Implementing Standard Privacy Settings

Submissions on the Privacy Commissioner's Discussion Paper on Privacy and Consent

Public Interest Advocacy Centre
Written by: Ben Segel-Brown
Edited by: John Lawford

Summary

Canadian consumers generally are not aware of and do not understand how information about their online activities is being collected and used. The problem is not that online businesses are unable to obtain consent, but that consumers' personal information too often is being used without meaningful consent.

PIPEDA requires online business to obtain informed consent for the collection, use and disclosure of individuals' personal information. Individuals' privacy rights are undermined by accepting hollow 'contractual-type' consent. Requiring true informed consent serves the objectives of privacy law, including giving user's confidence in sharing the information required to engage in online transactions, enhancing user's informational self-determination, and giving effect to the preferences of users as consumers and as citizens.

The current protections of PIPEDA must not be undermined to allow online businesses to collect, use, and disclose personal information against the will of consumers. The solution to online businesses abusing such personal information is not the relaxation of those rules, but stricter enforcement of the requirements for meaningful, informed consent set out in PIPEDA. To this end, the Privacy Commissioner should be given the power to make orders and impose fines.

Among the solutions proposed to enhance consumer control over their personal information online, we favour:

1. the implementation of a standard set of privacy preferences,
2. the implementation of a trustmark system,
3. tagging data to indicate limitations on its use and disclosure.

We are concerned that many of the proposed "Alternatives to Consent" are means of allowing online businesses to collect, use, and disclose personal information against the wishes of, or without the true informed consent of, consumers. De-identification and contractual backstops are useful strategies for minimizing the risks of authorized collection, use, and disclosure. They are not, however, alternatives to consent.

We support the defining of zones where collection, use and disclosure of personal information is prohibited irrespective of consent. We also support defining caution zones where the risk of harm means more disclosure and sensitivity around informed consent is required. We particularly support the implementation of age restrictions reflecting the capacity of children to provide informed consent.

Industry codes of practice and ethical assessments are no substitute for proper regulation. Allowing self-regulation in lieu of consent would not be reducing the transaction costs involved in explaining a use and seeking consent, it would be overcoming the will of most consumers.

Introduction

This paper has been prepared in response to the Office of the Privacy Commissioner's call for submissions on its *Consent Discussion Paper*.[1] This paper addresses four broad questions posed in that paper:

1. What solutions to reconcile privacy and consent have the most merit and why?
2. What solutions have not been identified that would help address challenges with consent?
3. What roles and responsibilities should each party play in advancing these solutions?
4. What legislative changes are required?

This paper also addresses some of the sub-questions posed in that paper and the broader theme of privacy and consent.

We are required to state:

1. We have read and understood the consultation procedures.
2. The Public Interests Advocacy Centre is an advocacy group representing the interests of consumers. We are not affiliated with industry, regulators, political parties or government.
3. The opinions expressed in this document are those of the author(s) and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada.

Identification of Problem

Canadian consumers generally are not aware of and do not understand how information about their online activities is being collected and used. Our organization, the Public Interest Advocacy Centre, commissioned a nationally representative survey to better understand consumer awareness and attitudes towards online privacy and consent.[2] We found that about half of consumers are not very or not at all familiar with consumer surveillance and the technical tools used by business to track their activities online.[3] This problem was particularly acute for those with lower incomes and education.[4]

In addition to not being aware of the degree to which their behavior is being tracked online, most consumers do not want to be tracked online, even if they are aware. Most (74%) were not very comfortable or not at all comfortable with online tracking for the purpose of behavioral advertising, and

---

[1] That paper is available on the Office of the Privacy Commissioner's website at https://www.priv.gc.ca/information/research-recherche/2016/consent_201605_e.asp

[2] Public Interest Advocacy Centre, *A Do Not Track List for Canada?* (Ottawa: PIAC, 2014), online: <https://www.piac.ca/our-specialities/tracking-consumers-online-behavioural-targeted-advertising-and-a-do-not-track-list-in-canada/>.

[3] *Ibid.,*at 82. When asked whether they were familiar with the existence of tracking devices and techniques like cookies and Web Beacons, 31% indicated they were not at all familiar while 19% indicated they were not very familiar.

