, P. C. van Oorschot & Andrew Patrick, "Passwords: If We're So Smart, Why Are We Still Using Them?" in Roger Dingledine, Philippe Golle, eds, *Financial Cryptography and Data Security*, (Washington D.C.: Springer, 2009) 237.

[81] Omer Tene & Jules Polonetsky, "A Theory of Creepy: Technology, Privacy and Shifting Social Norms", (2013) 16 Yale Journal of Law & Technology 59 [Omer Tene & Jules Polonetsky].

[82] Janet Lo, *supra* note 32, at 10; The responses varied, with 20% of total respondents very familiar, 30% of respondents somewhat familiar, 19% not very familiar and 31% not at all familiar with the technologies.

[83] Pedro Leon et al., "Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising", *Proc. CHI 2012,* ACM Press 2012, 589.

[84] See also: Omer Tene & Jules Polonetsky, *supra* note 81, at 26.

[85] US, Federal Trade Commission, *In the Matter of Realtime Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy, Complaint, Request for Investigation, Injunction, and Other Relief: Google, Yahoo, PubMatic, TARGUSinfo, MediaMath, eXelate, Rubicon Project, AppNexus, Rocket Fuel, and Others* (Washington D.C., April 2010).

[86] Article 29 Data Protection Working Party (2014), *supra* note 4, at 5.

[87] Florian Schaub et al., *supra* note 18, at p. 1.

> smart home appliances or wearable devices, is challenging.[88] The straightforward approach is to decouple the privacy notice from the system. For example, many manufacturers of fitness tracking devices provide a privacy policy on their websites, while the actual device does not provide any privacy notices.[89] As a result, users are less likely to read the notice and may therefore be surprised when they realize that their mental models do not match the system's actual data practices".[90]

In Europe, the Article 29 Working Party has also raised its concerns with the quality of user consent in light of wearable computing and IoT:

> "Wearable devices such as smart watches are also not noticeable:[91] most observers may not distinguish a normal watch from a connected one, when the latter may yet embed cameras, microphones and motion sensors that can record and transfer data without the individuals being aware of, and even less consenting to such processing. (…) Such situations lead to the question of whether the user's consent to the underlying data processing can then be considered as free, hence valid under EU law. In addition, classical mechanisms used to obtain individuals' consent may be difficult to apply in the IoT, resulting in a "low-quality" consent based in a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. In practice, today, it seems that sensor devices are usually designed neither to provide information by themselves nor to provide a valid mechanism for getting the individual's consent."[92]

More and more data exchanges are now taking place without the knowledge of users, which makes it difficult for organizations to achieve meaningful consent under PIPEDA.

[88] Federal Trade Commission (2015), *supra* note 65.

[89] S. R. Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" (2014) 93:85 *Texas Law Review* 176.

[90] Federal Trade Commission (2015), *supra* note 65.

[91] As described in Opinion 02/2013 on apps on smart devices, wearable computing also highlights challenges stemming from continuous data collection from others within close proximity and for extended periods of time.

[92] Article 29 Data Protection Working Party (2014), *supra* note 4, 7.

2. ADDRESSING CHALLENGES WITH THE CONSENT MODEL: A FEW CONSIDERATIONS

A consent-based privacy protection framework recognizes the subjective nature of privacy, and in any given context, allows individuals to decide for themselves what information they provide, for what purposes it can be used, and with whom it can be shared. At the same time, it is important to recognize the limits of such a consent-based protection regime. As discussed in previous section 1, to a certain extent, the premise of consent is a legal fiction: while individuals are concerned about their privacy, it has been authoritatively argued that they are generally lost in the plethora of different privacy policies, or worse, simply do not read them nor understand them. Privacy policies have become long and complicated documents, placing too high a burden on users to read, understand, and then exercise meaningful choices based on them.

Consent is also challenged by technological changes. Seeking consent is simply not practical or possible in certain circumstances, due to an inability to communicate with the individual. For example, personal information is collected by IoT-networked devices without any user interface. Consent-based privacy controls may also be ineffective if individuals do not have any meaningful control over the communication or capture of their information. The incidental creation and transmission of metadata that accompanies an individual's actions (such as sending an e-mail) is one example. The observation of individuals in public spaces (such as being captured on surveillance video while in a store) is another.

The limits of the consent-based regime will be put to the test even more in coming years. More and more, new technology causes radical evolutions in the ways individuals deal with, use and share personal information about themselves. In some cases, seeking consent may not be practicable or indeed even possible. With recent technological changes, some believe that there are essentially no longer any proponents of the pure notice-and-choice model, as it is regarded as no longer adequate.[93]

While there are various challenges confronting the "notice and choice" model, some also have argued that we should not be abandoning the "control" concept of privacy, and concurrently, the "notice and choice" model, for many reasons.[94] The need for some sort of global consistency in the data protection arena should also be considered.[95] The threat of loss of trade as a result of Directive 95/46/EC and its adequate protection requirements was a strong motivating factor for the Canadian Government's decision to enact PIPEDA.[96] Moreover, many believe that this conception is still relevant nowadays.

[93] See comments made by Daniel J. Weitzner, a senior policy official at the National Telecommunications and Information Administration of the Commerce Department, discussed in Steve Lohr, "*Redrawing the Route to Online Privacy*" *The New York Times* (27 February 2010): available at: <http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html>.

[94] Eloïse Gratton (2013), *supra* note 9; E. Ramirez, *Privacy and the IoT: Navigating policy issues* (CES Opening Remarks, 2015), FTC public statement: "However, just abandoning the concept of notice is not a viable option, as the transparency notices should provide is essential for users, businesses, and regulators alike", discussed in Florian Schaub et al., *supra* note 18, at 2.

[95] See Jose Vilches, "Google proposes global privacy standard" *Techspot* (14 September 2007), available at: <http://www.techspot.com/news/27032-google-proposes-global-privacy-standard.html>; See also Microsoft Corporation, *Microsoft Response to the Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data* (31 December 2009) at 8-9, available at: European Commission <http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/organisations/microsoft_corporation_en.pdf> , see comment of AT&T Inc., cmt. #00420, at 12-13; Comment of IBM, cmt. #00433 at 2, see also Comment of General Electric, cmt. #00392, at 3 (encouraging international harmonization), discussed in Federal Trade Commission (March 2012), *supra* note 38, at 9.

[96] See Steve Coughlan et al., "Global reach, Local Grasp: Constructing extraterritorial jurisdiction in the Age of Globalization", (2007) 6 CJLT 29, at 33.

Some argue that in the Information Age, with so much data available, "control over personal information" is more relevant than ever and that privacy is about "control".[97] Calo, for a variety of reasons, believe that the form of privacy disclosure is worthy of further study before we give in to calls to abandon notice as a regulatory strategy in privacy.[98]

This section 2 will not be proposing solutions to address each of the challenges detailed in section 1. Instead, this section will provide a few considerations which may be relevant if the current notice and choice model is maintained. More specifically, this section will discuss the fact that we need to be careful before considering amending PIPEDA on the issue of consent. It will also address the increasingly important role of policy development and guidance, which may also address the uncertainty surrounding the notion of meaningful consent and provide guidelines to address some of the challenges discussed in section 1. This section will also address the increasingly important role played by the interpretation of the notion of consent, and propose an interpretation that focuses on providing notices and choices to information or situations meant to be protected by PIPEDA, thereby limiting the number of consents obtained and concurrently, the "privacy policy fatigue" concerns already discussed.

2.1 Amending PIPEDA with Caution

Before considering amending PIPEDA, we first need to determine if the challenges now confronting the consent model, which are further discussed in section 1, can be addressed by modifying the language used in PIPEDA on the issue of consent or by making any other type of amendment to the law. If the answer is no (or if it is not clear), the law should not be amended.

PIPEDA was recently amended through Bill S-4, the *Digital Privacy Act*, to include certain provisions which were necessary: to provide for an exception for business transactions and to better reflect the reality of the relationship between employer and employees.[99] The *Digital Privacy Act* also amended PIPEDA to include a revised "valid consent" provision (PIPEDA, s. 6.1), by shifting from a subjective standard to a more objective standard.[100] Some have already voiced their opinion on the fact that before amending PIPEDA with respect to the notion of consent, we should determine what the problem is and whether the proposed amendments would address the relevant concern.[101] While there are many

[97] Peter Fleischer, ""The data deluge" Peter Fleischer: Privacy…?" (21 April 2010), available at: <http://peterfleischer.blogspot.com/2010/04/data-deluge.html?spref=tw>. See also Bruce Schneier, "*Privacy and Control*" *Schneier on Security* (6 April 2010), available at: <http://www.schneier.com/blog/archives/2010/04/privacy_and_con.html>.

[98] Ryan Calo (2012), *supra* note 22, at 1027.

[99] It was also amended to include an exception to the notice of consent in cases in which private sector organizations may wish to share personal information in specific cases in which they are investigating fraud; Éloïse Gratton, *Personal submission to the CAI pertaining to potential amendments to the Quebec private sector law, the Act respecting the protection of personal information in the private sector* (November 27, 2015), available at: <http://www.eloisegratton.com/files/sites/4/2015/12/Monsieur-Jean-Chartier-CAI-27-novembre-2015-2.pdf> [Éloïse Gratton, November 27, 2015].

[100] New section 6.1 of PIPEDA is clarifying that an individual's consent to the collection, use or disclosure of his or her personal information is valid only "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."

[101] Éloïse Gratton, *Bill S-4: My Appearance Before the Industry Committee* (March 26, 2015), available at: <http://www.eloisegratton.com/blog/2015/03/26/bill-s-4-my-appearance-before-the-industry-committee/>: "Still, I have a few concerns with this proposal. PIPEDA currently requires that consent be reasonably understandable by the individual. The questions that should be asked are: (i) Do we have a concern with this consent requirement? and if so, (ii) will the proposed

challenges with the notion of valid consent under PIPEDA, for the reasons discussed in section 1, it is not clear if such changes (i.e. new section 6.1) will be addressing the problems discussed in section 1. Moreover, such amendments might even be creating uncertainty for businesses that have been interpreting the notion of consent reflected in PIPEDA a certain way for the last ten to fifteen years.

Jean Carbonnier, one of the most important French jurists of the 20th century, has articulated the view that we should be nervous when enacting or amending laws ("Ne légiférer qu'en tremblant").[102] As a matter of fact, before amending a law, one should be careful to make sure that the amendment will not be detrimental or problematic as soon as new technologies emerge. Given that such amendments will be relatively permanent and allow less flexibility, this may be problematic, since PIPEDA was meant to be technology-neutral, and flexible enough to account for technological developments, new business models and the reasonable expectations of individuals, which is an evolving concept.

This section will discuss the fact that we need to be careful before amending PIPEDA given that PIPEDA, which incorporates the FIPPs, was meant to be technology-neutral and flexible. Moreover, this section will also discuss how before amending PIPEDA, we have to account for the fact that social norms pertaining to new technologies or business models may not necessarily be in place.

2.1.1 PIPEDA to Remain Technology Neutral

Data protection laws such as PIPEDA were initially drafted in order to address the management and handling of personal information in electronic form. The Article 29 Working Party states:

> "It is useful to recall that the reasons for enacting the first DPL in the seventies stemmed from the fact that new technology in the form of electronic data processing allows easier and more widespread access to personal data than the traditional forms of data handling."[103]

The initial concern was that individuals were going to lose control over their personal information since their data, once in electronic form, would become more easily shared among organizations from the private and public sectors, sometimes without the individual's knowledge.[104] In fact, the FIPPs were initially meant to apply only to electronic data, and this distinction (electronic data vs. non electronic data) is still present in certain data protection laws.[105] This distinction (paper vs. electronic) may have made sense forty years ago when data was passing from the "paper" form to an "electronic" one and was therefore to be shared more easily. More recently, however, this distinction is no longer present and certain data protection laws even have provisions for technology-neutral application. For example,

---

amendment address such concerns. If the proposed amendment is accepted, the message sent to organizations is that the way they used to get consent may no longer valid, and that perhaps they should be taking additional steps."

