Review of the *Personal Information Protection and Electronic Documents Act*:

All things come to those...

Brief submitted by Options consommateurs

to the

House of Commons Standing Committee on Access to Information, Privacy and Ethics

11 May 2017

Legal deposit
Bibliothèque nationale du Québec
National Library of Canada
ISBN: 978-2-89716-036-4

Option consommateurs
50 Sainte-Catherine Street West, Suite 440
Montréal, Quebec
H2X 3V4
Tel.: 514-598-7288
Fax: 514-598-8511
Email: info@option-consommateurs.org
Website: www.option-consommateurs.org

Table of Contents

Option consommateurs iv
Summary v
1. The issue 1
1.1 Background 1
1.2 About Option consommateurs 2
1.3 Our comments 2
2. Our concerns 2
2.1 Problems becoming more complicated 2
2.1.1 Diversification of practices 2
2.1.2 The changing value of personal information 5
2.2 Changing rules 6
2.2.1 Prevention 6
2.2.2 Information 7
2.2.3 Consent 9
2.2.4 The right to be forgotten 10
2.2.5 Other concerns 11
2.2.6 Powers of the Commissioner 11
3. Conclusions and recommendations 12
3.1 Looking to the future 12
3.2 In the meantime 14

Option consommateurs

MISSION

Option consommateurs is a not-for-profit organization whose mission is to promote and defend the rights and interests of consumers and ensure that they are respected.

BACKGROUND

Option consommateurs has been in existence since 1983. It arose from the family economics cooperative movement known as the ACEF [Associations coopératives d'économie familial], more specifically the Montréal chapter of the ACEF. In 1999, it broadened its reach by joining forces with the Association des consommateurs du Québec (ACQ), a consumer protection association which had been pursuing a similar mission for over 50 years.

KEY ACTIVITIES

Option consommateurs helps consumers who are experiencing difficulties, provides budget consultation services and conducts sessions on budgeting, indebtedness, consumer law and privacy protection.

Each year we produce research reports on important consumer issues. We also work with policy makers and the media to denounce unacceptable situations. When necessary, we institute class action suits against merchants.

Summary

The current study of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) by the House of Commons Standing Committee on Access to Information, Privacy and Ethics is made particularly vital by ongoing changes in modern society. In support of this review, the present brief briefly discusses some of the problems experienced by Canadians in this area; it also examines the state of our applicable legislative framework as well as any shortcomings it may contain, notably in comparison with the rules which the European Union is preparing to implement. Lastly, a number of recommendations are set out concerning legislative amendments and improvements to personal information management research and information programs.

Option consommateurs was established in 1983. This Quebec consumer association helps consumers who are experiencing difficulties by offering information and advice to individuals, lobbying policy-makers on behalf of consumers, and providing information to the general public. It has maintained an active interest in personal information protection issues since 1990.

As the types of personal information in circulation, the means of processing such information and the nature of the organizations that make use of it continue to evolve, the boundaries of the world in which we live continue to become more fluid and complex, and less comprehensible to ordinary citizens. Moreover, personal information is increasingly being bartered: identities are used to make transactions, and a growing number of payment methods require users to provide identification. This trend ultimately creates a risk of socioeconomic exclusion that must immediately be addressed.

Various regulatory measures can minimize the risks faced by citizens. At the prevention level, personal information protection principles must be incorporated into the design of management mechanisms. People must be better informed, and the clarity of the information they receive must be improved. Members of the public must be given more flexibility when it comes to consent, and the impact of unfair terms and conditions imposed by too many organizations must be mitigated. Focus must be placed on particularly sensitive issues, such as children's rights and the handling of information concerning deceased individuals. The Canadian system could also be improved by expanding its area of application and substantially increasing the responsibilities and powers of the Privacy Commissioner, who should, among other things, have the authority to impose dissuasive administrative monetary penalties.

In the longer term, it will be important to examine the very foundation of our personal information management system, which dates back to 1980 and may no longer exactly match what is needed in the 21st century.

All things come to those who wait.
F. Rabelais, *Pantagruel*, Book IV, c. 48

1. The issue

1.1 Background

Are we more than just a collection of more or less coherent personal information? One can only wonder, given the degree to which we are increasingly being reduced to the automated processing of codes assigned to us by businesses and governments in order that they might better "manage" our lives.

Philosopher Giorgio Agamben noted as much in 2009 when he pointed out that, instead of our social "persona" and the recognition of that persona, our identity now consists of data (and particularly biometric data).[1] Whether we resign ourselves to it or not, we currently have no choice but to cope with information practices that can potentially upset our lives; at the very least, we try to frame them with rules based on the simple principle that individuals should be able to maintain a certain degree of control over the information that concerns them and which makes up the "virtual twins" that policy-makers, lacking access to the individuals themselves, are constantly seeking ways to exert control over.

In Canada, these rules are set out, in particular, in the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which has been amended only slightly since it received Royal assent in 2000.[2] The problem is that technology and social practices have evolved much faster than the legislative framework over the past two decades, making that framework increasingly obsolete. To make matters worse, the rules established in other jurisdictions, in particular in the European Union, are also evolving. The inexorable progress of globalization has resulted in a massive increase in the cross-border flow of data, and we now have to deal with the rights and obligations established by other countries or groups of countries.

