SUBMISSION TO THE HOUSE OF COMMONS' STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

By Paige Backman and Aaron Baer, Aird & Berlis LLP[1]

April 2017

We welcome the opportunity to provide input to the House of Commons' Standing Committee on Access to Information, Privacy and Ethics (ETHI) in view of its study of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[2]

ETHI, together with the Office of the Privacy Commissioner of Canada (OPC), has the challenge of striking the right balance between: (i) allowing organizations to collect, use and disclose personal information for legitimate business interests; and (ii) protecting the rights of individuals to their personal information that is used by others for commercial purposes. Privacy laws and the implementation and enforcement of same have profound tangible impacts on both businesses and individuals.

The pace of technological advancement since the introduction of PIPEDA in 2000 has been staggering, as has been the ways in which businesses have created and continue to create new business models to take advantage of such new technologies. This results in an equally significant evolution in the ways in which individuals interact with technology; the nature and scope of personal information being collected, aggregated, re-identified, used, disclosed and sold; the manner in which businesses can commercialize information about individuals; and the resulting impact on individuals arising from the foregoing.

It is imperative that PIPEDA modernize and in so doing, account for new and emerging business models while adapting to individuals' behaviour in working within those new business models. This will not be achieved by subtle changes on the margins of the law.

When PIPEDA was introduced in 2000, fewer than 30% of Canadians owned a cell phone.[3] The most commonly used cell phones were Nokia and Motorola phones[4] with very limited capabilities, though Research in Motion (now Blackberry) had recently introduced its first device, the BlackBerry 850.[5] In 2007, Apple introduced the first iPhone. In 2014, 55% of Canadians owned a smartphone. Today, over 76% of Canadians own a smartphone.[6] The iPhone and the evolution of other smartphones and mobile devices fundamentally changed the way that individuals interacted with businesses and the nature and scope of information collected about individuals.

---

[1] Paige Backman, Partner and Co-Chair of Aird & Berlis LLP's Privacy and Data Security Group and Director of KnowledgeFlow Cybersafety Foundation. Aaron Baer, associate and member of Aird & Berlis LLP's Privacy and Data Security Group.

[2] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1 [*PIPEDA*].

[3] Canadian Wireless Telecommunications Association, Report on Statistics of Subscribers 2000-2004, online: <https://www.cwta.ca>.

[4] "Gartner Dataquest Says Worldwide Mobile Phone Sales in 2001 Declined for First Time in Industry's History", *Tech-Insider* (11 March 2002), online: <www.tech-insider.org>.

[5] Taylor Martin, "The evolution of the smartphone", *Pocketnow* (28 July 2014), online: <www.pocketnow.com>.

[6] "Smartphone Behaviour in Canada and the Implications for Marketers in 2016", *Catalyst Canada*, online: <www.catalyst.ca>.

Smartphones, mobile devices, smart appliances, smart cars, wearable technologies and the remaining Internet of Things has dramatically increased the amount of personal information collected; the nature, scope and sensitivity of the personal information; as well as the commercial uses for such information. This has also resulted in significant and substantive challenges to the application of PIPEDA to such new business models and practices.

PIPEDA was enacted based on principles to allow flexibility in application and evolution of technology. While introducing Canada to privacy laws over a decade ago using general principles may have been the prudent approach at the time, the evolution of technology and business practices has resulted in it being highly questionable whether PIPEDA effectively protects the rights of individuals.

While there are additional areas to which we can propose amendments to PIPEDA, for the purposes of our submission, we have identified 3 key areas for modifications to PIPEDA: (i) Consent Framework; (ii) Minors; and (iii) Right of Erasure. While we will not provide recommendations regarding the enforcement powers of the OPC, we will conclude with a few comments regarding same.