[4] *Ibid.,*at 83. 42% of persons with incomes under $20k and 46% of people with less than a high school education indicated they were not at all familiar with web tracking, compared with 33% in the general population.

even more were uncomfortable with information about their behaviors being shared with third parties. [5] Most (81%) supported the creation of a "Do Not Track" list and most (70%) also indicated that they would sign-up for a "Do Not Track List" if one was available. [6] This mirrors results of the Eurobarometer 431 survey which found that 86% of Europeans believed that their consent should be required for any kind of personal information is collected.[7]

As stated in the Office of the Privacy Commissioner's Guidelines for online consent:

> Under privacy laws, organizations are required to obtain meaningful consent for the collection, use and disclosure of personal information. Consent is considered meaningful when individuals understand what organizations are doing with their information.[8]

Since many users do not understand the information being collected about them and how it is used, it follows that businesses are not obtaining the required meaningful consent from many consumers for the collection, use, and disclosure of their personal information. In many cases, consent purportedly is obtained through acceptance of legalistic privacy policies which no individual could realistically hope to read and understand. Privacy policies are too long, too unclear, and too hard to understand to support the assumption that any assumed consent is meaningful or informed.[9]

The burden of obtaining meaningful consent, however, falls on businesses. The problem is not that businesses are unable to obtain consent for 'innovative' ways of exploiting consumer data. The problem is that often the lack of consent to these activities reflects consumer preferences. Consumer's unwillingness to consent to 'innovative' uses should be a barrier to such uses. The problem is that consumers' personal information is being used where meaningful consent has not been given – in our view, in many cases precisely because most individuals would not give consent to such uses.

Theory of Consent

Consent in a fundamental principle underlying Canada's privacy regime. Not only is it one of the Principles of the Model Code for the Protection of Personal Information, but it is the core mechanism used to determine whether or not the collection, use or disclosure of personal information should be

---

[5] *Ibid.,*at 11, 84, 86. When asked whether they were comfortable with their online activity being tracked for the purposes of targeted advertising, 49% indicated they were not at all comfortable with being tracked for that purpose, and 25% indicated they were not comfortable with being tracked for that purpose.

[6] *Ibid.,*at 92, 94.

[7] European Commissions, *SPECIAL EUROBAROMETER 359: Attitudes on Data Protection and Electronic Identity in the European Union (Report)* (2010), online: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> at 149. 74% of Europeans believed that their consent should be required for any kind of personal information is collected, with a further 12% believing consent should be required for personal information collected on the internet, and a further 8% believing consent should be required for sensitive information.

[8] Office of the Privacy Commissioner, *Guidelines for Online Consent* (2014), online: <https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp> at 1.

[9] European Commissions, *SPECIAL EUROBAROMETER 359: Attitudes on Data Protection and Electronic Identity in the European Union (Report)* (2010), online: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> at 87.

permitted in lieu of prescribing what collection, use and disclosure is desirable.[10] Before considering any changes to such a fundamental principle, it is important to talk about what we mean by consent and why we consider it important.

There are conflicting models of "consent" in the legal context. Contract law has developed a hollow theory of consent which will infer consent where a party has notice of terms and indicates their assent to those terms. Other fields, notably health law, require informed and specific consent predicated on an understanding the risk of harm arising from a choice. The obligation is on a doctor to ascertain whether the patient fully understands the risk of the choice they are making.[11]

Informed consent is explicitly required under PIPEDA. Section 6.1 specifies that

> […] 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 they are consenting.[12]

Specific and informed consent is also the standard for the EU. EU Data Protection Directive defines 'consent' not in terms of notice and assent to terms, but rather whether there is "any freely given specific and informed indication of [the data subject's] wishes […]" (Article 2(h)). The directive further specifies the information that must be provided to a data subject in order to satisfy this element.[13] The vast majority of consents obtained by online business would not meet this standard.