The review of PIPEDA embarked upon by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the committee) therefore could not be timelier. There is now an urgent need to revise the legislative framework governing the protection of the personal information of Canadians. That being said, we believe (as pointed out in section 3 of this brief) that the present process, however necessary it may be to the updating of that framework, will not be sufficient: ultimately, a far more substantial reform will likely have to be considered. But doubtless we will have to wait a bit before embarking on such an undertaking...

[1] Agamben, Giorgio. *Nudities.* Stanford University Press, 2010, 144 pages.
[2] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

1.2 About Option consommateurs

Option consommateurs was established in 1983. This Quebec consumer association helps consumers experiencing difficulties by providing them with information and advice, advocating on their behalf with policy-makers and informing the general public.

Option consommateurs has been active in personal information protection issues since 1990. Among other things, it contributed to the passage of PIPEDA as well as the passage of Quebec's legislation respecting the protection of personal information in the private sector. In recent years, it has conducted a number of research projects funded by Innovation, Science and Economic Development Canada's Office of Consumer Affairs or by the Office of the Privacy Commissioner of Canada.

1.3 Our comments

The following pages will briefly examine two types of issues. To begin with, section 2.1 discusses some of the social and technological trends that are making it necessary to review the Canadian legislative framework governing the protection of personal information held by undertakings. Section 2.2 then briefly looks at specific problems in a number of areas (e.g., prevention, information, consent, the right to be forgotten, the application and implementation of rules) that in our considered opinion require at the very least adjustments to our legal system. Section 3, in addition to setting out several specific recommendations flowing from these observations, raises some far more fundamental questions which the present legislative review will undoubtedly not be able to answer – specifically: Is it now time to rethink the very pillars upon which our personal information protection systems rest? Can we afford to wait 20 more years before adjusting the law to meet our needs?

2. Our concerns

2.1 Problems becoming more complicated

2.1.1 Diversification of practices

Personal information management is becoming increasingly challenging, notably because of a diversification phenomenon that can be seen in virtually all spheres of information protection. It is noticeable in many ways.

First of all, the types of information being targeted for collection and processing are increasing. Formerly, such information consisted of a few identifiers (name, address, credit card number, etc.) associated with a specific piece of data, such as entitlement to a benefit or the payment of a debt, for example. Nowadays, collected information includes genetic data, images, geolocation data, mouse clicks on a web page,[3] the expression of emotions, metabolic data,[4] the "friendliness" of our relations with others, opinions, and the list goes on – all of which can be archived, searched, analyzed and used for decision-making purposes.

To complicate matters, many individuals carry devices allowing them to gain access to a variety of networks. Also, the family computer can be used by numerous individuals, and people regularly borrow the smartphones of friends or family members.[5] Obviously, few people bother to create separate user profiles on these devices; insofar as companies regularly identify devices (rather than the users of those devices) for profiling purposes, it goes without saying that a user can compromise not only the protection of his or her own personal information, but also that of third parties. As an example, a girl might borrow her older sister's smartphone to search the web on the subject of abortion in order to assist a friend; the older sister, upon seeing that a number of websites are pushing ads and links at her on this subject, will be able to figure out what kind of sites her sister has been visiting. An inspection of the telephone by the father of the two girls, however, might lead him to react angrily against the older daughter, who had nothing to do with what he discovered.

Tracking methods also differ. People often provide information voluntarily, but information is often gleaned by means of cookies and other types of trackers that discreetly take up residence in our machines; information can also be skimmed by means of invisible pixels on the websites people visit[6] and from the metadata that is inevitably produced[7] while surfing the web. Canadians generally have a relatively poor knowledge of how all of this works, let alone the impact this information can have.[8]

---

[3] See for example a document produced by the Amazon corporation, cited in: Plourde, Alexandre. *How Free is "Free"? Setting limits on the collection of personal information for online behavioural advertising.* Option consommateurs, Montréal, June 2015, p. 20–21. Available online at: http://www.option-consommateurs.org/documents/principal/fr/File/option_consommateurs_2014_2015_gratuite_rapport.pdf (hereinafter "Plourde. *How Free is "Free"?*").

[4] These include information compiled by watches and bracelets that record heart rates, numbers of steps taken, etc. Such information can be stored, used to prepare profiles, and compared against similar recorded results for other individuals.

[5] Examples are given in: Green, Eileen and Singleton, Carrie. "Mobile connections: an exploration of the place of mobile phones in friendship relations." *The Sociological Review*, 54:1, 2009, pp. 125–144. Among other things, the authors explore smartphone sharing among siblings (or friends) when parents object to allowing younger children to have their own telephones.

[6] Plourde. *How Free is "Free"?*, pp. 12–14.

[7] The European Union is currently studying a proposed regulation focusing in particular on metadata. See: European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, 2017/0003 (COD), Brussels, 10 January 2017. The English and French versions are available for download at: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

[8] Plourde. *How Free is "Free"?*, pp. 30–36.