1. Consent - Framework to Streamline and Target Important Information

A) The Status Quo

Valid consent is the foundation to PIPEDA and to all privacy laws. To establish valid consent, PIPEDA provides that the following elements much be satisfied: The **knowledge and consent** of an individual are required for the collection, use and disclosure of personal information (except where inappropriate). Organizations are to make **reasonable efforts to ensure an individual is advised of the purposes** for which the information will be used and the purposes **must be stated in a manner that an individual can reasonably understand how the information will be used or disclosed**. 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.**[7] As well, consent is considered 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 the individual is consenting**.

It is arguable that the evolution of business models and practices, together with how individuals interact with those business models, has resulted in the failure to satisfy many, if not all, of these elements of consent. New business practices are based on real time, big data collected through our online engagement, our phones, our watches, our cars and our houses, and have evolved in a manner of which the average person is wholly unaware and cannot appreciate or understand. The mode of interaction between individuals (of all ages and demographics) and the business practices creates additional challenges to ensure individuals reasonably understand how their information will be used or disclosed. It also provides challenges to establishing that individuals to whom the organization's activities are directed understand the nature, purpose and consequences of the collection, use or disclosure of the personal

[7] *PIPEDA*, *supra* note 1, s 4.3.

information to which they are consenting. One may also argue that, due to the lack of clarity over what "legitimate business purposes" are, it is unclear when an organization must afford a positive opt-out right to practices that go beyond that which is necessary to fulfil a legitimate purpose.

Most organizations rely on privacy policies to obtain consent from individuals. Typically, privacy policies are posted on websites or linked-to in online applications, and range in length from a few pages to 30+ full-length pages. On a mobile device, this alone provides its own challenges.

Without discussing whether the content of such policies is appropriate, many studies have shown that privacy policies, as they are currently drafted and used, are an ineffective way to communicate information, provide choice or obtain valid consent from individuals. For example, a 2016 publication from York University assessed the extent to which individuals ignored privacy policies when joining a fictitious social networking site.[8] Seventy-four per cent of individuals skipped the privacy policy, preferring instead to choose the "quick join" option. The study also found that of the 26% of the individuals who did attempt to look at the privacy policy, the average time spent reading the privacy policy was only 73 seconds, when the average adult reading speed would have taken 30 minutes or more to read.

The results of this study are consistent with our observations. Most privacy policies are lengthy documents, filled with legalese and provisions that are not intuitive to most readers. To err on the side of disclosure, extensive terms are included in privacy policies, many of which address practices for which an organization should be able to rely on implied consent. The inclusion of these basic terms adds pages to privacy policies and takes time, focus and attention away from the information handling practices that are either supplemental to the basic information handling practices or describe secondary uses or disclosures of personal information for which express consent should be obtained.

Further, we would suggest that given the breadth of individuals to whom a particular organization's information handling policies are directed, an understanding of what a reasonable person would expect in the circumstances (a requisite of consent) is elusive. Business models will often engage minors and young adults, as well as senior members of society. Business models engage those who have a decent understanding in the ways of modern information handling practices, as well as those who have very limited (or no) understanding of modern information handling practices. As a result, it is questionable whether it is reasonable to expect that all such individuals to whom the organization's activities are directed understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. All of the people to whom an organization's practices are engaged can be reasonable people, and yet each person may come to a different conclusion on what a legitimate purpose is for the collection, use and/or disclosure of their personal information.

The result of this is that it is highly questionable whether individuals are providing knowledgeable consent to an organization's legitimate information handling practices. This is an issue for both the organizations and the individuals. Organizations relying on privacy policies

[8] Jonathan A. Obar & Anne Oeldorf-Hirsch, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services" (Paper delivered at the 44th Research Conference on Communication, Information and Internet Policy 2016, 30 September 2016), online: <https://ssrn.com/abstract=2757465>.

may have a false sense of security that they have obtained the requisite consent. It is also arguable that individuals are not given the requisite information in a manner that would allow them to reasonably understand how their personal information will be used or disclosed or that certain of the information handling practices are beyond that which is required to fulfil a legitimate purpose.