The hollowing out of consent in Canadian Contract Law

Originally, contract law required a meeting of the minds on the essential terms of the contract. This means that the parties must have identical or similar mindsets regarding the details of the contract they enter into. This theory worked well for the individual negotiation of contracts between parties who were physically present before each other and whose terms were not overly complex.[14]

However, to add an element of objectivity, the courts found a meeting of the minds where a party had notice of the terms and a reasonable observer would conclude they have consented to the terms. [15] Over time, this objective test for of a meeting of the minds has become a substitute for a meeting of the minds, where parties are bound if they have reasonable notice of reasonable terms. The requirement of notice, outlined in *Thornton v Shoe Lane Parking Ltd*, requires only that a business take sufficient steps

---

[10] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880 (2013), online <http://ssrn.com/abstract=2171018>.
[11] *Reibl v Hughes* [1980] 2 SCR 880. See also Frederik J. Zuiderveen Borgesius, *Informed Consent: We Can Do Better to Defend Privacy* ,<http://ssrn.com/abstract=2793769>.
[12] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 8.
[13] EU Directive 95/46/EC at Articles 2, 49.
[14] Dasuni Wijayasriwardena, *Consent in Online Contracts – Mindless or Mindful?* Queen Mary University of London, School of Law Legal Studies Research Paper No. 234/2016, online <http://ssrn.com/abstract=2783793> at 7-10.
[15] *Ibid.*

to bring the terms and conditions to the notice of the consumer before acceptance occurs,[16] subject in turn to a requirement to bring particular attention of the contracting party to exemption clauses.[17]

Canadian courts have extended this theory to online contracts, holding that a click indicating asset to terms and conditions is binding even though it may be obvious to the business and any reasonable observer that the consumer will not have read those terms.[18] In some cases, acceptance of terms and conditions has been held to occur merely by using a website or carrying out certain actions on it, depending on the prominence of the terms and conditions on the website. [19]

Applying this contractual consent or "offer and acceptance" model to online privacy analysis is unhelpful as it leads to an assumption that individuals do not have ultimate control of their personal information on an informed consent basis. That is, if "reasonable notice" of "information use" is made, consent is implied or deemed. However, when individuals are unaware of the contents of such notices, no true informed consent can be obtained. Yet that is effectively what is proposed if this model is accepted.

Why reasonable notice is insufficient in the online privacy context

Accepting reasonable notice of terms in the online context is problematic because few users will read those terms. Surveys and website visitor tracking show that very few users – about 7% – read the terms and conditions.[20] As a result, businesses have little to lose by imposing extremely invasive terms. Often, those terms essentially provide that users consent to unlimited collection, use, and disclosure of their personal information.[21]

More fundamentally, it seems unfair to transfer rights from user to business simply on the basis of an opportunity to read the terms when the user has not read the terms and the business could not reasonably have expected them to have done so.[22]

Theorists have developed more precise descriptions of the limitations of consent conveyed by online agreements. Barnett argues that there is consent to the terms the user is likely to have read and those

---

[16] [1971] 2 QB 163 (CA).
[17] *Tilden Rent-A-Car Co.* v. *Clendenning*, [1978] O.J. No. 3260, 18 O.R. (2d) 601 (Ont. C.A).
[18] *Kanitz v Rogers Cable Inc*, 58 OR (3d) 299; 21 BLR (3d) 104, 2002 CanLII 49415 (ON SC), <http://canlii.ca/t/1w1c2>; *Rudder v. Microsoft Corp*., 2 CPR (4th) 474; 47 CCLT (2d) 168, 1999 CanLII 14923 (ON SC), <http://canlii.ca/t/1w8rg>.
[19] *Century 21 Canada Limited Partnership v Rogers Communications Inc*, 2011 BCSC 1196 (CanLII), <http://canlii.ca/t/fn00h>.
[20] Dasuni Wijayasriwardena, *Consent in Online Contracts – Mindless or Mindful?* Queen Mary University of London, School of Law Legal Studies Research Paper No. 234/2016., online <http://ssrn.com/abstract=2783793> at 26.
[21] As a humorous example, in an April Fools prank, Gamestation included a provision signing over the user's immortal soul to which 7,500 users (88%) agreed, even with a specific link allowing users to opt out of the soul transfer and receive a $5 coupon. Huffington Post, *7,500 Online Shoppers Accidentally Sold Their Souls To Gamestation,* online: <http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html>.
[22] Dasuni Wijayasriwardena, *Consent in Online Contracts – Mindless or Mindful?* Queen Mary University of London, School of Law Legal Studies Research Paper No. 234/2016., online <http://ssrn.com/abstract=2783793> at 13-15.

terms the user is not likely to have read that are not unreasonable.[23] Brownsword argues that a more realistic and honest evaluation of the circumstances of the contract is needed to determine whether contractual obligations arise, where consent is only one factor to be considered alongside negotiating power and the reasonableness of terms.[24] What these theories convey is that consumers should not be bound by online terms and conditions which businesses could not realistically expect consumers to have actually read and agreed to.