In addition, the processing of personal information becomes all the more opaque when the users of such information employ big data to perform analyses of a scope that extends far beyond what might be expected by the individuals supplying such innocuous information.[9] The interconnection of a broad range of suppliers, analysts, subcontractors and so on does not simplify matters. Does the user of a credit card issued by a Canadian financial institution have a clear understanding of the extent to which information concerning the purchases made with this card almost inevitably flows through the United States, given the configuration of the electronic networks operated by major credit cards such as Visa and MasterCard?

Not only do we have to deal with the processing of information that concerns us during our lives, we are also increasingly called upon to manage situations in which a particular piece of information concerns several individuals who do not necessarily have the same interests or desires: there are innumerable examples of this on social media, such as expressions of support (e.g., "likes") and the viral forwarding from user to user of links and photos concerning one or numerous individuals... Our virtual twins thus become interlinked with those of many other individuals. And an even trickier problem arises when these doppelgangers persist beyond the lifetimes of the individuals they represent, leaving surviving friends and family members the task of managing their existence, often without any consent from the individuals involved.[10]

Added to all this is the growth of the "Internet of Things." Not only do we ourselves more or less voluntarily disclose our personal information, the things in our possession increasingly generate such data as well. Smart cars are the best example of this, but they are not the only example. Data on home electricity consumption, for instance, is now transmitted electronically to utility companies (and is therefore vulnerable to interception); even in our absence, without our consent and without any deliberate intervention on our part, these data can reveal meaningful information about the way we live. Soon, refrigerators may be able to order groceries automatically when

[9] Cameras inside a fast-food restaurant, for example, can determine that lines are getting longer and consequently adjust digital menu displays to focus more on products that can be prepared faster (see: Laskoski, Nicole. "Ten Big Data Case Studies in a Nutshell." *CIO Decisions*, December 2013–January 2014, consulted at: http://searchcio.techtarget.com/opinion/Ten-big-data-case-studies-in-a-nutshell. Prices could also be raised in response to peaks in demand (a practice employed by airlines on their websites), again based on real-time tracking of consumer traffic. Uber is a well-known case in point: your use of the Uber app impacts supply and pricing, although the nature of the personal information being collected and the use to which that information is being put remain largely unknown, leading to results that more often than not cannot be predicted.

[10] Option consommateurs will soon be publishing the results of a study of certain aspects of digital death, which was conducted with financial support from Office of the Privacy Commissioner of Canada. In this regard, we have taken note of the fact that the European Union has specifically stated, in whereas clause 27 of the *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [Official Journal of the European Union, 4.5.2016, p. L119/1], that "this Regulation does not apply to the personal data of deceased persons." However, the problem persists and the European authorities, like the Canadian authorities, will sooner or later have to look into these rather thorny and complex issues. Quite simply put, our information outlives us. The automatic deletion of such information is not always the best solution; however, deceased individuals cannot provide consent regarding the fate of such information: this fundamental paradigm of personal information management is thus called into question, as noted in section 3 of this brief.

they determine that the supply of yogurt, for example, is running low.[11] This information, although it does not emanate directly from individuals, concerns those individuals nonetheless. How will this information be processed? And how will it be possible to guarantee its security, when sites such as Shodan[12] make it possible for anyone to consult a myriad of information collected and supplied by all sorts of things, or when images from an untold number of surveillance cameras throughout the world are placed at the disposal of anyone who may have a voyeuristic bent?[13]

2.1.2 The changing value of personal information

Personal information has always fed informed decision-making with respect to individuals. Such information is traditionally factored into decision-making processes. But there is more to it now, as such information is increasingly being bartered.

An increasing number of businesses on the web operate on a two-sided market[14] business model that demands nothing more from users than the sharing of personal information. Google and Facebook, for example, can turn personal information to account in a variety of ways in order to generate revenue.[15] Individuals trade their personal information to these companies in order to gain access to their services, so to speak, and these companies in turn create revenue out of that personal information.

There is a resulting risk of exclusion for Internet users: individuals who do not consent to share their information will not be able to participate in networks that are growing in social importance. People may ultimately even be excluded from certain economic circuits, given the

[11] Pegoraro, Rob. "Samsung's Family Hub Smart Fridge: Would You Believe It Keeps Beer Cold, Too?" *Yahoo Tech*, 7 January 2016.

[12] See https://www.shodan.io/. On the subject of practices such as camera surveillance, see: Osborne, Charlie. "Shodan: The IoT search engine for watching sleeping kids and bedroom antics." *Zero Day*, 26 January 2016, consulted at: http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/. Shodan also provides access to heart rate monitors used in US hospitals and to the management of French hydroelectric power stations (see in particular: Goldman, David. "The Internet's most dangerous sites." *CNNtech*, 2 May 2013, consulted at: http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html.

[13] See for example, concerning a recent case in a Nova Scotia school: Bradley, Susan. "N.S. privacy watchdog investigating after Russian site shows surveillance video of school." *CBCNews / Nova Scotia*, 4 May 2017, consulted at: http://www.cbc.ca/news/canada/nova-scotia/privacy-commissioner-investigation-school-webcam-broadcast-1.4099658.