It would be unrealistic to argue that we can find an approach that will satisfy every individual across all such demographics. However, we suggest that a proper framework of consent and clarity surrounding the certain concepts (such as the bases on which consent can be implied and what is considered to be a legitimate business purpose) will allow businesses to have greater certainty that they have established the requisite consent and provide individuals with meaningful information on which they can provide their consent.

B) Our Recommendations

While many recommendations may be appropriate to solve the issues noted above, our recommendations will focus on providing greater certainty surrounding the business practices for which consent may be implied, shorter privacy policies, focusing individuals on information handling practices that deviate from basic information handling practices and providing meaningful options surrounding information handling practices that relate to secondary purposes.

Specifically, we recommend the following framework supporting consent be adopted:

1. Define the information handling practices for which consent may be implied and incorporate same in a model code. Certain suggestions for terms to include in this model code are attached hereto as Schedule 1.

Adoption of a model code that reflects basic information handling practices would clarify the information handling practices on which organizations can rely on implied consent. It would allow organizations to shorten privacy policies significantly by simply referring to the model code rather than repeating such policies. Organizations (typically smaller organizations) that use information solely in a manner that is captured by the model code, would simply refer to the model code and would not have to expend costs and resources to build their own.

To the extent an organization's information handling practices deviate from such model code, the organization's privacy policies would focus on those supplementary practices. Having privacy policies focus on supplementary practices would provide greater assurances that individuals are aware of those practices and further support the organization's ability to rely on an individual's consent to same.

For example, if the model code included the ability to transfer personal information to a supply chain partner *in Canada*, and an organization used supply chain partners in *the United States*, the privacy policy could draw attention to the fact that the organization's operations also require personal information to be transferred to supply chain partners in the United States. Such a provision, which is taking on greater importance in the recent political climate, would no longer be buried in a lengthy privacy policy; rather, it would be readily apparent to the reader and would increase the likelihood of the reader providing consent that is truly informed.

2. Require express consent for those information handling practices which deviate from or are in addition to those in the model code.

Organizations which incorporate information handling practices that deviate from or are in addition to the model code (we refer to those as supplementary information handling practices), would be required to set out those information handling practices in a clear manner in a privacy policy and obtain express consent in an auditable manner to such supplementary practices.

3. Separate information handling practices relating to secondary purposes from non-secondary purposes in privacy policies and provide a clear and readily available opt-out right for each secondary purpose.

Currently, secondary purposes are often mixed in with all other information handling practices in privacy policies and are portrayed as an all or nothing "acceptance." We recommend that terms in a privacy policy relating to supplementary practices be set out in separate sections:

> (i) information handling practices that, although they may deviate from the model code, are reasonably necessary for the provision of products and services requested by an individual; and
>
> (ii) information handling practices that relate to secondary purposes.

An example of a secondary purpose is the transfer of information to third parties for marketing purposes. For those information handling practices relating to secondary purposes, an opt-out from such secondary purposes should be clearly stated and readily available to the individual. If such secondary purposes have been communicated in an online environment, the opt-out could be provided immediately proximate to each of the secondary purposes stated and actionable in a readily-available manner (such as an opt-out box included right beside each secondary purpose).

4. For each instance where express consent is sought and has been obtained, a copy of the privacy policy should be delivered to the individual who provided express consent in a form that can be retained by the individual (e.g. by email or by mail to a specified address). The requirement to "provide" a copy of terms to which an individual is bound is consistent with many consumer protection acts across Canada.

2. Minors

A) The Status Quo

Currently, PIPEDA requires that consent is considered valid only if it is reasonable to expect that an individual to whom an 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. This is the closest protection PIPEDA affords to minors.