[102] Vincent Gautrais & Pierre Trudel, *Circulation des Renseignements Personnels et Web 2.0* (Montréal: Éditions Thémis, 2010) at 2: "Le doyen Carbonnier considérait qu'il 'fallait légiférer en tremblant'" [Vincent Gautrais & Pierre Trudel].

[103] Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", 01248/07/EN WP 136 at 5 [Article 29 Data Protection Working Party (2007)].

[104] Eloïse Gratton (2013), *supra* note 9, Section 1.1.2 "*Control over Personal Information and Fair Information Practices*", at 6.

[105] For instance, Directive 95/46/EC makes a distinction between the processing of personal data by automatic means and the processing of personal data by non-automatic means. EC, *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [1995] O.J., L. 281/31 at Whereas (27); See also Article 29 Data Protection Working Party (2007), *supra* note 103, at 5.

PIPEDA states that "organizations shall protect personal information regardless of the format in which it is held".[106] Furthermore, PIPEDA is based on flexible principles in Schedule 1, rather than on prescriptive rules. This translates into a piece of legislation able to accommodate various industries and new technologies, and it can therefore be considered as a technology-neutral legislation.

A general principle of lawmaking is that the law should be sustainable. It is obvious that nowadays, technology develops much more quickly than the law does.[107] Laws should be sustainable enough to cope with technological development over a sufficiently long period of time. If a law is too technology-specific, it is not likely to cover future technological developments, and it will therefore have to be amended often.[108]

We should ensure that PIPEDA remains as technology-neutral as possible.[109] European legal scholar Koops suggests that regulation should be technology-neutral in its effects.[110] Koops also argues that "the more detailed the legislation, the less transparent it may be and, particularly with technology, it will be the case that the more technology is put into the law or into its formulation, the less understandable it will be to ordinary citizens."[111] If we can find a way to work with the current provisions of "consent" from PIPEDA, which we arguably can with the necessary policy guidance and the right interpretation (see sections 2.2 and 2.3 which elaborate on these issues), then perhaps we should move forward with the current consent approach.

PIPEDA is meant to reach the proper balance between protecting the privacy of individuals and the need of organizations to collect, use or disclose personal information for the purposes that a reasonable person would consider appropriate in the circumstances.[112] The wording pertaining to obtaining consent under PIPEDA is technology-neutral, and it should remain that way. In the event that certain new technology or business models warrant a more specific type of consent, additional guidance should be provided at the policy level.[113]

2.1.2 PIPEDA to Remain a Flexible Law

In the 1970s, as the FIPPs were being established and data protection laws began to emerge in certain jurisdictions, it was already very clear that a certain flexibility was required and necessary in the application of FIPPs. For instance, the Lindop Report in the U.K. explained that the FIPPs were drafted in

---

[106] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, at Schedule 1 (s. 5), principle 4.7.1.

[107] Bert-Jaap Koops, "Should ICT Regulation be Technology-Neutral?" in Bert-Jaap Koops et al., eds., *Starting points for ICT regulation: Deconstructing prevalent policy one-liners*, coll. IT & Law Series, vol. 9, (2006) The Hague: TMC Asser 77 [Bert-Jaap Koops].

[108] *Ibid*, at 10.

[109] According to Vincent Gautrais, it would be in many cases impossible to have perfect technology neutrality. See Vincent Gautrais, *Neutralité technologique: Rédaction et interprétation des lois face aux technologies* (Montréal : Éditions Thémis, 2012).

[110] Bert-Jaap Koops, *supra* note 107, at 6.

[111] *Ibid,* at 12.

[112] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, s.3.

[113] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, s. 2.2.1 and 2.2.2 which elaborate on the type of guidance provided by the OPC on the issue of valid consent and transparency.

broad terms, specifically in order to provide some type of flexibility.[114] Too much specificity in defining the objectives of the FIPPs could lead to a loss of flexibility and laws incorporating these FIPPs were therefore to be as flexible as possible.[115]

As early as the 1970s, businesses and various organizations were already raising warning flags over potential restrictions to their data processing activities, if the objectives of the FIPPs were to be given a strict, literal interpretation.[116] In answer to these concerns, certain documents from the 1970s emanating from European jurisdictions illustrate that the FIPPs and their underlying obligations on users were to be imposed only "as far as reasonably practicable".[117] Clearly, the original intention was not to ensure that every conceivable data handling activity be covered:

> "We believe that regulation should be as light and as flexible as possible, and exercised with any stringency only where there is a special need to overcome substantial risks for the citizen's privacy. Our recommendations for the scope of the statute, for the powers of the DPA and for the form of the statutory guidelines are therefore deliberately cast widely. This is not because it is our intention that every conceivable data handling activity should be capable of accommodating the changes in the automatic handling of personal information which will occur during its foreseeable lifetime."[118]

More specifically, great importance was attached to flexibility in the application of the principles of FIPPs, as evidenced by a report dating back from this period which mentions that: "the appropriate level of compliance with each applicable principle will vary for different information systems which handle personal data in different ways and for different purposes."[119]

The main purpose of adopting a very broad yet flexible legislation (through data protection laws) was therefore initially meant to ensure that the law would keep up with technological developments.[120] This

---

[114] Chairman Sir Norman Lindop, *Report of the Committee on Data Protection: Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty* (London, UK: H.M.S.O., 1978), at 199, para. 21.04 [Chairman Sir Norman Lindop]; See also *ibid*. at 148, para. III.04.

[115] This is now the case with PIPEDA, which is very flexible, as it is based on a standard.

[116] Chairman Sir Norman Lindop, *supra* note 114, at 200, para. 21.05: "The great majority of users who commented on the objectives set out in paragraph 34 of the White Paper were concerned to explain to us the problems which would be imposed on their data processing activities if those objectives were to be strictly applied, across the board, to everyone and with literal adherence to their wording."

[117] *Ibid*. at 199, para. 21.04.

[118] *Ibid*. at 147, para. III.04.

[119] *Ibid*. at 202, para. 21.15.

[120] *Ibid*. at 13, para. 3.04: "Because the lifetime of the legislation on which we are asked to advise will be substantial, we have informed ourselves both about the current state of the art and about foreseeable developments in it, to ensure that the legislation will not need to be amended by reason of technical changes alone." See also *ibid*. at 18, para. 3.21: "We took these considerations into account when deciding upon our recommendations for data protection legislation. An approach which would have been appropriate in 1970 and 1975 would not be suitable for the technology of 1980 and 1985. Technological developments are happening with increasing speed and economy; this requires flexibility in the mechanics of control to allow new potential threats to be contained."

being said, the interpretation of the FIPPs was crucial and would largely determine the effect of their objectives as implemented.[121]

PIPEDA provides flexibility on the form of the consent sought by an organization. For instance, consent may vary, depending upon the circumstances and the type of information:[122] An organization should generally seek express consent when the information is likely to be considered sensitive; implied consent would generally be appropriate when the information is less sensitive.[123] Moreover, in obtaining consent, the "reasonable expectations" of the individual are also relevant.[124] The form of consent in other data protection laws, such as Quebec's *Act Respecting the Protection of Personal Information* in *the Private Sector*, which provides that consent be "manifest", has been criticized for not being flexible enough on the notion of consent.[125]

Under principle 3 of Schedule 1 of PIPEDA, which deals with consent, the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, "except where inappropriate." This principle includes a note which further explains the fact that it may be *impossible or impractical* to seek consent in cases involving legal, medical or security reasons; that obtaining consent *might defeat the purpose* of collecting the information when information will be used for the detection and prevention of fraud or for law enforcement; that seeking consent may be *impossible or inappropriate* when the individual is a minor, seriously ill, or mentally incapacitated. Moreover, the note raises the fact that organizations that *do not have a direct relationship with the individual* (i.e. direct marketing organizations) may not always be able to seek consent.

To add to PIPEDA's flexibility, under article 5 (3), there is a catch-all reasonableness test, which dictates the limits of PIPEDA applicability: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." This provision applies even if consent was obtained from users,[126] therefore allowing any additional privacy risk to be addressed.

PIPEDA, in its current form, therefore provides for great flexibility on the issue of "consent". It may be considered as flexible enough to accommodate new types of technologies and business models under which, in light of the ubiquity of the data exchange taking place and the number of players involved, consent would be considered as *impossible* or *inappropriate*, if the activity is *reasonable* and in line with the user's *reasonable expectations*. If the notion of consent under PIPEDA is flexible enough, no amendments should be made at this time to specifically accommodate new technologies or business practices.

---

[121] *Ibid*. at 45-46, para. 5.34.

[122] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, Schedule 1, s. 4.3.4, 4.3.6.

[123] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, Schedule 1, s. 4.3.6.

[124] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, Schedule 1, s. 4.3.5.

[125] See Éloïse Gratton (November 27, 2015), *supra* note 99.

[126] Philippa Lawson & Mary O'Donoghue, "*Approaches to consent in Canadian data protection Law*", *Lessons from the identity trail,* 2009, available at: <http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_02.pdf>.

2.1.3 Amendments to Consider the Evolution of Social Norms

The privacy policy is only one piece of the consent puzzle: in order to assess the legitimacy of data practices, some argue that regulators should analyze *users' expectations* rather than corporate statements.[127]

Under PIPEDA, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.[128] Also, in determining the form of consent to use, organizations shall take into account the "reasonable expectations" of the individual.[129] What these expectations are in any given context, and whether certain activities are legitimate from a privacy perspective, is often a function of many factors, including the social norms that are in place at the relevant period of time and which norms may affect the users' expectations regarding such new technology or business practices.

Some of these so-called privacy social norms are intuitive. For example, everyone knows that facing other passengers in an elevator violates a certain social norm and therefore, elevator passengers will usually face the doors until they reach their destination.[130] Instinctively, passengers will often even move in the elevator as other passengers leave or enter, to ensure that they are leaving others as much space as possible (i.e. to re-equilibrate the shared space).

Social norms are constantly evolving and individuals may even sometimes change their mind on whether a technology violates their privacy. For instance, it is reported that when ID caller was launched in the late 1980s, many people thought it to be a privacy violation to see who was calling a person, to the point where some U.S. states regulated against it.[131] Today, many users refuse to answer the phone if the number is not displayed on their caller ID, and therefore this technology is now considered a privacy-enhancing technology.[132]

The law and social norms will always lag behind technology. A good example to illustrate this statement is cameras and the evolving social norms around them. In 1890, U.S. law students Samuel Warren and Louis Brandeis invented the modern legal right to privacy, in their famous article about the "Right to be alone", in reaction to the threat of "instantaneous photography" in the popular press which was then invading the sacred precincts of private and domestic life.[133] Still, it took another 70 years for the U.S. to elaborate relevant common law privacy torts.[134] More recently, the ubiquity of cameras on mobile phones (most cell phones now have embedded cameras) has created a new distortion, and the social

---

[127] Larry Downes, *A Rational Response to the Privacy "Crisis"*, Cato Institute Policy Analysis, January 7, 2013, available at: <http://www.cato.org/publications/policy-analysis/rational-response-privacycrisis:>.

[128] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, Schedule 1, s. 5(3); In Europe, legitimate interests are relevant when assessing lawful processing: see Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 844/14/EN WP 217.

[129] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, Schedule 1, s. 4.3.5.

[130] Omer Tene & Jules Polonetsky, *supra* note 81, at p. 11.

[131] Steven Oates, "Caller ID: Privacy Protector or Privacy Invader", 1992 U. ILL. L. REV. 219.

[132] Omer Tene & Jules Polonetsky, *supra* note 81, at p. 11.

[133] Samuel Warren & Louis Brandeis, *supra* note 2; It has led the *New York Times* in 1902 to decry "Kodakers lying in wait".