[14] "Two-sided markets" are markets in which a supplier is simultaneously dependent on two markets: a newspaper publisher, for example, must convince both readers and advertisers to make use of its services; the prices for those services may differ or even be free of charge for one of the two market sides. A classic economic study of this phenomenon is presented in: Rochet, Jean-Charles and Tirole, Jean. "Two-Sided Markets: A Progress Report." *The Rand Journal of Economics* 37:3, 2006, pp. 645–667, available at: https://www.jstor.org/stable/pdf/25046265.pdf?seq=1#page_scan_tab_contents. Professor Tirole was the recipient of the 2014 Sveriges Riksbank prize in economic sciences in memory of Alfred Nobel. See also: Hoofnagle, Chris Jay and Whittington, Jan. "Free: Accounting for the Costs of the Internet's Most Popular Prize." *UCLA Law Rev*., 2014, pp. 606–670.

[15] Plourde. *How Free is "Free"?*, pp. 37–42.

growing disconnect between anonymity and the payment process: payments are now sometimes made through the exchange of identifiers, and increasingly by supplying at least some amount of information to authenticate payment operations. This insidious relationship between payment and the capture of personal information should be examined more closely. All too often, moreover, organizations will require personal information to be provided even though it is not required for the operation they are planning to conduct with an individual; too few people are aware or remember that the collection of unnecessary information is prohibited under subsection 5(1) of PIPEDA and clause 4.2.2 of Schedule 1 to PIPEDA.

Thus personal information is no longer simply valuable in itself, but has become valuable as a kind of password that will open the door to an increasingly networked society. It is no longer merely a matter of knowing whether, as an individual, I want to provide a given piece of personal information for decision-making purposes; if I do not consent to providing that information, I can be barred from access to entire systems, not because the information in question is necessary, but because it is required for "optional" but socioeconomically quasi-essential services.

2.2 Changing rules

Since the information universe is changing, its regulatory framework must also evolve; otherwise, the growing gap between practices and rules will lead to a proliferation of problems that, sooner or later, will generate crises detrimental to most of those concerned. However, the work done in recent years within the European Union, in particular, indicates that it is possible to reform the regulatory framework underlying the management of personal information. While it may not be possible to fully transpose the solutions proposed in *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (hereinafter referred to as "the EU Regulation") to the Canadian context, they can at least provide us with food for thought and be a source of inspiration. Indeed, some of the principles underlying the EU Regulation, such as placing more emphasis on preventive measures, improving practices pertaining to information and consent, and updating the powers of regulatory authorities, are ideally suited for application to the Canadian system.

2.2.1 Prevention

More than ever, an ounce of prevention is worth a pound of cure when it comes to the management of personal information. This philosophy is embraced in Article 25 of the EU Regulation, which requires personal information collection and processing mechanisms to be designed in such a manner as to facilitate the implementation of the personal information

management principles set out in the EU Regulation. It should be noted in passing that this concept of "integrated protection," starting with the design of a service, was first developed in Canada about 20 years ago under the name "privacy by design."[16] It is undoubtedly high time for us to in turn formally incorporate it into our legislative framework.

The integrated protection approach is all the more attractive in that it rests on an economic principle of cost allocation that seems incontrovertible in its logic: the economic player who can most easily avoid imposing costs should be required to do so. This is known as the least-cost-avoider concept. Since personal information management practices which derogate from the rules impose disadvantages – and therefore costs – on their victims, they must be avoided. That being said, it is the designers and suppliers of services who are most readily able to eliminate these disadvantages by improving the design of their products. It is much easier and less expensive for Facebook, for example, to launch a product that complies with personal information protection rules than to ask nearly 2 billion users[17] to amend their usage parameters after the fact or to submit requests to correct or withdraw certain information.

In order to prevent risks, of course, they must first be uncovered and assessed. The EU Regulation thus requires, in certain cases within the European Union, that data protection impact assessments be conducted pursuant to Articles 35 and 36. This approach would undoubtedly have to be adapted somewhat before it is applied to Canada, but we see it as constituting a sometimes indispensable accessory to the implementation of an effective integrated system for the protection of personal information starting with the design of mechanisms for the collection and processing of such information.

Individually, the availability of "do not track" options would also be useful, by making it possible to avoid at the very outset the collection and accumulation of personal information.[18]

A strong effort is therefore required to improve the prevention side of our system; however, this is not enough.

2.2.2 Information

In order for an individual to give adequate consent, understanding is required. And understanding can only be achieved through information. The existing Canadian rules, as formulated by the legislator and subsequently interpreted by the courts or by administrative

[16] A summary of the brief history of this concept, among other things, may be found in: Bélanger-Krams, Annik. *Enquête sur les paiements mobiles au point de vente: qu'en est-il de la vie privée des consommateurs?* Option consommateurs, Montréal, June 2016, pp. 42–44. [Available in French only]
[17] As of March 2017, Facebook had 1.94 billion users. See: Zephoria Digital Marketing. *The Top 20 Valuable Facebook Statistics – Updated May 2017*, consulted at: https://zephoria.com/top-15-valuable-facebook-statistics/.
[18] On this subject, see: Plourde, Alexandre. *Paying for Oblivion: Legal and commercial aspects of the right to be forgotten in Canada.* Option consommateurs, Montréal, June 2016, consulted at: http://www.option-consommateurs.org/documents/principal/en/File/Option_consommateurs-RTBF_2016.pdf (hereinafter "Plourde. *Paying for Oblivion*"), p. 58.

bodies, however, do not guarantee that citizens will be able to obtain all of the information they need in order to gain full understanding, nor do they guarantee the comprehensibility of such information.