Quite apart from these modified "contractual" theories of consent, however, there is a more fundamental argument about the consent that PIPEDA requires. Namely, it is that privacy affects the individual like a physical touch or invasion of space, as with consent in the medico-legal context.

The medical model of specific and informed consent is an appropriate analogy for privacy

Personal information is not just a property right. The right to privacy is a personal right central to individuals' dignity. In EU jurisprudence, it is a fundamental human right.

Surgery, or indeed any touching, whether or not "in a medical context", or performed by a health professional without consent is battery, a tort – an actionable wrong. Similarly, the unauthorized collection, use, and disclosure of personal information arguably now has been legally recognized asa tortious wrong. The tort of intrusion upon seclusion arises where a defendant intentionally or recklessly invades the plaintiff's private affairs, where a reasonable person would regard the invasion as highly offensive, causing distress humiliation or anguish.[25] Another privacy tort, for the public disclosure of embarrassing private facts has been recognized in the context of playing a secret recording at a public meeting and publishing an intimate video without consent.[26] A breach of confidence may also be made out where confidential information, imparted in circumstances importing an obligation of confidence, is used for an unauthorized purpose to the detriment of the party communicating it.[27] All of these threads are leading to a legal recognition of privacy violations generally becoming a tort.[28] In all of these cases, "consent" is clearly meant as informed consent. The issue arose squarely in *Englander* v. *Telus Communications Inc.*, 2004 FCA 387, in which the Federal Court of Appeal found that (even prior to the Act's amendment to add s. 6.1) that PIPEDA requires informed consent (at para. 56):

---

[23] Frederik J. Zuiderveen Borgesius, *Informed Consent: We Can Do Better to Defend Privacy*,<http://ssrn.com/abstract=2793769>at 37.
[24] *Ibid.*at 38.
[25] *Jones v Tsige*, 2012 ONCA 32.
[26] *Saccone v Orr* (1981); Doe *464533 v ND*, 2016 ONSC 541 at para 46-47.
[27] *Doe 464533 v ND*, 2016 ONSC 541.
[28] See especially *Somwar* v. *McDonald's Restaurants of Canada Ltd.* (2006), 2006 CanLII 202 (ON SC), 79 O.R. (3d) 172, [2006] O.J. No. 64 (S.C.J.) at para. 29:

> With advancements in technology, personal data of an individual can now be collected, accessed (properly and improperly) and disseminated more easily than ever before. There is a resulting increased concern in our society about the risk of unauthorized access to an individual's personal information. The traditional torts such as nuisance, trespass and harassment may not provide adequate protection against infringement of an individual's privacy interests. Protection of those privacy interests by providing a common law remedy for their violation would be consistent with Charter values and an "incremental revision" and logical extension of the existing jurisprudence. . . . . .

> Principles 2, "Identifying Purposes," and 3, "Consent," are at the heart of this appeal. Principle 3, I hasten to add, despite its name, "requires `knowledge and consent'" (clause 4.3.2). *In other words, Principle 3 requires informed consent*. [Emphasis added.]

PIAC believes that the medico-legal conception of consent therefore is the better model for PIPEDA's privacy consent standard and indeed that PIPEDA legally requires informed consent. This consent standard preserves the individual's control, his or her dignity, and avoids unwanted interference with the individual's informational profile and space.

Why we protect privacy

There are a few theories underlying the protection of privacy, but each supports requiring meaningful (and informed) consent to the collection, use, and disclosure of personal information theory.

One theory is that quoted in the OPC discussion paper, namely the Westin theory, that "privacy [is] rooted in personal autonomy, which in turn underpins our democratic system." It is based on individual control of information about that individual which provides a sense of autonomy – which in turn provides a check on state power as each individual is freely able to express his or her opinions and to act relatively freely.