[134] William L. Prosser, "Privacy", 48 CAL. L. REV. 383 (1960); also see *Restatement (Second) of Torts* § 652D (1976).

norm surrounding cameras is, once again, not quite in place. While walking around a gym's locker room with a digital camera in hand would probably be violating a social norm and be considered inappropriate, given that these functionalities are relatively recent, many still continue to carry around their phones in locker rooms. This has led certain gyms to post signs warning that cellphone cameras should not be used in locker rooms.[135]

We can also consider that a new innovative technology such as Google Glasses, could be used inappropriately or against social norms. Polonetsy suggests that users, who have yet to figure out which pictures to share on Facebook or how to make sure they do not tweet while drunk, are now required to navigate a whole new map of social rules with this recent technology, designed to let users search as they walk, navigate, record what they see in real time and share it with their friends:

> "Should you take off your Google Glass in a public restroom, lest other visitors think you are recording? Is it acceptable to Google someone while speaking to them? (…) In this case, the potential lurch threatens the privacy not of the early new product adopters but rather of those who will be observed and recorded. Will users of Google Glass manage to conduct their activities while respectful of existing social norms, perhaps following a newly invented code of etiquette, or can we expect disruptions and dismay such as those caused by early "Kodakers"?" [136]

Google's Executive Chairman Eric Schmidt has also raised the fact that "people will have to develop new etiquette to deal with Google glasses that can record video surreptitiously and bring up information that only the wearer can see. There are obviously places where Google Glasses are inappropriate."[137]

In some situations, corporate behaviour may be labeled as pulling against social norms. These cases or behaviours do not necessarily involve a breach of the law. They may instead involve the deployment of a new technology or some new use of an existing technology, the implementation of a new feature or program, or an unexpected data use or customization.[138]

Examples of recent new technologies which illustrate a social norm not yet entrenched include social listening, which is the analysis by organizations of social media content for sentiment analysis, customer service and early crisis warning.[139] A recent study comprising surveys of more than 1,000 customers has confirmed that a double standard was evident for social media listening, since perceptions of social

---

[135] Catherine Saint Louis, "Cellphones Test Strength of Gym Rules", *New York Times* (December 7, 2011), available at: <http://www.nytimes.com/2011/12/08/fashion/struggle-to-ban-smartphone-usage-ingyms.html>.

[136] Jules Polonetsky, "When Do You Take Off Your Google Glasses?", *LinkedIn Influencers* (February 21, 2013), available at: <http://www.linkedin.com/today/post/article/20130221045735-258347-when-doyou-take-off-your-google-glasses>.

[137] Aaron Pressman, "Google's Schmidt says talking to glasses can be weird, inappropriate", *Reuters* (April 25, 2013), available at: <http://www.reuters.com/article/2013/04/25/us-google-harvard-idUSBRE93O1FF20130425> (speaking at Harvard University's Kennedy School of Government.)

[138] Omer Tene & Jules Polonetsky, *supra* note 81, at p. 2.

[139] *See, e.g.*, Marshall Sponder, *SOCIAL MEDIA ANALYTICS: EFFECTIVE TOOLS FOR BUILDING, INTERPRETING, AND USING METRICS* (McGraw-Hill, 2011); Stephen Rappaport, *LISTEN FIRST!: TURNING SOCIAL MEDIA CONVERSATIONS INTO BUSINESS ADVANTAGE* (Wiley, 2011).

media-based customer service were clearly ambivalent amongst surveyed individuals.[140] More specifically, the survey results illustrated that while companies were getting credit from about half of their customers for being responsive to consumer sentiment, half of their customers also felt that a corporate response was "creepy" and preferred being able to just vent off some air on social media, without the organization responding.

Another recent example to illustrate the fact that a new business practice may violate social norms pertains to British Airways and its "Know Me" program, recently launched and intended to provide a more personalized service to frequent fliers.[141] Under this program, airline personnel were instructed to google passengers' names to learn more about them and provide them with a personalized greeting and experience. Many British Airways customers felt that it was inappropriate for agents to find information about them online for such purposes. Interestingly, with the social norm evolving around personalized services, a customer could eventually expect to receive this kind of personalization by an airline company that he or she frequently uses or, worse yet, be offended that with all the information available on the web, his or her preferred airline does not provide a more personalized experience or that his or her preferences must be repeated on each flight (i.e. "Don't you know who I am by now?").

In 2012, the New York Times Magazine ran a cover story about Target, assigning customers with a "pregnancy prediction score," based on their purchase habits, in order to beat its competitors in identifying a precious moment when shopping habits are most amenable to change – the birth of a baby.[142] Target had employed statisticians to sift back through historical buying records of women who had signed up for baby registries, discovering latent patterns. They were able to determine a set of products that, when grouped together, allowed Target to accurately predict a customer's pregnancy and due date.[143] While this marketing operation by Target was highly criticized by the public,[144] it also raises the fact that the reasonable expectations of the user are quite relevant when assessing the type of consent that should be obtained in a given context. For instance, while customers may not expect that their purchases will be compiled to determine and assign them a pregnancy score, they may expect to receive advertising for baby products upon subscribing to a pregnancy and newborn magazine.

PIPEDA provides that the "reasonable expectations" of the individual be considered when determining the form of consent to use in a given situation. While this expectation threshold may vary and could be considered as subjective, it also introduces additional flexibility into the notion of consent reflected in PIPEDA. Moreover, this flexibility is quite useful when we need to consider the social norms (including

---

[140] Brian Solis, "Are Businesses Invading Consumer Privacy By Listening to Social Media Conversations?", *Brian Solis Blog* (February 25, 2013), available at: <http://www.briansolis.com/2013/02/arebusinesses-invading-consumer-privacy-by-listening-to-social-media-conversations>; For original study *see* Netbase & J.D. Power, "SOCIAL LISTENING V. DIGITAL PRIVACY", (February 12, 2013), available at: <http://www.slideshare.net/secret/NqlMQFvbATIfLX> .

[141] Tim Hume, "BA Googles passengers: Friendlier flights or invasion of privacy?", *CNN* (August 22, 2012), available at: <http://edition.cnn.com/2012/08/22/travel/ba-google-image-passengers>.

[142] Charles Duhigg, "How Companies Learn Your Secrets", *New York Times Magazine* (February 16, 2012), available at: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

[143] *Ibid*.

[144] *See, e.g.*, Matt Stanford, "Brilliantly *Creepy: Marketing Technology and Your Privacy"*, *Experts-Echange* (February 21, 2012), available at: <http://blog.experts-exchange.com/ee-tech-news/brilliantly-creepymarketing-technology-your-privacy>; also see Kashmir Hill, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did", *Forbes*, February 16, 2012, available at: <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girlwas-pregnant-before-her-father-did>.

the reasonable expectations of users pertaining to a specific technology or business practice) in place at any given time, given that these norms are constantly evolving.

Social norms take some time to become stable. Any amendment to the law (i.e. PIPEDA) on the issue of consent pertaining to a specific technology or business model would necessarily have to take into account the fact that social norms in connection with such new technology or business practice may not yet be firmly established.

The prudent approach may dictate ensuring that the law will not be amended at a time when the social norm in connection with a new technology or business practice is not yet etched in stone. In the past, privacy values and norms took years or even centuries to develop.[145] The reality is that, more and more, only very short timeframes are available for society and the law to react to technological innovation. According to Tene and Polonetsky, as technological innovation accelerates, so does the need to recalibrate individual expectations, social norms and ultimately laws and regulations, although it is not clear how we should regulate in the absence of stable social norms:

> "Another is the lingering indecision among policymakers with respect to the role of regulation in the absence of stable social norms. Should restrictions on conduct be based on law or on "softer" social norms? Should regulation drive or be driven by volatile individual expectations, market best practices and social norms? Should we wait for norms to develop to form societal expectations?" [146]

Shifting social norms, combined with powerful business interests and technological developments, threaten to make laws irrelevant. This should be considered before deciding to amend PIPEDA on the notion of "consent" or to amend it in order to address a specific technological development. For example, the EU "cookie directive", which requires websites to obtain users' affirmative opt-in consent before placing a cookie on their machine, has been considered by many as out of sync with technological and business realities: individuals simply do not want to be obstructed from reaching their online destination by repetitive notices and prompts for consent.[147]

While PIPEDA should not be amended at a time when the social norm in connection with a given new technology or business practice is not yet fully defined, since the notion of "consent" under PIPEDA is quite flexible, a lot of uncertainty also surrounds what type of consent is adequate upon such new technology or business model being developed. In order to address this uncertainty, the OPC will have to continue playing an important role in casting some light on some of challenges pertaining to the notion of meaningful consent. Moreover, interpreting this notion of consent in a balanced way may be part of the solution, as further discussed in the following sections.

2.2 Increased Role of Research and Policy Development

Section 2.1 discusses how we should be careful before amending PIPEDA on the issue of consent; especially given that PIPEDA is very flexible on that issue and neutral from a technology standpoint. With

---

[145] Omer Tene & Jules Polonetsky, *supra* note 81, at p. 10.

[146] *Ibid*.

[147] *Ibid*, at p. 13. In addition, these authors contend that it is quickly becoming technologically obsolete with the development of server-side surveillance mechanisms such as browser fingerprinting. See Electronic Frontier Foundation, Panopticlick: *How Unique – and Trackable – is Your Browser?*, available at: <https://panopticlick.eff.org>.

this flexibility also comes huge uncertainty. As a matter of fact, there are many downsides of having such a flexible framework. For one, when new practices and business models make their appearance, the industry has to wait for the OPC to provide guidance on what is considered legal and legitimate from a "consent" point of view. Moreover, it should be noted that the type of consent to be obtained under PIPEDA is directly linked to the notion of "sensitivity", which is also a flexible notion (i.e. PIPEDA states that any information may be sensitive depending on the context), which spawns additional uncertainty. This, further linked with the "reasonableness test",[148] triggers the situation in which there is so much uncertainty for organizations when innovating, that for some, launching a new product or program may not be worth the risk of receiving a negative finding confirming that their practice is not legal from a "consent" standpoint.

Since PIPEDA features so much uncertainty regarding what type of consent should be considered as adequate as new technologies and business models are developed, policy guidance will be increasingly necessary on the issues of enhanced transparency, valid consent, as well as with respect to users' expectations, as discussed below.

2.2.1 Guidance on Enhanced Transparency

Section 1 discusses how privacy policies have, to a certain extent, failed to provide users with meaningful insight into corporate data management practices. With new and complex technologies, how to properly disclose data management practices is more and more challenging. Therefore, policy direction from the OPC has been, and will continue to remain, necessary, in order to assist organizations to better explain their practices to users, in a more understandable way, so as to ensure that truly meaningful consent is elicited from them.

Recently, the *Digital Privacy Act* (Bill S-4) provided for a revised "valid consent" provision, by shifting from a subjective standard to a more objective standard. Section 4.3.2 of Schedule 1 from PIPEDA requires that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. New section 6.1 clarifies that an individual's consent to the collection, use or disclosure of his or her personal information is valid only:

> "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."

Since this section is new, and since there are many challenges in connection with providing adequate policies (and obtaining meaningful consent), any guidance would most probably be welcomed to determine to what extent organizations should be reviewing and updating their privacy policies to ensure compliance with this new requirement.

This guidance may generally take the form of reports and publications, such as reports to Parliament, audit or accountability reports and similar publications. For instance the OPC published, in 2012, a useful guide entitled "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps, Reports and

[148] PIPEDA provides a "reasonableness" test (s. 5 (3) under which "an organization may collect, use or disclose personal information *only for purposes that a reasonable person would consider are appropriate in the circumstances*", which is also relatively subjective).

Publications",[149] providing valuable input on the issue of transparency (and on obtaining meaningful consent), despite the small screen challenge.[150]

Scholars in multiple disciplines have explored shortening privacy policies or otherwise changing their format to reduce the burden on consumers and avoid discouraging users from reading them. The FTC, in a recent report, suggested that: "privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[151]

Wearables, such as Google Glasses, may incidentally collect information about bystanders. Social media and mobile applications enable users to share information with and about others, e.g., by tagging someone in a geo-referenced photo. These technologies may therefore collect information from different types of users. Understanding which audiences have to be addressed by privacy policies should be considered.[152] This is increasingly important in light of complex technologies involving many players. For instance, while determining a website's audience may be straightforward (typically, the visitors of the website), mobile applications, wearables, smart cars, or smart home appliances expand the audiences and user groups that need to be considered. Such systems may have a primary user, but potentially also multiple users with different privacy preferences.[153]

Some are proposing multi-layered and contextualized notices, since it has been reported that stating everything at once in a single notice is rarely effective.[154] Timing of the notices is also crucial,[155] providing information about a specific data practice when it becomes relevant for the user.[156] For example, notice could be provided when a system is used for the first time, or when a data practice is active, for example when information is being collected, used, or shared. It was also suggested that notices be "context dependent", meaning that the user's and system's context be considered to show additional notices or controls, if deemed necessary. For instance, some locations may be particularly sensitive; therefore users may appreciate being reminded that they are sharing their location in a given context.[157] It was further proposed that notices be "periodic" (since periodic reminders of data practices

[149] Office of the Privacy Commissioner of Canada, "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps", *Office of the Privacy Commissioner of Canada - Reports and Publications* (October 2012), available at: <https://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf>.