First, the information provided by service providers often takes the form of "policies" that are more or less easy to find on their websites or elsewhere, or of provisions in the terms and conditions of service. All too often, these texts are illegible and incomprehensible: tiny fonts and page layouts that are daunting to even the most hardened reader are coupled with content rendered abstruse by unintelligible jargon, excessively complex syntax and the implicit or explicit use of legal concepts that are unfamiliar to ordinary users. It is important to bear in mind that half of the Canadian population is functionally illiterate,[19] and that all of this documentation is consequently of little or no use to those individuals.

In short, although the necessary information is formally placed at our disposal, it remains virtually useless.[20]

It would undoubtedly be more accurate to state instead that part of the information is available; in some cases, lack of transparency is the real issue. All too often, decisions regarding particular individuals are made on the basis of algorithms that are beyond comprehension, but which are presumed to be reliable. However, there is every reason to believe that automated decision-making mechanisms have considerable shortcomings.[21] We therefore concur fully with the fears expressed in this regard by professor Michael Geist when he appeared before the committee on 21 March.[22]

In this perspective, we feel it is essential for Canadian authorities to draw inspiration from Article 22 of the EU Regulation to provide as quickly as possible a framework for automated decision-making mechanisms, and to ensure that the data necessary to evaluate their effectiveness are in the public domain or, at the very least, can be gauged rigorously by control agencies such as the Office of the Privacy Commissioner.

With regard to information transmitted to us, assuming it may be potentially useful, we should at least draw inspiration from Articles 12 to 14 of the EU Regulation to emphasize the requirement that it be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language," as stipulated in Article 12 of the EU Regulation.

---

[19] Specifically, on a five-point scale measuring literacy, 49% of Canadians are deemed to have a proficiency level of two or less. See: Statistics Canada, Employment and Social Development Canada, and Council of Ministers of Education Canada. *Skills in Canada: First Results from the Programme for the International Assessment of Adult Competencies (PIAAC)*. Statistics Canada, Catalogue number 89-555-X, Ottawa, 2013, pp. 16–17, consulted at: http://www.statcan.gc.ca/pub/89-555-x/89-555-x2013001-eng.pdf.

[20] See, among others: Plourde, *How Free is "Free"?*, pp. 16–36 and Bélanger-Krams, pp. 50–67.

[21] Regarding the relative efficiency of the automated credit score mechanisms used by Canadian financial institutions, see: Allen, Jason, Damar, Evren and Martinez-Miera, David. *Consumer Bankruptcy and Information*. Bank of Canada Working Paper 2012-18. Bank of Canada, Ottawa, July 2012, consulted at: http://www.bankofcanada.ca/wp-content/uploads/2012/07/wp2012-18.pdf. The authors refined their analysis in: Allen, Jason, Damar, Evren and Martinez-Miera, David. "Consumer Bankruptcy, Bank Mergers and Information." *Review of Finance*, 2016, pp. 1289–1320. See also: Drozd, Lukasz A. and Serrano-Padial, Ricardo. "Modeling the Revolving Revolution: The Debt Collection Channel." *American Economic Review*, 107(3), 2017, pp. 897–930.

[22] See also: Plourde, *How Free is "Free"?*.

2.2.3 Consent

The cornerstone of the legislative framework governing the protection of personal information, the concept of consent has been drained of all substance. As professor Vincent Gautrais noted in his appearance before the committee on 4 April, the exchange of consent mechanisms proposed in contractual form by organizations are designed, first and foremost, to protect the companies that draft such forms and not the users. PIPEDA contains almost no rules governing these adhesion contracts that would make it possible to invalidate the kind of abusive clauses they more often than not contain.[23]

Usually, people have no choice: they must either give blanket consent to all of the requirements imposed by providers or do without their services. Since most service providers have similar rules in this regard, competition no longer plays an effective role in the framing of practices. We consequently agree with the suggestion made by professor Geist in his appearance before the committee that an "à la carte" consent system be implemented that would truly make it possible for consumers to freely determine the extent to which they consent, or not, to the collection and use of personal information that is not absolutely necessary to the provision of the products or services they are seeking to obtain.[24]

The problems raised by the concept of consent are obviously exacerbated when children come into play, since children do not have the knowledge and information or, in many cases, the judgement which adults are presumed to be able to call upon.