A 2014 study of young Canadians found that 24% of Grade 4 students and over 50% of Grade 7 students had their own cell phones.[9] Grade 4 students are typically 9 and 10 years old. Grade 7 students are typically 12 and 13 years old. Of course, young Canadians are not limited to cell phones to access the Internet. Internet access is widely available to young Canadians on laptops, tablets, gaming consoles and wearable technologies, and much of this Internet access is free from the oversight of their parents.

The increasing availability of Internet access to young Canadians poses a series of privacy concerns. A recent report by the Children's Commissioner for England (Commissioner) highlighted the growing concerns about personal information being provided by youth to organizations.[10] The Commissioner tested the terms and conditions of Instagram, which is used by 56% of 12-15 year-olds and 43% of 8-11 year-olds in England. Instagram's terms and conditions were 17 pages long and contained over 5,000 words, with language and sentence structure well beyond the capability of the average youth. Unsurprisingly, when asked to read through the terms and conditions, the youth were frustrated and confused.[11]

While young Canadians may be tech-savvy, they often lack the knowledge and understanding required to provide informed consent to the collection, use or disclosure of their personal information. Young Canadians are less likely to recognize the short-term and long-term implications of their choices online, including sharing their personal information. The impact of the choices made by minors in the online environment can result in significant short-term and long-term harm to the minor.

B) Our Recommendations

We recommend that organizations be required to obtain **verifiable consent** of a parent or guardian of individuals under the age of 16 in order to collect, use or disclose their personal information in the course of commercial activities. Any method to obtain verifiable consent should be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent or legal guardian.

While the age of 16 is not a magic number, this age is consistent with domestic laws as well as international laws such as the European Union's **General Data Protection Regulation** (GDPR), which will take effect in May 2018 and with which Canada must offer comparable protection.

Ontario's *Personal Health Information Protection Act, 2004* requires, in most circumstances, the consent of a parent or guardian to the collection, use or disclosure of personal health information of a child under the age of 16.[12] The GDPR also requires the consent of a parent

[9] Valerie Steeves, "Young Canadians in a Wired World, Phase III", *Life Online: MediaSmarts* (2014), online: <http://mediasmarts.ca/ycww>.
[10] UK, Children's Commissioner's Growing Up Digital Taskforce, *Growing Up Digital*, (London: Children's Commissioner, January 2017).
[11] *Ibid* at 8.
[12] SO 2004, c 3, Schedule A.

or guardian to information handling practices to which the GDPR applies where the child is under the age of 16.[13]

The United States Federal Trade Commission's *Children's Online Privacy Protection Rule* (COPPA) requires organizations to make *reasonable efforts to obtain verifiable parental consent*, taking into consideration the available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent or guardian. Similar to COPPA, the GDPR also requires organizations to make reasonable efforts to verify that consent was provided by the child's parent or guardian, with consideration given to the available technology.[14]

3. Right of Erasure

(a) Status Quo:

According to the American Academy of Child and Adolescent Psychiatry, over 60% of 13-17 year olds have at least one profile on a social networking site, with many spending more than two hours per day on social networking sites.[15] The CBC reported, based on a privacy sweep involving enforcement organizations in 21 countries that examined 1,494 apps and websites such as games, educational and social media websites hosted by children-friendly organizations like museums and zoos, that[16]:

- 67% of websites and apps surveyed collected personal information such as names, photos, addresses and phone numbers or via a chat function. Some of the worst offenders were music websites.
- 51% indicated they may disclose personal information to a third party for advertising purposes or otherwise.
- 71% had no simple way to delete account information.
- 58% sometimes directed children to other sites, often via contests or ads, including some that were inappropriate for children, such as those promoting dating websites and alcoholic beverages.

Privacy Commissioner, Daniel Therrien, concluded "too many developers are collecting particularly sensitive personal information such as photos, videos and the location of children, and often allowing it to be posted publicly…."