[150] Advice include layering the information, such that important details are up front in the developer's privacy policy and also embed links to the details of your privacy rules so that those who want more detail can find it. The OPC further recommends providing a privacy dashboard and discusses how the timing of user notice and consent is critical.

[151] Federal Trade Commission (March 2012), *supra* note 38, at viii, 61.

[152] R. Calo, *supra* note 22, at 1072.

[153] For example, a home lock automation system may collect information about all family or household members, including guests. See Florian Schaub et al., *supra* note 18, at 4.

[154] *Ibid*, at p. 5; Article 29 Data Protection Working Party, *Opinion 10/2004 on More Harmonised Information Provisions*, WP 100.

[155] R. Balebako, "Mitigating the Risks of Smartphone Data Sharing: Identifying Opportunities and Evaluating Notice", PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 2014; S. Egelman et al., "Timing is everything?: the effects of timing and placement of online privacy indicators", in *Proc. CHI '09*, ACM, 2009; N. S. Good et al., *Noticing notice: a large-scale experiment on the timing of software license agreements*, in *Proc. CHI '07*, ACM, 2007; S. Patil et al., "Reflection or action ? : How feedback and control affect location sharing decisions", in *Proc. CHI '14*, ACM, 2014.

[156] Federal Trade Commission, *Mobile privacy disclosures: Building trust through transparency* (FTC staff report, Feb. 2013).

[157] F. Schaub, B. Konings, & M. Weber, *"Context-adaptive privacy: Leveraging context awareness to support privacy decision making",* (2015) 14(1):34 *IEEE Pervasive Computing* 43; See Florian Schaub et al., *supra* note 18, at 7.

can further help users maintain awareness of privacy-sensitive information flows), with the sensitivity of the data practice determining the appropriate frequency.[158]

Auditory notices may also be considered. Visual notices (text, images, icons, or a combination thereof) may play more and more of an important role.[159] For example, the advertising industry has developed self-regulatory programs to govern advertisements online: the Digital Advertising Alliance of Canada (DAAC) encourages organizations to provide notice of advertising practices to Internet users, and an ability to opt out of OBA programs, and the core feature of the program is the AdChoices icon.[160]

Moreover, many privacy policies inform about data management practices but do not offer any real choices. It has been suggested that whenever possible, privacy policies should not only provide information about data management practices, but also include privacy choices or control options, since they make the information actionable:

> "Using a website, an app, a wearable device, or a smart home appliance is interpreted as consent to the data practices regardless of the user having seen or read them. Even if notices are seen by users, they largely describe a system's data practices, with few choices to opt-out of certain practices, such as sharing data for marketing purposes. Thus, users are effectively left with a take-it-or-leave-it choice give up your privacy or go elsewhere. Users almost always grant consent if it is required to receive the service they want. In the extreme case, privacy notices are turned into mere warnings that do not empower individuals to make informed choices (e.g., "Warning: CCTV in use" signs). Yet, privacy notices can only be effective if they are actionable and offer meaningful choices. Awareness of data practices can enable users to make informed privacy decisions, but privacy controls are needed in order to realize them."[161]

Another issue is the fact that too many choices create a similar burden for individuals, with a similar perverse effect. Facebook has been criticized for providing too many choices.[162] By offering too many choices, individuals are likely to choose poorly.

As new technologies and business models evolve, policy direction will become even more important to ensure that industry players are guided on how to develop and deploy new technologies and practices, in order to ensure compliance with PIPEDA on the issue of consent. Certain authors have recently evaluated the transparency of various policies and propose that their score system for the *Model Privacy Form* be used as a benchmark standard for acceptable ambiguity, against which other policies should be measured.[163] They believe that regulators may wish to present new scores and thresholds that companies can seek to achieve through better policy language that consumers can understand. Given

---

[158] Florian Schaub et al., *supra* note 18, at 7.

[159] *Ibid*, at p. 9.

[160] The icon tells consumers that participating companies adhere to an accepted set of principles that provide consumers with transparency and control over interest-based ads and allows consumers to opt out from this type of advertising if they choose.

[161] Florian Schaub et al., *supra* note 18, at 2. See also Fred Cate (2010), *supra* note 19; L.F. Cranor (2012), *supra* note 17.

[162] Chris Jay Hoofnagle, *supra* note 68; It was reported that a previous Facebook privacy policy provided for 50 different settings and 170 different options.

[163] Joel R. Reidenberg et al., *supra* note 23, 28.

that providing useful notices and obtaining valid consent is becoming more complex, it has also been suggested by some that a Privacy Impact Assessment (PIA) be performed before developing a privacy policy.[164]

2.2.2 Guidance on Valid Consent

Direction and guidance on how organizations can elicit meaningful consent will be increasingly necessary. This may include guidance and information provided by the OPC, for instance, in the form of interpretation bulletins, guidance information and tools. For example, the OPC, over the last few years, has provided guidance on the notion of "consent", through a document entitled "Determining the appropriate form of consent under the *Personal Information Protection and Electronic Documents Act*"[165] and the Interpretation Bulletin entitled "Form of Consent".[166] both of which are available on its website. After the evidence before the Standing Committee on Access to Information, Privacy and Ethics pointed to the difficulties faced by Canadians when they are asked to provide their knowledge and consent for social media contracts and agreements,[167] the OPC, in May 2014, published *Guidelines for Online Consent*,[168] as well as *Frequently Asked Questions for Online Consent.*[169]

On the issue of OBA, the OPC has published various useful documents, including the 2011 *Guidelines on Privacy and Online Behavioural Advertising*,[170] and a *Policy Position on Online Behavioural Advertising*[171] in June 2012, which documents have been updated as of December 2015. While follow-up investigations have provided even more concrete information on how the OPC's position on consent in the context of OBA practices should be applied in practice,[172] organizations have, since 2012, already had a good idea as to how the OPC would consider OBA practices and the type of consent which would be acceptable. In

[164] See Florian Schaub et al., *supra* note 18, at 3; Article 29 Data Protection Working Party (2014), *supra* note 4, at. 21.

[165] Office of the Privacy Commissioner of Canada, "Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act", *Guidance and Information* (September 2004), available at: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_24_e.asp>.

[166] Office of the Privacy Commissioner of Canada, "Form of Consent", *Interpretation Bulletin*, available at: <https://www.privi.gc.ca/leg_c/interpretations_07_consent_e.asp>.

[167] *Privacy and Social Media in the Age of Big Data: A Report of the Standing Committee on Access to Information, Privacy and Ethics* (April 2013) available at: <http://www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf>.

[168] Office of the Privacy Commissioner of Canada, "Guidelines for Online Consent", *Guidelines* (May 2014), available at: <https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp>.

[169] Office of the Privacy Commissioner of Canada, "Frequently Asked Questions for Online Consent", *Guidelines* (May 2014), available at: <https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_faq_e.pdf>.

[170] Office of the Privacy Commissioner of Canada, "Guidelines on Privacy and Online Behavioural Advertising, Guidance and Information", *Guidelines* (2011), available at: <https://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf>.

[171] Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising", *Guidelines* (June 2012) available at: <https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp>.

[172] PIPEDA Report of Findings #2012-001, *Social networking site for youth, Nexopia, breached Canadian privacy law*; PIPEDA Report of Findings #2014-001, *Use of sensitive health information for targeting of Google ads raises privacy concerns*, January 14, 2014; PIPEDA Report of Findings #2014-011, *Investigation into the personal information handling practices of Ganz Inc.*, October 7, 2014.

2014, the OPC also published its position on the issue of genetic test results, concluding that such results should not be used for insurance purposes.[173]

These types of position papers will be increasingly important, in view of the complexity of recent technologies and business models, since knowing "up front" how to deploy a new technology or program, what type of consent would be considered as adequate, and whether the organization would be considered as having legitimate interests, will be most helpful. As a matter of fact, the OPC will usually react once a complaint is filed against an organization. For the organization that has to wait for a finding to be issued following a complaint and an OPC's investigation, uncertainty ensues for a certain period of time. For instance, after Bell announced the imminent launch of its RAP program in the fall of 2013,[174] it had to postpone implementation of the program for the duration of the OPC's investigation. Given that the finding pertaining to this program was released only in April 2015,[175] for a period of 18 months, no other businesses launched any innovative, targeted marketing program, given the uncertainty surrounding the consent issue involved with these types of programs. Moreover, the risks associated with PIPEDA's ombudsman model are increasing. In some cases, upon findings issued by the OPC concluding that the organizations concerned should have obtained consent, or that the type of consent obtained was inadequate, privacy class actions were filed against those organizations.[176] Given that privacy class actions are on the rise in Canada,[177] businesses have every incentive to ascertain *ahead of time* (i.e. *a priori*), whether their new technology or program is compliant with PIPEDA's consent provisions.

One downside from organizations not being able to know what type of consent is legal under PIPEDA before launching a new technology or program is that it may affect innovation. Following the OPC's decision pertaining to the Bell RAP, no other relevant advertising programs have been launched in Canada. Perhaps no other organization is willing to take the risk, given the uncertainty around what type of program would require which type of consent. As a matter of fact, we should be mindful of the fact that while flexibility around the notion of consent under PIPEDA is necessary, this flexibility is also triggering uncertainty which may, in turn, affect or have an impact or innovation and/or the launch of new technologies and programs. Providing more policy guidance ahead of time, and before any complaint is filed against a new technology or practice, should therefore be considered seriously.

Another issue germane to this point is that the OPC's findings on the issue of consent are increasingly complex, probably reflective of the complexity of many new technologies and business models.[178] For

---

[173] Office of the Privacy Commissioner of Canada, *Statement about the use of genetic test results by life and health insurance companies* (July 10, 2014), available at: <https://www.priv.gc.ca/media/nr-c/2014/s-d_140710_e.asp>.

[174] Office of the Privacy Commissioner of Canada, *Announcement: Privacy Commissioner to investigate Bell Canada's privacy policy changes* (October 23, 2013).

[175] Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2015-001*, *Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program* (April 7, 2015) [PIPEDA Report of Findings #2015-001].

[176] For example, many class actions have been filed after the OPC releasing a negative finding, including class actions against Google and Bell; See Éloïse Gratton, *2015 Privacy Class Actions in Canada*, available at: <http://www.eloisegratton.com/blog/2015/06/23/2015-privacy-class-actions-in-canada/>.

[177] Borden Ladner Gervais LLP, *Top 10 Legal Risks for Business in 2016*, raising that "*Privacy Class Actions are on the Rise in Canada*", at 3, online <http://www.blg.com/en/NewsAndPublications/Documents/2016_Top_10_Business_Issues.pdf>.

[178] See for example PIPEDA Report of Findings #2015-001**,** *supra* note 175; See also PIPEDA Case Summary #2009-004, *supra* note 34.

instance, in the recent RAP decision, the OPC found that express (opt-in) consent was required, given the sensitivity of the information involved[179] and the reasonable expectations of customers, as determined by four contextual factors surrounding the RAP, which had to be "*considered in combination and in concert with each other*".[180] It may be a difficult task for an organization to determine what are these expectations, if, for instance, only one criterion is removed. For instance, it is yet to be determined if a similar decision would have been reached by the OPC on the consent issue, if the organization in question was not enabling the delivery of third party advertising, but was instead promoting its own products and services.