What child – and what parent, for that matter – would suspect that interactive teddy bears are recording children's words and storing them in the cloud, where they could possibly be analyzed and pirated?[25] Who could imagine that the manufacturer of these toys, sold under the brand name *CloudPets*, would decline to take action to remedy the situation when it was advised more than once by specialists that there were huge gaps in its security measures? And how is it that a doll that can connect to the Internet, search the web and communicate with third parties was allowed to enter the marketplace without proper security measures being put into place to prevent malevolent third parties from communicating with the children involved?[26]

We consequently share the concern expressed notably in whereas clause 38 of the EU Regulation, as demonstrated in point (f) of the first subparagraph of Article 6, in Article 8 and in subparagraph one of Article 12, among others, concerning the need, for data collection and

[23] Regarding the content of contracts and policies, see in particular: Plourde, *How Free is "Free"?*, pp. 24–29 and Bélanger-Krams, pp. 53–63.
[24] In this regard, see also: Plourde, *How Free is "Free"?*, p. 44.
[25] Hunt, Troy. *Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages.* Blog, 28 February 2017, consulted at: https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/.
[26] Huggler, Justin. "Germany bans internet-connected dolls over fears hackers could target children." *The Telegraph*, London, 17 February 2017, consulted at: http://www.telegraph.co.uk/news/2017/02/17/germany-bans-internet-connected-dolls-fears-hackers-could-target/.

processing purposes, to obtain consent and ensure transparency when it comes to obtaining and using personal information relating to or supplied by children. We also agree with the pith and substance of the recommendations made in this regard by the Public Interest Advocacy Centre in the brief it submitted to the committee on 20 February 2017.[27]

Moreover, the Canadian legislative framework makes few distinctions respecting the types of personal information being processed; this is not the case in Europe, where Article 9 of the EU Regulation establishes specific rules governing the more "sensitive" categories of information. While it is unlikely that this regime could be imported to Canada in its entirety, we should consider paying particular attention to information of a "biological" nature (e.g., genetic, biometric, metabolic and pathological information) by requiring particularly well-informed consent, and we should pay closer attention to consent issues regarding the growing amounts of information simultaneously involving two or more individuals who might have differing interests or express different wishes regarding the processing of that information.

2.2.4 The right to be forgotten

Is it necessary for our virtual twin to enjoy eternal life, even when it is not in the public interest to preserve information about this doppelganger? We don't think so. That being said, there is no cure-all remedy that can resolve all of the problems that can arise from the continued indeterminate storage of information which an individual may have considered relevant at one time, but which now seems useless, obsolete or ambiguous to that same individual. Nor do we believe that an individual should only be able to ask for information to be expunged if it is inaccurate or contains, for example, some aspect that can be deemed harmful to the individual's reputation. A person's control over the information which concerns him or her is what characterizes our personal information management system, and it should be possible to exercise this control flexibly and easily, subject to the existence of higher interests benefiting other individuals or the community at large.

We believe, consequently, that a wide range of simple and effective measures should be put in place that will make it possible for an individual to have information withdrawn, in particular online content that can be variously detrimental to the individual's interests and rights, including the right to dignity.[28] The right to be forgotten, as set out in Article 17 of the EU Regulation, should be part of this arsenal available to individuals. In this regard, we support the recommendations made by the Public Interest Advocacy Centre in its aforementioned brief to the committee.

[27] Lawford, John and Lau, Alysia. *Final written submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics – Review of PIPEDA*. PIAC, Ottawa, 20 February 2017.
[28] Plourde, *Paying for Oblivion*.

2.2.5 Other concerns

Some problems which form the subject of specific provisions of the EU Regulation are either overlooked or not satisfactorily addressed in Canadian statutes. We believe that, in order to improve the Canadian regime and ensure its adequacy for the purposes of Article 45 of the EU Regulation, it would be appropriate to draw inspiration in this regard from current European rules.

First of all, the status and obligations of processors and of those who assign various tasks to them, for example, are framed extensively in Articles 24, 26 and 28 of the EU Regulation.

Next, the right to data portability forms the subject of Article 20 of the EU Regulation. Adopting a matching approach in Canada would have clear benefits for individuals, and would also favour mobility and competition in various marketplaces.

Moreover, the territorial application of PIPEDA should also be examined. Under section 4 of the Act, as currently written, PIPEDA applies first and foremost to organizations located in Canada, and consequently to the operations that are conducted in Canada. In contrast, Article 3(2) of the EU Regulation clearly stipulates that the EU Regulation applies not only to operations conducted within EU States but also to certain operations directed at persons in the European Union, even if the organization responsible for the processing activities is physically located outside the European Union. In our view, this concept of jurisdiction based on the location of the person, which matches the approach used in private international law with respect to consumer protection, should be incorporated into PIPEDA.[29]

With respect to the cross-border flow of data, we note that Article 45(2)a) of the EU Regulation stipulates that decisions regarding the adequacy of the level of protection shall take account of the rule of law in a third country (in this case Canada) regarding the subsequent transfer of personal information from the European Union to another country. In our view, PIPEDA could benefit from greater precision in this regard.