There are significant benefits to children and youth engaging in social media, including developing new social contacts with peers with similar interests and developing and expressing their individual identity. The consequences of an error in judgment of a minor, or judgment of another (including businesses and other individuals) which involves the information of a minor, can have significant short-term and long-term consequences on the minor and on society. More frequently, we are seeing that an online footprint can lead to or be central to online bullying,

---

[13] EC, *Commission Regulation (EC) 679/2016 of 4 May 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 at 8 [*EC Regulation*].

[14] *EC Regulation*, *supra* note 16 at 8.

[15] American Academy of Child & Adolescent Psychiatry, "Social Networking and Children", No. 100, February 2017.

[16] CBC News, "*Most Kids apps, websites collect and share personal information, Privacy sweep finds many allow photos, video and location information to be posted publicly.*", September 3, 2015, http://www.cbc.ca/news/technology/most-kids-apps-websites-collect-and-share-personal-information-1.3214213

which can significantly impact the physical and mental health of the minor and lead to long-term consequences for the minor and society.

Aside from the very real and significant issues of physical and mental harm to a minor, whether through an error in judgment or simply the result of a business practice, the sharing of a minor's information can impact the minor's ability to obtain or retain employment and can lead to the minor being taken advantage of by predatory adults.

For our recommendation in response to this issue, we incorporate, by reference, the data set forth in the immediately preceding section entitled "Minors." A significant percentage of children who are 9-12 years old have their own smartphones and are communicating with others in an online environment on various business platforms.

Our recommendation requiring parental or guardian consent involving youth and children under the age of 16 addresses parental and legal guardian involvement at one point in time. However, we need to also address the ongoing information sharing and use of minors' information in commercial activities that occurs throughout the involvement of a child or youth in the online environment.

While we would hope that parents and guardians of children of that age are supervising their child's use of the Internet and information shared over the Internet at all times, when children who are 9 to 12 years old have their own smartphones and mobile devices, we need to accept that adult supervision for these children is limited. Supervision for youth aged thirteen years or older is even less likely. We cannot ignore this fact or that certain businesses are targeted towards children and youth, yet we must try and protect our children and youth for the same reasons and in a manner consistent with the protection we afford our children and youth in other areas of the law.

(b) Recommendations:

We strongly recommend that the right of erasure be enacted in relation to minors where their personal information has been collected, used or disclosed in the course of commercial activities.[17]

As part of our children's general education, we believe it is important to encourage our children and youth to learn to use online resources and learn to participate in an online environment. However, we must also provide a mechanism to protect this very vulnerable part of our society. The right of erasure (or the right to be forgotten) as applied to minors is not only for the short-term benefit of the minor, but the long-term impact on the minor and society at large.

We note that the European Union, through the GDPR, also specifically supports the increased need for the right of erasure when personal information of a minor is involved. "*That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal*

[17] In our submissions, we use the term minor to mean individuals under the age of majority generally; however, we use the term children to refer to those individuals under the age of thirteen and use the term youth to refer to those individuals between the ages of 13 to age of majority.

data, especially on the Internet. The data subject should be able to exercise that right, notwithstanding the fact that he or she is no longer a child."

Specifically, we recommend the following, and in a manner consistent with the GDPR:

Individuals whose personal information which is subject to PIPEDA (collected, used or disclosed in the course of commercial activities) and that is or was collected, used and/or disclosed during the time such individual was a minor, should have the right (along with their parents or legal guardians) to have such personal information deleted without undue delay, except in the following circumstances: (i) using or disclosing such information is required to comply with statutory or other legal obligations including government or court order; or (ii) for the establishment, exercise or defence of legal claims.

To the extent that such personal information has been disclosed or transferred to a third party or otherwise made public, the organization who originally collected the information, and all parties who are using or disclosing such information, should take reasonable steps, including the use of reasonably available technology, to delete all copies and links to such personal information.

4. Enforcement

We have reviewed the numerous submissions regarding expanding the enforcement powers of the Office of the Privacy Commissioner of Canada (Privacy Commissioner). We acknowledge and appreciate the goals of those who wish to expand the enforcement powers of the Privacy Commissioner and that such expanded powers will be consistent with the enforcement powers of other jurisdictions.