In February 2016, the OPC released its paper on the IoT,[181] which addresses the fact that this technology poses challenges for the consent model. More specifically, the OPC states that it has identified challenges with the consent model as an issue under its "Economics of Privacy" priority and has adopted a strategy to identify, explore and validate enhancements to the consent model, so that concerns raised both by individuals and organizations are addressed.

In terms of the type of guidance which may be useful, we can think of guidance on business models involving location tracking and analytics (bluetooth, beacons, etc.), as well as consent in connection with wearables. More guidance would also be useful on the issue of de-identification (i.e. at what point is information no longer subject to PIPEDA).[182] This last issue is quite important, as it may determine the type of consent necessary for new types of analytics business models.

Following the issuance of a policy statement by the OPC, follow-ups should be made to determine if the industry is complying with the recommendations and if not, what are the underlying reasons for not doing so.[183] This may be an indication that the industry is having a hard time complying with PIPEDA and the OPC's recommendations, due to various reasons, such as the complexity of the implementation of the guidance in practice, etc. Also, this notion of consent under PIPEDA, which has to consider the "expectations of users", triggers the situation under which the OPC's position may evolve over time, for

[179] The RAP was using sensitive URLs for the purpose of generating customer profiles was taken into account. In the OPC's view, the sheer breadth of information being used or contemplated for the RAP (including internet, telephone and television network usage information, as well as account/demographic information) rendered such information more sensitive when compiled.

[180] See for example PIPEDA Report of Findings #2015-001**,** *supra* note 175: More specifically, the OPC considered that the telco: (i) began using information it already collected for the purposes of delivering its primary services for the new secondary purpose of delivering behaviorally targeted ads; (ii) delivers paid services, for which customers may pay up to hundreds of dollars per month; (iii) was enabling the delivery of third-party ads; and (iv) is a telecommunications service provider to whom users must entrust vast amounts of their sensitive personal information in order to gain access to mobile, internet, telephone and television communications in Canada.

[181] Policy and Research Group of the Office of the Privacy Commissioner of Canada (2016), *supra* note 74.

[182] It is not clear at what point information qualifies as "personal information". Many authors have proposed framework to address this concern. See Ira Rubinstein & Woodrow Hartzog, "Anonymisation and Risk", (2015) 6:2 Washington Law Review 2016; Eloïse Gratton, "If Personal Information is Privacy's Gatekeeper, then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information", Albany Law Journal of Science and Technology, Vol. 24, No. 1, 2013 [Éloïse Gratton, Albany Law Journal of Science and Technology (2013)]; Paul Schwartz & Daniel Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 N.Y.U. Law Review 1814.

[183] Office of the Privacy Commissioner of Canada, "Online Behavioural Advertising (OBA) Follow Up Research Project", *Report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada* (June 2015), available at: <https://www.priv.gc.ca/information/research-recherche/2015/oba_201506_e.pdf>; For instance, after the OPC issued its position on this issue of consent in the context of OBA in 2012, it then followed up with a report entitled "*Online Behavioural Advertising (OBA) Follow-Up Research Project*" in June 2015, in which it notes that advertising practices may not be consistent with the OPC's recommendations.

instance as the social norms around a given technology or practice also evolve. For example, the OPC was cautious enough, in its position on genetic testing results, to make it clear that "recognizing that the state of medical technology is changing rapidly, this position should be revisited on a periodic basis".[184] This also means that if a finding is issued on a given business practice, but the expectations of users have evolved over time, a process under which the OPC may "update" some of its previously published position or findings should be considered and implemented.

Finally, the feasibility should be explored of a system or process under which organizations can, on a voluntary, and perhaps even on an anonymous, basis (if possible), test and validate their methods of consent, especially if these are creative and innovative, or if they pertain to an upcoming launch of a new technology or practice.[185] This would allow organizations to ensure that they are complying with PIPEDA and interpreting its consent provisions adequately.

2.2.3 Guidance on Consumers' Expectations

PIPEDA is quite flexible on the issue of consent and states that in obtaining consent, the "reasonable expectations" of the individual are relevant.[186] Surveys on consumer attitudes towards specific technologies, business models and privacy may reveal valuable information, including whether individuals understand certain technologies, as well as whether they consider them to be either useful or harmful. Moreover, these studies may provide valuable information on users' attitudes, including whether such attitudes may be different when it comes to information privacy, depending on the audience concerned.[187]

As discussed in section 2.1.3, what these reasonable expectations are in any given context, and whether certain activities are legitimate from a privacy perspective, are often a function of many factors, including the social norms that are in place at the relevant period of time. In order to determine what these expectations are, in light of new technologies and business models, some type of guidance and research will be welcome, if not necessary. This may include privacy research, conducted or commissioned by the OPC, and contributions program information and research.

For instance, in the spring of 2010, the OPC held consultations with Canadians on online tracking, profiling and targeting, and cloud computing. It received numerous written submissions and held public events in Toronto, Montreal and Calgary, the goal being to learn more about certain industry practices, explore their privacy implications, and find out what privacy protections Canadians expect with respect to these practices. In October 2010, the OPC released a draft report[188] and later published its final

---

[184] Office of the Privacy Commissioner of Canada, *Statement on the use of genetic test results by life and health insurance companies* (July 10, 2014), available at: <https://www.priv.gc.ca/media/nr-c/2014/s-d_140710_e.asp>.

[185] Some have been proposing stronger "accountability" mechanisms under which organizations will demonstrate compliance with their current legal obligations, which could be considered, in some circumstances, as a substitution for informed consent. While these mechanisms should be further explored, they do not address the uncertainty around what would constitute a meaningful consent upon a new technology being commercialized or business practices adopted.

[186] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, Schedule 1, s.4.3.5.

[187] See for example, Hoofnagle, Chris Jay, King, Jennifer, Li, Su and Turow, Joseph, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (April 14, 2010), available at: <http://ssrn.com/abstract=1589864>.

[188] Office of the Privacy Commissioner of Canada, *Draft Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing* (October 25, 2010), available at: <https://www.priv.gc.ca/resource/consultations/report_2010_e.pdf>.

report,[189] summarizing what the OPC had gleaned from the submissions, the public discussions, as well as the feedback received, on the draft report. This type of exercise will be increasingly important and necessary going forward and perhaps, whether private sector organizations or industry associations should play a more active role in conducting these consumer researches and bearing the related costs (similar to the role played by pharmaceuticals in clinical trials) should be further explored.

Even more on point, the OPC has conducted much research and many public opinion surveys over the years, which are available on its website.[190] In more recent years, the OPC commissioned Harris/Decima, in 2011, to undertake a survey of Canadians, to gauge their understanding and awareness of privacy issues, legislation and federal privacy institutions, particularly in each of four priority areas: information technology and privacy, national security and privacy, identity integrity and protection, and genetic privacy.[191] The OPC also commissioned Phoenix Strategic Perspectives Inc., in 2012 and 2013, to conduct a survey of Canadians on privacy-related issues and, more specifically, to explore Canadians' awareness, understanding and perceptions of such issues. [192] In 2015, the OPC commissioned Nielsen Consumer Insights to prepare a report based on qualitative research, exploring Canadians' immediate and emerging privacy concerns.[193]

Consultations and public opinions and surveys are playing, and will continue to play, an increasingly important role, allowing us to better understand consumers and their expectations with regard to more recent technologies and business practices. Thus they will help evaluate adequately how the social norm in connection with a given technology or business practice is evolving.

2.3 Increased Role of Interpretation

This section discusses the fact that the challenges with our consent-based model can potentially be addressed through policy guidance and the proper interpretation of the already flexible notion of "consent". Using an approach under which the notion of consent will be interpreted in light of the technology or business model at stake, as well as the privacy concerns pertaining to such technology or business practice has various benefits. It is always less disturbing to provide a solution which can be incorporated within the current legal framework, such as a proposed interpretation and guidelines, than to propose a new amendment to the law.[194]

---

[189] Office of the Privacy Commissioner of Canada, *Final Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing* (May 2011), available at: <https://www.priv.gc.ca/resource/consultations/report_201105_e.pdf>.

[190] available at: <https://www.priv.gc.ca/information/02_05_c_e.asp>.

[191] Harris/Decima, "2011 Canadians and Privacy Survey, Public Opinion Surveys", *Final Report for The Office of the Privacy Commissioner of Canada* (March 31, 2011), available at: <https://www.priv.gc.ca/information/por-rop/2011/por_2011_01_e.asp>.

[192] Phoenix Perspectives Strategic Inc., *Survey of Canadians on Privacy-Related Issues*, (Final report prepared for the Office of the Privacy Commissioner of Canada, January 2013), available at: <https://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.asp>; Phoenix Perspectives Strategic Inc., *Survey of Canadians on Privacy-Related Issues*, (Final report prepared for the Office of the Privacy Commissioner of Canada, December 2014), online:<https://www.priv.gc.ca/information/por-rop/2015/por_2014_12_e.asp>.

[193] The Nielsen Company, *Nielsen Consumer Insights, Exploring the Privacy Concerns and Priorities of Canadians, Public Opinion Surveys,* (Final Research Report prepared for the Office of the Privacy Commissioner of Canada, February 2015, available at: <https://www.priv.gc.ca/information/por-rop/2015/pcp-can_201503_e.asp>.

[194] Vincent Gautrais & Pierre Trudel, *supra* note 102, at 2: "Le doyen Carbonnier considérait qu'il 'fallait légiférer en tremblant'".

As discussed above, the notion of "consent" under PIPEDA is already quite flexible and is technology-neutral, allowing for this concept to be interpreted. This means that the OPC will be playing an important role in ensuring that the notion of consent is interpreted, maintaining the proper balance between the protection of privacy, on the one hand, and, on the other, the need for organizations to collect, use or disclose personal information for the purposes that a reasonable person would consider appropriate in the circumstances. This interpretation should also consider the impact of a given decision on innovation, as well as ethical issues that may go beyond PIPEDA compliance. The adoption of a new risk-based approach should also be taken into account.

2.3.1 Considering the Impact on Innovation

Many authors outline the benefits of a society dominated by open information flows.[195] Personal information is necessary to provide and obtain public services.[196] We can think of the value in collecting, sharing and disclosing personal information in order to address national security concerns or to investigate and prosecute criminal activities. The free flow of data would also be important to economic efficiency, as it would enable cost cutting in the private and/or public sector (by eliminating various inefficiencies).[197] For example, individuals with bad credit could be identified more easily, thereby protecting lenders, as well as the financial system (i.e. the collective).[198] Personal information would be increasingly used in healthcare, particularly in research and large-scale epidemiological studies.[199]

Technological advances also provide for new ways to address health trends at an early stage. For example, Google makes it possible to use its search engine, in correlation with the geographical region examined (using IP addresses), in order to detect regional flu outbreaks early on. A few years ago, Google launched a "Flu Trends" service,[200] which is basically a site that monitors increases in health-related searches in different parts of the world, which can accurately predict the outbreak of a flu epidemic in a certain region, long before public health authorities even suspect its existence.[201]

In 2009, Hal Varian, Google's chief economist, published a paper showing that Google searches can also be used to predict a bevy of economic data, including retail sales[202] and unemployment claims.[203] There

[195] Fred H. Cate, "The Changing Face of Privacy Protection in the European Union and the United States", (1999) 33 Ind. L. Rev. 173, at 174; Pierre Trudel & Karim Benyekhlef, "Approches et Stratégies pour Améliorer la Protection de la Vie Privée dans le Contexte des Inforoutes", in *Mémoire présenté à la Commission de la Culture de l'Assemblée Nationale dans le Cadre de son Mandat sur l'Étude du rapport quiquennal de la commission d'accès l'information* (Montréal : CRDP, Université de Montréal, 1997) at 4; See also Vincent Gautrais, "Introduction générale: Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle" (2004) 9:2 Lex Electronica at 7-8.

[196] Vincent Gautrais & Pierre Trudel, *supra* note 102, at 3.

[197] Neil Robinson et al., *Review of the European Data Protection Directive* (Santa Monica, CA: RAND Corporation, 2009) at 13 [Neil Robinson et al.].

[198] Ron A. Dolin, "Search Query Privacy: The Problem of Anonymization" (2010) 2:2 Hastings Science and Technology Law Journal 137, at 144 [Ron A. Dolin].