2.2.6 Powers of the Commissioner

For the system put in place by PIPEDA to be effective, its implementation must be assured. When PIPEDA was enacted, we felt that the legislation did not confer upon the Privacy

[29] The legal characterization of matters pertaining to personal information management is both complex and delicate; it is generally acknowledged, however, that matters associated with status of a person are governed by the laws of his or her place of residence, whereas Article 5 of the *1980 Rome Convention on the Law Applicable to Contractual Obligations*, for example, stipulates that "a choice of law made by the parties shall not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence." Since the vulnerability of persons whose personal information is being processed is frequently analogous to that of consumers, it would be advisable to incorporate a similar rule into PIPEDA in order to protect Canadians doing business with companies located abroad. The full text of the Convention may be found at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:41998A0126(02)&from=EN.

Commissioner the duties and powers the Commissioner would need to ensure its enforcement. Despite the efforts deployed since then by the Office of the Privacy Commissioner, we still believe that it should have more wide-reaching powers (and far more resources – although this is a matter for an entirely different debate). Consequently, we share the views expressed by professor Gautrais and the Public Interest Advocacy Centre on this subject.

Articles 57 and 58 of the EU Regulation indicate the extent to which the supervisory authorities of the individual EU member states have a broad range of mechanisms and powers that extend their range of action from investigations to warnings, orders and penalties, as required. Such penalties, in the form of administrative fines levied against undertakings, can in the most serious cases be "up to 4 % of the total worldwide annual turnover [sales]" achieved by an offender in the previous fiscal year (Article 84(6) of the EU Regulation). In the case of Facebook, for example, such an administrative fine could amount to more than a billion Canadian dollars.[30] This is enough to deter any undertaking...

Moreover, we believe that increasing the powers of the Privacy Commissioner, far from restricting the Commissioner's ability to act, would enhance the credibility of the Office of the Commissioner. While the diversification of these powers, including the establishment of monetary administrative penalties, may require certain administrative arrangements to ensure that the rights of the organizations subject to PIPEDA are respected, it appears to us that the legal characterization recently assigned to such penalties by the Supreme Court of Canada[31] ensures that it is entirely possible to reconcile a wide range of powers within an agency such as the Office of the Privacy Commissioner.

The obligations of organizations once they are alerted to deficiencies in their security measures, or once they determine the existence of such deficiencies, should also be specified. Such organizations should be legally required to diligently apply adequate corrective measures, and they should notify the persons concerned in cases where personal information may have been compromised. Articles 33 and 34 of the EU Regulation set out obligations in the latter regard.

3. Conclusions and recommendations

3.1 Looking to the future

Emerging concerns regarding the automated processing of personal information prompted the Organisation for Economic Co-operation and Development (OECD) in 1980 to adopt guidelines

[30] According to summary financial statements issued by Facebook, the company recorded sales in 2016 totalling US$26.885 billion (consulted at: https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx). Four percent (one twenty-fifth) of that amount represents more than US$1 billion.

[31] *Guindon v. Canada*, 2015 SCC 41, [2015] 3 S.C.R. 3.

to frame practices that were increasing in number and generating more and more confusion, notably in light of the growing diversity of legislative approaches that had been improvised by individual authorities baffled by how to go about dealing with the mushrooming problems in this area.[32] These guidelines, revolving around respect for an individual's control over his or her personal information, sought in particular to foster a certain degree of legislative harmony while restoring public confidence in the ultimate fate of personal information – two objectives that remain entirely commendable. Moreover, these guidelines still form the backbone of virtually all legal frameworks governing personal information management, including those of the European Union and Canada. However, things have changed completely since then.

In 1980, the focus was on personal information processing by public agencies and major corporations, which were the only organizations at that time able to harness the information technology infrastructure required for this purpose. Still in its infancy, microcomputer technology was still a few years away from truly taking off.[33] A primitive version of the Internet (then known as the ARPANET) already existed, but it linked only a few academic and government institutions.[34] The worldwide web would not be invented until 1989, and would not become really accessible to the public until 1991. It is worth noting that Google was founded in 1996 and Facebook in 2004. Twitter came into being in 2006.

When the OECD guidelines were adopted, matters were relatively simple: a large organization collected information from individuals, most often directly and for purposes that could be clearly defined; in addition, this organization had the necessary resources to adequately notify affected individuals if any problems arose concerning personal information. Consequently, these were bilateral relationships, the ins and outs of which could be readily understood by people if they received adequate explanations.

As noted in section 2 of this brief, the landscape has now become far more complicated. Millions of organizations of all sizes are gathering and exchanging information that is much more diversified in nature, for purposes that can grow like wildfire as marketing whizzes come up with new ideas, within remarkably complex networks and through means that are often undetectable and largely unintelligible to the average user. That being said, anyone who refuses to jump into this rushing data stream runs the risk of being socially and even economically isolated.

This consequently raises an important issue. Is the framework established in 1980, which is modelled on a contract between an individual and an organization and founded on an exchange of informed consent, adapted to this new, far more complex and increasingly incomprehensible

[32] Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris, 1980. These guidelines, in the form of a Recommendation by the Council of the OECD, were adopted on 23 September 1980. The full text of the guidelines is available on the OECD website at: http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm.

[33] IBM (which led the way in developing the computer market) started selling its first personal computer in 1981. The Apple Macintosh PC entered the market in 1984. Although various models of microcomputers had been under development since the 1970s, the phenomenon only became really significant a decade later.