Another theory is that "privacy is necessary if we are to maintain the variety of social relationships with other people."[29] Under this theory, requiring specific and informed consent will allow people to provide information online more freely, confident that their privacy will not be undermined by a term buried in an organizational Privacy Policy. As stated in the Office of the Privacy Commissioner's Guidelines for online consent, "If people are confident about putting their personal information online, they can more fully participate in the digital economy, which will spur innovation and create economic benefits for Canada."[30]

American theories of privacy focus on privacy as freedom from intrusions by the state. Privacy is seen as a means of carving out a zone for people to engage in personal and political activities free from government. [31] Government can make extensive use of information collected by private parties, even Google Search queries.[32] Limiting the collection and disclosure of personal information by the private sector through the nominal acceptance of Privacy Policies will help to prevent the purchase or expropriation of that information by governments.

---

[29] James Rachels, "Why Privacy is Important" (1975) 4:4 Philosophy & Public Affairs 323 at 326.
[28] Office of the Privacy Commissioner, *Guidelines for Online Consent* (2014), online: <https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp> at 1.
[31] Gabriela Zanfir, "EU and US Data Protection Reforms: A Comparative View" (Paper delivered at the7th edition of the International Conference on European Integration: Realities and Perspectives, 10 March 2012), online: SSRN <http://ssrn.com/abstract=2079484> ["in the US, privacy protection is essentially liberty protection, i.e. protection from government, while for Europeans, privacy protects dignity or their public image" at 218]; Edward J Eberle "The German Idea of Freedom" (2008) 10 Oregon Rev of Int'l L 1at 2.
[32] Shoshana Zuboff, *The Secrets of Surveillance Capitalism*(2016) in Frankfurter Allgemeine Zeitung, online:<http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616-p2.html?printPagedArticle=true>.

European theories of privacy generally focus on privacy as a right to informational self-determination. Alan Westin echoes this body of thought when he emphasizes the importance of privacy as a social process safeguarding individual dignity and individuality,[33] yet there are elements of civil law thinking in the European regulation that allows for collective good to in some cases override pure individualism.

A final populist theory is that privacy should be protected because Canadians want their privacy to be protected.[34] Our surveys indicate that most Canadians do not want to be tracked online and Canadians think that they should be able to choose not to be tracked online without their specific informed consent.[35] Such a theory, however, lacks a normative basis and can change depending upon popular viewpoints of the day.

To sum up, however, all of these theories of why we protect privacy to a greater or lesser extent value individual control. Control over one's personal information allows individuals to self-actualize and function more fully in society. Proposals to weaken consent therefore can be seen as an attempt to wrest control and autonomy from individuals, most often to benefit business or the state.

Of the solutions identified in this paper, which one(s) has/have the most merit and why?

The current protections of PIPEDA must not be undermined to allow online businesses to collect, use, and disclose personal information against the will of consumers. The solution to online businesses abusing such personal information is not the relaxation of those rules, but stricter enforcement of the requirements for meaningful consent set out in PIPEDA. To this end, the Privacy Commissioner should be given the power to make orders and impose fines.[36] Furthermore, the burden should be shifted to businesses to establish that they have complied with PIPEDA where a bona fide complaint is received.

---

[33] Office of the Privacy Commissioner of Canada, *Consent and Privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* (May 2016), online: <https://www.priv.gc.ca/information/research-recherche/2016/consent_201605_e.asp>.

[34] Ben Segel-Brown, "A Principled Approach to Identifiability", online: <https://www.researchgate.net/publication/305698898_Government_Data_Sharing> at 9.

[35] Most Canadians (74%) were not very comfortable or not at all comfortable with online tracking for the purpose of behavioral advertising, and even more were uncomfortable with information about their behaviors being shared with third parties. Most (81%) supported the creation of a "Do Not Track" list and most (70%) also indicated that they would sign-up for a "Do Not Track List" if one was available. Public Interest Advocacy Centre, *A Do Not Track List for Canada? (2009),* online: <https://www.piac.ca/wp-content/uploads/2014/11/dntl_final_website.pdf> at 82-99.

[36] We note here that at the start of her second term as Privacy Commissioner of Canada, Commissioner Jennifer Stoddart called for order making and fining powers to be added to the OPC toolkit in a speech at the University of Ottawa in early 2011 (just after the finding against Facebook):

> I would also like to take a few moments to talk about incentives for compliance. I am increasingly of the view that we may need stronger powers in order to be an effective privacy guardian for Canadians.
>
> We've become one of the few major countries where the data protection regulator lacks the ability to issue orders and impose fines.