While we will not provide recommendations addressing specific enforcement powers, for purposes of the discussion surrounding same, we strongly suggest that it is important to keep in mind that the general principles on which PIPEDA is based, while creating flexibility, create great uncertainty surrounding an organization's compliance obligations. Without greater certainty surrounding the compliance requirements under PIPEDA, it will be unfair and highly prejudicial to impose additional penalties and fines on such organizations. Without this added clarity, organizations could be unfairly exposed to fines, penalties and orders, despite acting in good faith to comply with PIPEDA.

While we are not arguing against increased enforcement powers, we are strongly recommending that prior to increasing enforcement powers, greater certainty and more details surrounding compliance obligations be addressed in PIPEDA. As discussed above, greater clarity on obtaining the requisite consent (implied or express, minors versus adults, etc.) is critical. We believe the consent framework recommended above can assist in this regard, though other regulatory guidance may also be required. For example, depending on the specifics set out in the final regulations surrounding data breach response requirements, additional clarity surrounding those may also be required.

If the goal is to encourage compliance with PIPEDA, and not simply to punish, presumably greater clarity on these core areas is in everyone's best interest.

Conclusion

The task facing the ETHI is challenging, but extremely important. We commend you for your time and effort in modernizing PIPEDA and ensuring amendments to PIPEDA are relevant and valuable in achieving its purposes. The effort to modernize PIPEDA and ensure the protections afforded thereunder are relevant and valuable will not come without challenges. However, decisions to not modernize PIPEDA or to amend PIPEDA in a way that does not result in real protections for business and individuals also come at a cost.

We hope our submission is of some value. While we limited our proposed changes to three key areas, we are happy to discuss these or any other proposed changes to PIPEDA with you further.

Schedule 1
Model Code

The following are proposed terms for inclusion in the Model Code:

Purposes for Collection and Use of Personal Information:

An organization (“Organization”) may rely on the implied consent of the individual when the Organization collects and uses Personal Information for the following purposes:

a) to establish and maintain responsible commercial relations with the individual and to provide ongoing services;
b) to contact the individual about changes, enhancements or similar notices related to Organization's products and services;
c) for those purposes set forth in agreements between the individual and Organization;
d) to understand the individuals' needs;
e) to develop, enhance, market or provide products and services; and
f) to meet legal or regulatory requirements, including to protect or defend a legal interest.

Purposes for Disclosure of Personal Information and Transfer of Information:

An organization (“Organization”) may rely on the implied consent of the individual when the Organization discloses Personal Information for the following purposes:

a) to provide the products and/or services requested by the individual;
b) to establish and maintain responsible commercial relations with the individual;
c) to fulfil the terms of agreements between the individual and Organization; and
d) to meet legal or regulatory requirements, including to protect or defend a legal interest;

Organization sometimes transfers Personal Information to others, including to affiliated entities or unrelated companies ("service providers"), that carry out certain functions on the Organization’s behalf, such as order fulfilment, data processing, accounting and administrative services, customer service and information technology services including, without limitation, hosting and data storage services. In those cases, Organization requires those service providers not to use or disclose individuals' Personal Information for any purpose other than as directed by Organization.

From time to time, Organization may be required to provide Personal Information in response to a court order, subpoena, government investigation, or as otherwise required by law. Organization also reserves the right to report to law enforcement agencies any activities that Organization, in good faith, believes to be unlawful. Organization may release certain Personal Information when Organization believes that such release is reasonably necessary to protect the rights, property and safety of others and Organization.

Note to Children

An organization does not knowingly accept any Personal Information from or about children under the age of majority without the consent of the minor’s parent or legal guardian. We encourage parents and guardians to spend time with children and to monitor their online

activities. Please protect your child's privacy by instructing them to never provide Personal Information online without your knowledge and permission.

28933371.1