[199] E.g. see CNIL, *2008 Annual Report of the Commission Nationale de l'Informatique et des Libertés* (Paris: CNIL, 2008) at c. 1 "Measuring Diversity: Ten Recommendations", discussed in Neil Robinson et al., *supra* note 197, at 14.

[200] See available at: <http://www.google.org/flutrends/>.

[201] Ron A. Dolin, *supra* note 198, at 143.

[202] Hal Varian & Hyunyoung Choi, "Predicting the Present with Google Trends" *Google Research Blog* (2 April 2009), available at: <http://googleresearch.blogspot.com/2009/04/predicting-present-with-google-trends.html>.

[203] *Ibid*.

may also be an interest in Google's ability to analyze search logs, to detect large-scale computer security threats.[204] It has also been argued that preserving, and not anonymizing, online search queries would be ultimately beneficial to society.[205] Substantive restrictions may impede innovation, leading to fewer useful services, or else privilege one technology over another.[206]

Data collection can also promote innovation.[207] It has been argued that blocking Google from collecting and analyzing information about its users would be a negative outcome, and that Google's best products (including the spell checker) would not be possible without users' data.[208] Location data is also quite valuable and serves many purposes.[209] By collecting and analyzing location information, Google has been able to create real-time traffic reports on highways and even surface streets.[210] Location information pertaining to individuals, collected over time, may have the potential to provide traffic engineers and planners with rich data feeds necessary to promote optimal traffic flows and would also allow them to efficiently allocate transportation resources and to properly reroute traffic in emergency situations.[211] Today, some offline businesses follow consumers around shopping malls, using their cell phone signals or other methods similar to the way online businesses track online users.[212] Consumers currently live in a world in which television commercials differ by household and billboards change with the radio habits of drivers.[213] Information means knowledge, which in turn can promote the innovation of science and technology and benefits for society as a whole.[214]

The knowledge gained by organizations using analytics solutions so as to better understand the behaviour of their users may, in certain cases, be translated into direct or indirect benefits for consumers. Direct benefits could potentially include personalised services, products and advertising

---

[204] Farhad Manjoo, "No More Privacy Paranoia, Want Web companies to stop using our personal data? Be ready to suffer the consequences" *Slate* (7 April 2011), available at: <www.slate.com/articles/technology/technology/2011/04/no_more_privacy_paranoia.html?wpisrc=newsletter_tis> [Farhad Manjoo].

[205] Ron A. Dolin, *supra* note 198, at 143.

[206] *See* Ian Ayers & John Braithwaite, *Responsive Regulation* 4 (1992), at 4, discussed in Ryan Calo (2012), *supra* note 22, at 1048-1049.

[207] See also Neil Robinson et al., *Review of the European Data Protection Directive* (Santa Monica, CA: RAND Corporation, 2009) at 13. See also Farhad Manjoo, *supra* note 204.

[208] *Ibid*.

[209] Dave Barth, "The Bright Side of Sitting in Traffic: Crowdsourcing road congestion data" *Official Google Blog* (25 August 2009), available at: <http://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html>.

[210] Farhad Manjoo, *supra* note 204.

[211] U.S., Federal Communications Commission, *In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles: Intelligent Transportation Society of America Reply Comments* (WT Docket No. 01-72) (Washington, D.C.: 24 April 2001) at 7 [FCC].

[212] See, e.g., Keith Wagstaff, "Will Your Mall Be Tracking Your Cellphone Today?", *TIME* (Nov. 25, 2011), available at: <http://techland.time.com/2011/11/25/will-your-mall-be-tracking-your-cellphonetoday/>; See also Elizabeth Dwoskin, "What Secrets Your Phone is Sharing About You", *Wall Street Journal* (January 17, 2014).

[213] See, e.g., Robert Salladay, "High-Tech Billboards Tune In to Drivers' Tastes: Roadside Signs Coming to Bay Area Listen to Car Radios, Then Adjust Pitch', *S.F. CHRON.* (Dec. 22, 2002), at A1 (discussed in Ryan Calo, *Digital Market Manipulation*, 82 George Washington Law Review 995 (2014), at p. 1015 [Ryan Calo (2014)]).

[214] Eloïse Gratton (2013), *supra* note 9, at 60: See section 2.1.1.1.1. entitled "*Ignoring the Importance of Information Flow for Society*" which elaborates on the value of having personal information free flow in our society.

enabling online businesses to offer the right services to the right users at the right times.[215] Indirect benefits could see organizations upgrading their current products and services based on their users' needs, developing new products and deploying new applications and services, or the "repackaging" certain products and services. This could mean that their users might only be charged for the services that they actually use, instead of sponsoring other users' usage of certain services in which they have no interest (thus potentially reducing costs for those users).

Another point is that requiring that individuals be entitled to give the most stringent form of consent (i.e. express consent) may also negatively impact innovation. Some readers may recall that in the past, when users logged onto Facebook, all they could see was their face, *i.e.*, their own profile. To view another user's news, they had to actively enter that other user's profile. It was only when Facebook launched its News Feed feature in 2006, and data started flowing that users became accustomed to the change, which is viewed today as an indispensable service. According to certain authors, Facebook's News Feed may have struggled if asked to obtain individuals' prior opt-in consent to data practices which were truly innovative, unanticipated and therefore out of context.[216] In fact, many Facebook users initially reacted negatively to the introduction of *News Feed*, criticizing the changed user experience.[217] Once they adjusted to this change in context, however, *News Feed* became a vital part of the Facebook experience, driving user engagement and playing a crucial role in spreading information globally. Downes observes that today's privacy crisis is a function of innovation that happens too quickly and that the accelerating pace of new information technology introductions, new uses of information, usually, after the initial panic, users almost always embrace the service that once violated their visceral sense of privacy.[218]

Big Data could be considering as challenging PIPEDA's principles of purpose limitation and data minimisation. Under s. 4.3.3 of PIPEDA, an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes.[219] Some have raised their concern with the interpretation of this principle that may have a negative impact on innovation.[220] That being said, the OPC's interpretations of this principle, and of the notion of meaningful consent when evaluating new business models, have considered innovation. For instance, in CIPPIC complaint against Facebook, the OPC took into account the fact that Facebook is free to users, and that since advertising is essential to the provision of the service, individuals who wish to use the service must be willing to

[215] Benefits include remembering customization settings, making product recommendations based on the user's previous purchases or browsing history, developing and improving the website to increase its usability for users and customizing how information is displayed on websites to appeal to each user's tastes. Behavioural advertising provides benefits to consumers in the form of free web content and personalized advertisements or by displaying more relevant advertisements that reflect the user's interests.

[216] Omer Tene & Jules Polonetsky, *supra* note 81, at 23-24.

[217] Michael Arrington, "Facebook Users Revolt, Facebook Replies", *Techcrunch* (September 6th, 2006), available at:<http://techcrunch.com/2006/09/06/facebook-users-revolt-facebook-replies>; John Leyden, "Facebook mods controversial 'stalker-friendly' feature", *The Register* (Sept. 8, 2006), available at: <http://www.theregister.co.uk/2006/09/08/facebook climbdown>.

[218] Larry Downes, "A Rational Response to the Privacy "Crisis"", *Cato Institute Policy Analysis* (January 7, 2013), available at: <http://www.cato.org/publications/policy-analysis/rational-response-privacycrisis>.

[219] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, Schedule 1, s. 4.3.3.

[220] Eloïse Gratton, *Personalization, Analytics and Sponsored Services: The Challenges of Applying to Online Tracking and Profiling Activities*, Canadian Journal of Law and Technology (Thompson-Carswell, November 2010).

receive a certain amount of advertising.[221] The OPC, in a recent decision, has further recognized the organization's valid business objective to generate increased advertising revenue, and determined that a relevant advertising program did not represent a use of customers' personal information for an "inappropriate purpose."[222] These interpretations are definitely good news for innovation innovative business models.

Tene and Polonetsky argue that the ingenuity of the FIPPs, which has made them resilient to momentous change, lies in their flexibility: some principles retract, while others expand, depending on the circumstances. They explain how, in the context of Big Data, this means relaxing data minimization and consent requirements, while emphasizing transparency, access and accuracy.[223] This reasoning should be considered when evaluating consent in connection with business analytics.

When it comes to business analytics, we should consider whether innovation would be negatively impacted by interpreting the notion of consent so that the mere act of analyzing personal information, even on an aggregated basis (i.e. anonymous information), would be considered a new "use" of information, therefore requiring prior consent. Such an interpretation should instead focus on whether the analysis is done on an individual basis vs. whether it is done on an anonymous basis. If the analysis is conducted using an adequate level of aggregation, (i.e. the information is anonymized and therefore no longer subject to PIPEDA), it may not require prior consent.[224] At the same time, consent could be required at the point where the information is then *used* to take a decision pertaining to an individual. For instance, the OPC's research paper on predictive analytics explains how intelligent predictive analytics could potentially be used as a basis for discriminatory outcomes and infringements on the right to equal treatment.[225] In the U.S., the FTC issued a Big Data report in January 2016, in which it advocates that when sensitive information is used in Big Data, steps should be taken to ensure that the information is not employed for potentially harmful purposes, such as to support eligibility decisions (affecting entitlement to credit, employment, insurance, housing, government benefits, and the like).[226] Big Data techniques and the general knowledge gained on consumers can be used against individuals, either to market to them[227] or to take eligibility decisions impacting them.[228] While Big Data has led to useful and innovative advances and benefits for society, the potential exists for information to be misused in ethically questionable ways, as discussed in the next section.

---

[221] PIPEDA Case Summary #2009-008, *supra* note 47.

[222] PIPEDA Report of Findings #2015-001**,** *supra* note 175.

[223] Omer Tene & Jules Polonetsky, *supra* note 81, at 5.

[224] Deciding otherwise may trigger the situation under which even anonymizing data may be considered a new use which would require prior consent.

[225] The Research Group at the Office of the Privacy Commissioner of Canada*,* "The Age of Predictive Analytics: From Patterns to Predictions" (August 2012), available at: <https://www.priv.gc.ca/information/research-recherche/2012/pa_201208_e.pdf>.

[226] US, Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* (January 2016), at 24, available at: <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf> [FTC (January 2016)].

[227] The information could be used in online advertisements based on racial profiling as discussed in Latanya Sweeney, *Discrimination in Online Ad Delivery*, (Harvard University, January 28, 2013), available at: <http://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf>.

[228] See FTC (January 2016), *supra* note 226; See also Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values*", The White House (*May 2014), available at: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

2.3.2 Considering Ethical Issues

The argument has been raised that language is not the only means to convey information, nor is it always the most efficient.[229] As a matter of fact, there is extensive evidence that individuals (i.e. test subjects) react in specific, predictable ways to certain kinds of visual and audio cues, irrespective of their underlying familiarity with technology.[230] Organizations could leverage these techniques to provide better user understanding. At the same time, organizations could also start looking at consumer behaviour datasets to identify consumer vulnerabilities. As a matter of fact, emerging methods of Big Data present a new and vastly more efficient way to identify cognitive bias, by attempting to pinpoint profitable anomalies.[231] One example is with consent and default settings: it is known that if consumers must opt out of data collection instead of opting in, more data will end up being collected, as users hold to the status quo.[232] To illustrate this point further, it is interesting to note that in countries where organ donation is on an opt-in basis, donation rates tend to be very low, compared to countries that are culturally similar but have an opt-out regime.[233]

Alessandro Acquisti and his colleagues at Carnegie Mellon, which are behavioural economists focusing on privacy issues, have demonstrated how knowledge of bias and design psychology make it possible to modulate the amount of information that people are willing to disclose.[234] They found, in a recent experimental study, that, paradoxically, more control over the publication of users' private information decreases their privacy concerns and increases their willingness to publish sensitive information, even when the probability that strangers will access and use that information stays the same or, in fact, increases.