[34] The TCP and IP protocols were implemented in 1983, and the removal of the military segment from the rest of the network in 1984 resulted in the creation of what we now know as the Internet.

universe? If the answer is no, then we are truly facing a Copernican revolution...and we suspect that this is in fact the case.

We are aware of the problems, discussed earlier in this brief, that clearly go hand in hand with the concept of consent. Soon, however, we will have to consider the status of information gleaned from things possessed by individuals and capable of making decisions on their own that could alter the information profiles of those individuals. Moreover, information can concern more than one individual; examples include genetic data and group photographs. What are the rights of each individual in such cases and how far do they go? As noted earlier in this brief, we remain perplexed by the framework governing information concerning deceased persons who are no longer able to provide consent. The straightforward person/consent/organization model can no longer be adequately applied to events as we see them. A new paradigm is needed.

The fourth whereas clause of the EU Regulation reminds us that "the processing of personal data should be designed to serve mankind." Our fate should not be dictated by the fate of our virtual twins, and it is up to us to exert control over these twins as much as possible. However, this task is growing in complexity even as it becomes more urgent.

In 1532, François Rabelais reminded us that all things come to those who wait, but it is now clear that our society cannot afford to wait much longer for a reliable and coherent framework to govern the use of data. This need is now vital in our hyper-linked world.

We know full well that the review which the committee is embarked upon cannot resolve this new order of problems. But we feel it would be important to point out the need for a fundamental examination of this issue and perhaps propose a research program that would strengthen the horizon scanning that is required and, in particular, would rely on the active participation of all stakeholders in society, including consumer organizations.

3.2 In the meantime...

In the shorter term and within the scope of the committee's present terms of reference, taking into account the comments set out above in this brief, we have consequently formulated recommendations pertaining on the one hand to legislative amendments and on the other hand to the pursuit of research and information work.

1. Option consommateurs recommends that the committee propose to amend PIPEDA in order to incorporate into it:

(a) provisions stipulating that the Act applies in general to the processing of data concerning persons who are usually domiciled in Canada;

(b) obligations concerning the integrated protection of data right from the design stage of information collection and processing mechanisms (i.e., protection by design);

(c) **obligations concerning the conduct in advance, by the organizations designing such mechanisms, of impact assessment studies in those cases that require such analyses;**

(d) **rules setting out the sharing of responsibilities among controller organizations and their processors;**

(e) **obligations concerning the form in which information is provided to the persons concerned, in order to guarantee that such information is concise, transparent, comprehensible, readily accessible, and formulated in clear and precise terms;**

(f) **measures to control the validity, in adhesion contracts, of provisions to obtain the consent of the people concerned, in order to ensure that such provisions do not unduly or unreasonably disadvantage those persons and can be invalidated in whole or in part as required;**

(g) **measures allowing persons concerned to qualify the consent they provide and, in particular, to oppose tracking when it is not necessary;**

(h) **measures to enable a rigorous and transparent framing of automated decision-making mechanisms, which should be subject to specific control by the Privacy Commissioner;**

(i) **measures focusing specifically on the protection of children;**

(j) **measures to specifically establish a framework governing the use of information pertaining to deceased persons;**

(k) **measures to facilitate the withdrawal, upon the request of an individual, of information pertaining to that individual – such measures to include implementing a form of right to forget and delineating the obligations imposed upon an online intermediary informed of the false or defamatory nature of a piece of information;**

(l) **measures to establish a data portability regime;**

(m) **measures requiring organizations to diligently keep track of information transmitted to them that exposes the vulnerability of their systems and in particular of their security measures, and to notify persons affected by any failings as required; and**

(n) **measures substantially expanding the duties and powers of the Office of the Privacy Commissioner, including the putting into place of a dissuasive system of administrative monetary penalties.**

2. **Option consommateurs recommends that the committee propose to the Privacy Commissioner or other competent authorities that research be conducted in the near future on:**

(a) the increasingly important role played by personal information as a mode of payment, or as an accessory to modes of payment, and the risk of socioeconomic exclusion that can arise from this;

(b) a framework for the use of biological information, including genetic, biometric and metabolic information, as well as other types of so-called "sensitive" information;

(c) the effective implementation of the necessity principle in the collection and use of personal information, within the actual current practices of the organizations that are subject to the Act;

(d) the workings and effect of automated decision-making processes;

(e) a framework for the use of information that simultaneously concerns more than one physical individual and the particular problems that such situations may entail;

(f) the economic and social impact of the hypermnesia of the web, which tends to never forget anything; and

(g) a review of the conceptual framework underlying our personal information protection system, in order to adapt it as necessary to observed fundamental changes in personal information management practices.

3. Option consommateurs recommends that the committee propose to the Privacy Commissioner or other competent authorities that particular emphasis be placed on information efforts to:

(a) make the public, organizations and professionals concerned more aware of issues stemming from the problem of digital death;

(b) make the public and organizations more aware of the particular risks associated with information concerning children; and

(c) make the public and organizations more aware of the fact that, in principle, a person cannot be required to provide information that is not necessary for the performance of an operation.