Among the solutions proposed to enhance consumer control over their personal information online, we favour:

1. the implementation of a standard set of privacy preferences,
2. the implementation of a trustmark system,
3. tagging data to indicate limitations on its use and disclosure.

Standard Privacy Preferences

We have developed our own proposal for a standard privacy preferences system.

The foundation for this system would be strict enforcement of the existing provisions of PIPEDA requiring meaningful consent to the disclosure of personal information.

The customer's selection of a global or site-specific privacy preference provides the meaningful consent required to collect, use, and disclose personal information as authorized by that preference.

Communication of Privacy Preferences

The standard privacy preferences will be managed through a web browser plug-in. In an ideal transaction, the plug-in invisibly communicates the user's privacy preference and the website complies with that preference.

If a Canadian has not installed this plug-in, their personal information cannot be collected without their specific and informed consent. Since the website could not recognize the user without tracking personal information, this would be onerous. We expect web browsers would choose to integrate the plug-in for the convenience of Canadian users, and sites would encourage their users to adopt the plug-in. Web browsers would have to authorize no collection, use or disclosure by default, or they would be misrepresenting that users had provided meaningful consent to those activities.

The plug-in will:

1. Locally store the user's privacy preference.
2. Allow the user to review the available privacy preferences in plain language
3. Check a central registry and warn the user unless the website the user is about to visit:
    a. Is configured to handle standard privacy preferences
    b. Has a trustmark and does not have a black mark.
4. Communicate the user's privacy preference to the website via a standard web traffic header
5. If the website refuses the user's privacy preferences, prompt the user to choose whether to provide the requested consent for the site and/or group of sites nonetheless.

We note that Commissioner Therrien has broached the subject of order-making and fining powers, in a speech this year to the IAPP, stating that the question is part of a holistic review of privacy regulation, of which this consent consultation is a part. We urge the OPC to pursue the goal of increasing OPC enforcement powers.

Many security programs already warn users about disreputable sites, and most browsers already allow users to attach a "Do not track" HTTP header to their web traffic. The plug-in also might offer to mask or obfuscate the computer's identity on non-compliant or non-participating sites.

A website may:

1. Invisibly confirm their acceptance of the user's expressed privacy preference and provide their content or services in accordance with that preference;
2. Limit access unless the user allows broader collection, use, and disclosure of their personal information as expressed in a more liberal standard privacy preference. If the site objects, the plug-in will prompt the user to choose whether to provide that more liberal standard privacy preference for that site and groups of similar sites (for example, major Canadian retailers);
3. Request, through their own prompt, that the visitor provides specific informed consent to a particular collection, use, or disclosure of their personal information, in spite of their stated privacy preference for that site.

A similar negotiation of privacy preferences already occurs on many websites when the website encounters a user who has disabled cookies.[37]

Defining Privacy Preferences

The privacy standards would be defined by a body independent of industry, like the Office of the Privacy Commissioner.

The preferences would be expressed in plain language and can be viewed at any time via the plug-in.

The plug-in would allow consumers to specify preferences for groups of websites. The groups would have to be developed based what consumers tend to be willing to entrust with similar levels of personal information. Sites might be grouped based on content (social media platforms), characteristics of the owner (large Canadian business), or whether a site is endorsed by some other privacy management standard (such as those established by civil liberties associations). The option to rely on standards established by non-profits could allow those non-profits to negotiate better privacy terms in exchange for inclusion in a trusted sites group.

Defining informed consent

Any information collected in violation of the user's privacy preferences will be deemed to be a violation of PIPEDA unless the business can demonstrate that the user provided specific informed consent. This conclusion flows from the present requirement of informed consent set out in PIPEDA, Principle 4.3 and s. 6.1.

Specific informed consent could be defined to exist where the overwhelming majority of users (high 90% range) would understand the general nature of the data being collected pursuant to the consent and how it would be used and disclosed.

[37] Cookies are one method of storing unique identifiers to allow websites to track the user.

Understanding the general nature of the information collected could be defined as being able to correctly identify:

1. what data they enter or that is transmitted by a web browser or other app or program will be collected;
2. which of their actions on the website will be collected.