Calo, in his article entitled *Digital Market Manipulation*,[235] also cites interesting studies in which researchers and others have realized that people's biases lead them to give up more personal information than they would, absent the manipulation.[236] He refers to this type of practice as *Disclosure Ratcheting*. For instance, studies reveal that people value their privacy more if they already have it than if they must acquire it, and will pay more to protect information from a third party than they will accept to sell it.[237] Moreover, one experiment suggests that making a website more casual in appearance, as opposed to formal, makes subjects more likely to admit to controversial behaviour such as cheating or

[229] Ryan Calo (2012), *supra* note 22, at 1034.

[230] Ryan Calo (2012), *supra* note 22, at 1038.

[231] Ryan Calo (2014), *supra* note 213.

[232] There is a revealing set of graphs in a 2012 communications paper showing how personal disclosure on the social network Facebook was trending fairly sharply downward until, around 2009, the company changed some of its privacy defaults. See Fred Stutzman et al., "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook", 4:2 J. PRIVACY & CONFIDENTIALITY 7, at 17, available at: <http://repository.cmu.edu/jpc/vol4/iss2/2/>. From that point on, disclosure began steadily to climb again.

[233] Omer Tene & Jules Polonetsky, *supra* note 81, at 24.

[234] Laura Brandimarte and Allesandro Acquisti, *Misplaced Confidences: Privacy and the Control* Paradox, 4 SOC. PSYCHOL. & PERSONALITY SCI. 340, 340-47 (2013). *Ibid*, discussed in Ryan Calo (2014), *supra* note 213, at 1013.

[235] Ryan Calo (2014), *supra* note 213, at 1013.

[236] See, e.g., Alessandro Acquisti & Jens Grossklags, "What Can Behavioral Economics Teach Us About Privacy?", in Alessandro Acquisti et al., eds., 2008 *DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES* 363, at 363–379.

[237] *Ibid*.

drug use.[238] Other experiments have evidenced the manner in which reciprocity (i.e. the questioner offering up information first) increases the likelihood that a subject will answer a personal question, even when the questioner is a computer.[239] For example, Calo explains that if the computer begins with, "I was made in 2007," before prompting the subject with the question, "When were you born?", individuals might be nudged into disclosing information about themselves, perhaps inadvertently.[240] He explains how a company might treat the possibility of leveraging consumer bias to increase self-disclosure. [241]

Can organizations use consumer bias when obtaining consent? Is it ethically acceptable to do so? These questions are also important in light of analytics. For instance, organizations are increasingly analyzing large data sets anonymously, in order to uncover trends. These trends can then be re-applied to individuals in order to elicit consent. For example, AdWeek ran a story a few years ago, entitled "Marketers Should Take Note of When Women Feel Least Attractive", discussing a recent marketing study which purported to show that women feel less attractive on Monday mornings. The article suggested that the results of their studies had implications for marketers and recommended that companies concentrate on these "prime vulnerability moments" to market beauty products to women on Mondays. [242] The advertising strategy attracted many criticisms.[243]

In 2008, U.S. academics revealed the results of their studies: that people are subconsciously swayed by individuals who share their facial features.[244] Again, marketers which know that users are subconsciously attracted to people that look like them could merge the user's face (for instance using their Facebook or Twitter profile picture) with the face of the model used to advertise their product for increased personalization. Some users may be attracted to the advertisement, without realizing that it is because the model advertising the product looks like them. While these practices may not be currently illegal under PIPEDA, they also illustrate how the "consent" and concept of "control" may not catch these types of more ethical issues and that more reflection is necessary on the issue of marketers using known bias or user vulnerabilities without their knowledge, let alone their consent.

Another practice that may raise ethical issues is dynamic pricing, also known as "adaptive pricing", or "discriminatory pricing", a practice whereby organizations attempt to perfectly exploit the differences in price sensitivity between consumers. Dynamic pricing is an old practice that has been around forever,

---

[238] Ryan Calo (2014), *supra* note 213, at 1014, discussing Leslie K. John et al., "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information", (2011) 37 J. CONSUMER RES. 858, at 863–868.

[239] See, e.g., B.J. Fogg & Clifford Nass, "How Users Reciprocate to Consumers: An Experiment That Demonstrates Behavior Change", in (1997) CHI '97 Extended Abstracts On Human Factors In Computing Systems 331, at 331–332, available at: <http://dl.acm.org/citation.cfm?id= 1120419&CFID=391340722&CFTOKEN=55472072>; S. Parise et al., "Cooperating with Life-Like Interface Agents", (1999) 15 COMPUTERS HUM. BEHAV. 123, at 123–142 [S. Parise et al.].

[240] Ryan Calo (2014), *supra* note 213, at 1014 discussing S. Parise et al., *supra* note 239, at 130–31.

[241] Ryan Calo (2014), *supra* note 213, at 1015.

[242] Lucia Moses, "Marketers Should Take Note of When Women Feel Least Attractive - What messages to convey and when to send them", *AdWeek* (April 2, 2013), available at: <http://www.adweek.com/news/advertising-branding/marketers-should-take-note-when-women-feel-least-attractive-152753>.

[243] See Rebecca J. Rosen, "Is This the Grossest Advertising Strategy of All Time?", *ATLANTIC* (Oct. 3, 2013, 1:46 PM), available at: <http://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/>.

[244] Jeremy N. Bailenson et al., "Facial Similarity Between Voters and Candidates causes Influence", (2008) 72:5 Public Opinion Quarterly 935, available at: <http://vhil.stanford.edu/mm/2008/bailenson-facial-similarity.pdf>.

although it is recently making a comeback.[245] With user profiling, consumers can be sorted as individuals or groups by retailers and this makes it possible for retailers to create a pricing scheme tailored to individual users, based on their purchase, online usage or product usage. Many have raised their concerns with online businesses charging certain products differently, depending on the profile of the online user. Adaptive pricing could arguably raise data protection issues, in the sense that personal information (i.e. profile information of a user) is used to take a decision that may have an impact for the individual (i.e. the price offered for a product).[246] Price discrimination could also be considered as raising ethical issues, especially if consumers are left in the dark.

Certain information, which may fall outside the scope of PIPEDA (i.e. the data may not qualify as personal information because it is not associated with any identifiable individual) could nonetheless, in some cases, be used against the individual. For instance, a website that offers certain insurance products could conclude, rightfully or not, that a particular online visitor is afflicted with AIDS, based on the profile information collected by cookies and the websites previously visited, and therefore block that visitor's access to certain sections of its content. Certain type of profile information, which may fall outside the scope of PIPEDA (i.e. "identifiable individual" information) may therefore still be used against the individual behind the profile, for instance to deny certain products or services.[247] In Europe, Article 29 Working Party, has recently suggested amending the current definition of "personal information" to also include "(…) and any information allowing a natural person to be singled out and treated differently"[248] to address this type of concern. New ethical issues that may be beyond those pertaining to the application of PIPEDA and the issue of meaningful consent are nevertheless quite important, and also merit consideration.

2.3.3 Considering a Risk-based Approach

Section 1 illustrates how ineffective privacy disclosures really are, and the problem with a consent-based or a choice-based approach, in view of the number of data exchanges and collections taking place in modern society, the excessive time required to read privacy policies, overly complex technologies, the increasing number of players involved, the ubiquity of data collection practices, and the dynamic nature of business models and, concurrently, of privacy policies.

While the right to privacy is a very important one, the very broad notion of privacy as "control over personal information" (the "control" definition of privacy), which is the basis of data protection laws around the world, including PIPEDA, results in protecting not only the privacy of individuals, but also prohibiting the circulation of any kind of personal information relating to individuals. Some authors have argued that the expansive definition of "personal information" dilutes its effect and undermines its main objective.[249] These authors argue that instead of having data protection laws declare that all personal

[245] Jack Nicas, "Now Prices Can Change From Minute to Minute", *Walt Street Journal* (December 14, 2015), available at: <http://www.wsj.com/articles/now-prices-can-change-from-minute-to-minute-1450057990>.

[246] Frederik J. Zuiderveen Borgesius, "Online Price Discrimination and Data Protection Law" (Conference paper for the Amsterdam Privacy Conference 23-26 October 2015), Amsterdam Law School Research Paper No. 2015-32.

[247] See Eloïse Gratton (2013), *supra* note 9, at section 2.1.2.1.2 entitled "Potentially Under-Inclusive Definition".

[248] Article 29 Working Party, "Opinion 08/2012 providing further input on the data protection reform discussions", 01574/12/EN WP199, at 5.

[249] See Eloïse Gratton (2013), supra note 9, at sections 2.1.1 "Privacy as an Absolute Right" and 2.1.2.1.1 "Potentially Over-inclusive Definition"; See also McKay Cunningham, "Free Expression, Privacy and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship" (2015) Arkansas Law Review [forthcoming], at 30-31 and 35.

information shall be protected, these laws should instead target specific harms that attend specific privacy violations.[250] The current legal framework therefore translates into a burdensome one, under which consents for random data handling activities are being obtained from individuals, while reducing the relevancy of the consents which would in fact be necessary (because of "notification fatigue").

Article 29 Working Party, *Opinion 15/2011 on the definition of consent* has raised that consent is not always the primary or the most desirable means of legitimizing the processing of personal data and that the use of consent "in the right context" is crucial:

> "There is a need to emphasize that consent is not always the primary or the most desirable means of legitimizing the processing of personal data. Consent is sometimes a weak basis for justifying the processing of personal data and it loses its value when it is stretched or curtailed to make it fit to situations that it was never intended to be used in. The use of consent "in the right context" is crucial. If it is used in circumstances where it is not appropriate, because the elements that constitute valid consent are unlikely to be present, this would lead to great vulnerability and, in practice, this would *weaken* the position of data subjects in practice."[251]

The Article 29 Working Party has also been recently exploring the role of a risk-based approach in data protection legal frameworks.[252] Instead of rejecting the notice and choice model, the adoption of an interpretation that limits the notices and choices to more specific information and/or situations meant to be protected by data protections laws such as PIPEDA could be explored. This approach would also be in line with the initial intent of lawmakers at the time of the adoption of data protection laws (incorporating the FIPPs).[253] The idea is to address the challenges brought on by the application of PIPEDA in the context of new technologies and the Information Age with a new interpretation, one that is in line with PIPEDA's ultimate goal.

Data protection laws, such as PIPEDA, regulate the actions of collecting, using and disclosing personal information. Koops suggests that instead of regulating the means (the action itself), we should be regulating functions and effects and that regulation should therefore be focused on the effects of actions.[254] He articulates the view that "of particular importance is exactly what effects must be regulated."[255] Some argue that data protection laws such as PIPEDA were meant to protect individuals against the *risk of harm* to individuals that data management threatens to cause.[256]

Under the proposed framework, before determining if a certain activity should be governed by PIPEDA (and consent being required), one would need to take into account the *risk of harm* to individuals, so

---

[250] *Ibid*. See also Éloïse Gratton, Albany Law Journal of Science and Technology (2013), supra note 182, at 105.

[251] Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", 01197/11/EN WP187, at 10.

[252] Article 29 Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, Adopted on 30 May 2014.

[253] For example, Lindop had raised the fact that the interpretation of the FIPPs was crucial and would largely determine the effect of the objective as implemented. Chairman Sir Norman Lindop, *supra* note 114, at 45-46, para. 5.34.

[254] Bert-Jaap Koops, *supra* note 107, at 6.

[255] *Ibid*.

[256] Eloïse Gratton (2013), *supra* note 9.

that principles such as notice, disclosure and consent may become more efficient.[257] Data protection laws such as PIPEDA generally provide that individuals be told who is collecting their data and the purpose of such collection, so as to enable them to decide whether to release control of all or part of such data. Given that individuals may be overloaded with information in quantities that they cannot realistically be expected to process or comprehend, obtaining proper consent from individuals may be impossible in many cases. An interpretation which focuses on the *risk of harm*, would have the result of reducing the burden of the notification obligation (and concurrently, the consent obligation). While transparency of data processing would remain a fundamental principle, notification and consent would be required only in cases of the presence of some *risk of harm*.

For example, instead of detailing all of the information that has been collected, as well as the uses which will be made of the data, in a lengthy privacy policy,[258] a very short notice relating exclusively to the collection, use or disclosure of data that may present a *risk of harm* to the individual would (arguably) be just as effective. Privacy policies could become one-paragraph, user-friendly statements outlining, for example, the possible sale of profile information to third parties for marketing purposes (instead of detailing what is blatantly obvious, what the individual already knows or which constitutes no risk of harm for him or her).

This proposed risk-based approach may allow organizations to streamline their communications with individuals, reducing the burden and confusion on individual consumers. Also, it may assist in providing for a framework allowing for organizations handling personal information to focus on disclosing the collection, the use and the disclosure of personal information in line with the original purpose of PIPEDA. This may translate into shorter and more efficient privacy policies.

PIPEDA provides for a subjectivity test when it comes to organizations disclosing their data management practices to individuals: organizations shall make "a reasonable effort" to ensure that the individual is advised of the purposes for which the information will be used.[259] Under the proposed risk-based approach, if a given use or disclosure of personal information creates a high *risk of harm*, organizations may wish to ensure that they dedicate more efforts and resources, in hopes of ensuring that individuals are properly and clearly advised of the purposes for which the information collected will be used or disclosed. This may be done, for example, by having individuals click to confirm that they have read the organization's privacy policy, or by drawing their attention to the data handling practices which are potentially more harmful to them. On the other hand, if this *risk of harm* is nonexistent or minimal, organizations may logically dedicate fewer resources to complying with these notice requirements (and may simply post a short and simple privacy policy on their website).

[257] See Eloïse Gratton (2013), *supra* note 9, for details on how this approach may work; See also Éloïse Gratton, Albany Law Journal of Science and Technology (2013), *supra* note 182.

[258] For example, many transactional websites state in their privacy policy that "upon you purchasing a product through our website, we may collect your name, email and physical addresses as well as your financial information in order to process your transaction, send you a confirmation and deliver the products that you have purchased on our website". Under the proposed risk-based approach, since these activities pertaining to the processing of online transactions are expected by the consumer and not in any way potentially harmful, they would not need to be mentioned in the policy.

[259] *Personal Information Protection and Electronic Documents Act*, *supra* note 14, at Schedule 1 (s. 5), principle 4.3.2. See also new s. 6(1) of this Act.

The FTC's staff has recently proposed that organizations provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past.[260] Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework reflects the concept that it is reasonable for organizations to limit their disclosure obligations to their data handling practices that may create a *risk of harm* to individuals. Those "commonly accepted" data practices (which create no risk harm for the individuals) would include product and service-fulfillment, internal operations, such as improving services offered, fraud prevention, legal compliance, and first-party marketing.[261] This approach would address the concern raised by certain authors about how frequent exposure to seemingly irrelevant privacy notices results in notice fatigue, i.e., notices are dismissed without even registering their content.[262]

Certain authors have been proposing to focus on accountability and ethical uses of personal information, instead of on consent.[263] Others have been proposing a risk-based approach under which data practices that are consistent with users' expectations may not require any immediate notice.[264] According to the proposed risk-based approach, a best practice would be to prioritize what and when notices are shown, based on privacy risks associated with the respective data practice.[265] Just-in-time notices, and obtaining express consent, are particularly relevant for data practices considered sensitive or unexpected. For instance, it has been suggested that in the case of mobile apps, access to sensitive information such as the user's location, contacts, photos, calendars, or the ability to record audio and video should be accompanied by just-in-time notices.[266] Another example is cars with automatic headlamps that continually sense ambient light conditions; providing notice about this type of data collection might not be necessary.[267] The FTC also notes with respect to the IoT that not every data collection requires choice, but that users should have control over unexpected data practices, such as data sharing with third parties.[268]

Under the proposed risk-based approach, privacy policies would focus on data practices which are potentially harmful for individuals (which may include the unexpected ones) to ensure the effectiveness

---

[260] Federal Trade Commission, March 2012, *supra* note 38, at vi.

[261] *Ibid*, at 36 and following.

[262] *Ibid,* section 1.1.2 which elaborates on this issue.

[263] Fred H. Cate, Peter Cullen, & Victor Mayer-Schönberger, *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (March 2014), available at: <http://www.repository.law.indiana.edu/facbooks/23/>.

[264] Microsoft, *Privacy Guidelines for Developing Software Products and Services*, Technical Report version 3.1, 2008, discussed in Florian Schaub et al., *supra* note 18, at 5.

[265] A. Felt, S. Egelman, M. Finifter, D. Akhawe, & D. Wagner, *How to ask for permission* (Proc. HOTSEC '12 2012).

[266] See Florian Schaub et al., *supra* note 18, at 6-7.

[267] Federal Trade Commission, *Mobile privacy disclosures: Building trust through transparency* (FTC staff report, Feb. 2013); See also Florian Schaub et al., *supra* note 18, at 6-7.

[268] FTC chairwoman Ramirez explains this rationale as follows: "Consumers know, for instance, that a smart thermostat is gathering information about their heating habits, and that a fitness band is collecting data about their physical activity. But would they expect this information to be shared with data brokers or marketing firms? Probably not." In these cases, users need clear privacy notices." See E. Ramirez, *Privacy and the IoT: Navigating policy issues* (CES Opening Remarks, 2015, FTC public statement).

of notices provided to users.[269] Although this new approach would imply rethinking, to some extent, the current PIPEDA consent model, it should nonetheless be further explored in the near future.

[269] See Florian Schaub et al., *supra* note 18, at 4.

CONCLUSION

At the time that the FIPPs were initially drafted in the early 1970s, their main purpose was to address specific concerns pertaining to computerized databases. The best way to deal with these data protection issues was deemed to be having individuals keep control of their personal information. Forty years later, that selfsame concept is still one of the most predominant theories of privacy and the basis for data protection laws around the world. PIPEDA was built on the FIPPs and generally provides that individuals be told who is collecting their personal information and the purpose of such collection, in order to enable them to decide whether to release control of all or part of such information.

Section 1 of this paper explains how the "notice and choice" approach is no longer realistic. Individuals are overloaded with information in quantities that they cannot realistically be expected to process or comprehend. Most privacy notices are ineffective at informing consumers and this stems from hurdles that can be attributed not only to general shortcomings of the notice and choice concept, but also to the challenges in designing effective privacy notices and using complex language. With new business models based on sponsored services or greater customization, organizations may have an incentive to collect as much personal information as possible and to be able to use that information as they wish. Personal information is often viewed as a commodity and certain studies even show that individuals do not want and do not expect to be paying for web services.

Although individuals are aware that there are some risks involved with data collection when they are active on the web or using new technologies, these risks are only potential to them, not very visible, and not quite quantifiable. Consent is challenged, in light of the increase in the volume of players providing new products and services, as well as the dynamic aspect of privacy policies and business models. Moreover, providing notice and choice in the context of new technologies can be challenging due to the ubiquity of devices, persistence of collection, and practical obstacles for providing information, if devices lack displays or explicit user interfaces. Data collection by devices in the IoT context or through wearables may often be invisible to users; so if they are not aware of the data collection, they are unlikely to be in a position to understand it or weigh in on the manner in which it is done. Recent technologies and new types of business models are becoming more complex, creating additional challenges, given that individuals typically get privacy defaults wrong and generally struggle to keep up with the astounding surge in digital economy and culture. More and more data exchanges now take place without the knowledge of users, which makes it difficult for organizations to achieve meaningful consent.

Section 2 of this paper explains that while there are various challenges with the "notice and choice" model, we should not be abandoning the "control" concept of privacy and, concurrently, the "notice and choice" model, at least for now. For many, this approach is still relevant. Moreover, global consistency in the data protection arena is increasingly important, and we should keep in mind that the threat of loss of trade as a result of Directive 95/46/EC and its adequate protection requirements was a strong motivating factor for the Canadian Government's decision to enact PIPEDA in the first place.

Section 2.1 discusses how, before amending PIPEDA on consent, one should be careful to make sure that the amendment will not be detrimental or problematic as soon as new technologies emerge. As a matter of fact, PIPEDA is meant to reach the proper balance between protecting the privacy of individuals and the need of organizations to collect, use or disclose personal information for the purposes that a reasonable person would consider appropriate in the circumstances. The wording pertaining to obtaining consent under PIPEDA is quite flexible and technology-neutral, and it is therefore

flexible enough to accommodate new types of technologies and business models. Another argument against amending PIPEDA on the issue of consent pertains to the fact that social norms in connection with any new technology or business practice may not yet to be established.

Section 2.2 addresses the downside of the flexibility surrounding the notion of consent, in that it creates uncertainty. For one thing, when new practices and business models make their way, the industry has to wait for the OPC to provide guidance on what is considered legal and legitimate from a "consent" point of view, or worse still, obtain guidance through findings, after a complaint has been filed with, and decided by, the OPC. Since there is a lot of uncertainty under PIPEDA concerning what type of consent would be considered as adequate upon new technologies being developed and commercialized, policy guidance on enhancing transparency and obtaining valid consent will be increasingly necessary to address some of this uncertainty and allow organizations to innovate without taking major legal risks, if they know upfront what constitute meaningful consent for new types of technologies or business practices. Since users' reasonable expectations must also be considered when determining the form of consent to use, frequent surveys on consumer attitudes towards specific technology, business models and privacy may reveal a lot of valuable information, including whether individuals understand certain technologies and whether they consider them as useful or instead, harmful.

It is always less disturbing to provide a solution which will be incorporated within the current legal framework, such as a proposed interpretation, than to propose a new amendment to the law. Section 2.3 discusses how the notion of "consent" under PIPEDA is already quite flexible and is technology-neutral, allowing for this notion to be interpreted with the proper balance between the protection of privacy and the need for organizations to collect, use or disclose personal information for the purposes that the reasonable person would consider appropriate in the circumstances. It also addresses the fact that this interpretation should consider any impact on innovation, as well as certain new ethical issues that may, to a certain extent, go beyond the current application of PIPEDA.

For instance, under an interpretation which would consider the impact on innovation, analyzing personal information on an acceptable, aggregate basis (i.e. anonymous information) may not require prior consent, therefore favouring business analytics. At the same time, consent could be required at the point where the information is then used to take a decision pertaining to an individual, especially if the information may be used for discriminatory purposes, eligibility decisions and may thus infringe on the right to equal treatment. Organizations can now analyze consumer behaviour datasets to identify consumer vulnerabilities, identify cognitive biases by attempting to pinpoint profitable anomalies and then use this to manipulate users. For instance, they may use the information by enticing them to provide consent, to reveal more personal information, to market to them when they are most vulnerable, to manipulate them on an unconscious basis, to exploit the differences in price sensitivity between consumers, all of which practices, according to some, raise ethical issues, which should be considered, especially if users are left in the dark.

Given that individuals may be overloaded with information in quantities that they cannot realistically be expected to process or comprehend, obtaining meaningful consent from individuals may be impossible in many cases. Section 2.3 proposed exploring the possibility of adopting an interpretation which focuses on the *risk of harm*, which would have the result of reducing the burden of the notification obligation (and concurrently, the consent obligation). For example, instead of detailing all of the information that has been collected, as well as the uses which will be made of the data, in a lengthy privacy policy, a very short notice relating exclusively to the collection, use or disclosure of data that may present a *risk of harm* to the individual would be just as effective. This may translate into shorter

and more efficient privacy policies, which would become short, user-friendly statements outlining, for example, the possible sale of profile information to third parties for marketing purposes (instead of detailing what is blatantly obvious, what the individual already knows or which constitutes no risk of harm for that person). This proposed risk-based approach may allow organizations to streamline their communications with individuals, reducing the amount and length of privacy notifications, as well as burden and confusion on individual consumers. Although this new approach would imply rethinking, to some extent, PIPEDA's current consent model, this approach should be further explored in the near future.

The objective of the present white paper is to provide input on the current challenges with PIPEDA's, consent-based model and to determine considerations and lines of thoughts that could be further explored, in order to ensure that this consent-based model remains efficient. A corollary of this work is to provide guidance to lawmakers, policymakers, privacy commissioners and courts in assessing whether and how consent should be interpreted in given situations. This will provide for a useful framework, under which PIPEDA remains efficient in light of modern Internet technologies. It may also guide the law toward a more coherent understanding of the challenges that we have with PIPEDA and its consent-based regime and to serve as a framework for the future development and review of PIPEDA.