Understanding the general nature of how the information will be used could be defined as being able to correctly identify how the personal information is used:

1. To process the transaction
2. To target the advertisements, content or even layout of the site presented to the user
3. For research

Understanding the general nature of how the information will be disclosed could be defined as being able to correctly identify:

1. Whether the information will be disclosed to a specific third party involved in the transaction;
2. Whether the information will be disclosed to unrelated third-parties, whether immediately or in the future and whether anonymized, de-indentified or not.

Other data collection, use and disclosure, which should be more exceptional, would have to be more specifically identified.

How business will obtain specific informed consent

The discussion paper mentions just in time notices, layered notices, and icons as methods of enhancing consent. These are methods that business might implement in order to demonstrate specific and informed consent. It may be appropriate to specify methods that business could use to achieve informed consent to the standard required by PIPEDA in legislation, regulations or guidelines.

However, these methods also create new risks. Companies may simplify their privacy policies in misleading ways that minimize the risks involved. They may also present consent to those policies at point in the transaction when the user is already invested in the transaction, or in ways which are misleading. Similarly, privacy symbols may be developed by industry=dominated organizations and not fairly represent the risks involved. It would be difficult to regulate in detail how privacy policies are summarized and presented. Any steps forward in this area, therefore, should be developed with a fair and balanced stakeholder input and OPC oversight rather than being developed solely by business groups.

More fundamentally, businesses should seek out business models which incorporate privacy by design. By minimizing the collection, use, and disclosure of personal information, privacy by design will help business avoid needing to seek consent.

Privacy by design strategies include:

1. Minimizing the amount of personal information that is collected and used;
2. Hiding personal data using techniques like encryption, anonymization, and pseudonyms;
3. Separating data, for example by processing and storing data locally where feasible, or by separating anonymized data used for marketing research from identified customer data;
4. Aggregating data, including over time (for example, "aggregation over time" for smart metering) or geographically (for example, "dynamic location granularity" for location based services).[38]

More broadly, privacy by design calls for

1. minimizing the collection of personal information,
2. making privacy the default setting, and
3. planning for maximum privacy from the start of the process.

This idea might seem alien to online businesses, particularly those whose revenue model is based on targeted advertising. But it is certainly possible. For example, rather than requiring users to consent to a lengthy privacy policy, an online newspaper might offer one level of access that required opting-into targeted advertising based on specified information as an alternative to purchasing a subscription. The plug-in might also offer a different level of access without targeted advertising, which included a micro-transactions system to make nominal anonymous payments for access in lieu of revenues that would be generated by the targeted advertising revenues (but still not require a full subscription). Users might specify the financial cost they are willing to tolerate for privately accessing groups of sites. By having the plug-in periodically query websites with the tag, this could also serve as a means of notifying individual in the event of a data breach even if the database does not contain individual's contact information.

There may also be technological solutions to minimize the collection of personal information. For example, rather than uniquely identifying each user and storing their marketing information on a centralized server, it may be feasible to have a user's device hold the personal information and run a provided algorithm to determine for itself the ads it wishes to receive. This avoids the collection of the marketing data by the business.[39]

Privacy by design is more directly applicable to Internet of Things devices, where users should be offered clear privacy choices without being penalized in terms of the device's limited interface or functionality.

---

[38] European Union Agency for Network and Information Security, *Privacy and Data Protection by Design* (2015), online: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> at 19-20. Other "Process oriented strategies" include "inform"; "control"; "enforce" and "demonstrate" which largely map onto similar concepts in PIPEDA's schedule 1.

[39] Consent would still be required to collect the information on the user's device, but this minimizes the privacy risk associated with unauthorized access to such data.

Implementing restrictions on use and collection

Where an individual limits the use and disclosure of data they allow to be collected, that data should be tagged in a standard format indicating those limitations as proposed by the 2013 World Economic Forum (WEF) report Unlocking the Value of Personal Data: From Collection to Usage.[40]

Untagged data would no longer be able to be used or disclosed. Businesses would have to seek specific informed consent to continue to use existing data.

When individual's personal information is collected, they should be offered a unique arbitrary identifier that will be associated with that data. Those identifiers would, if the users opts-in, be stored locally by the standard privacy preferences management system. Eventually, online businesses should be required to implement systems that allow users to use those identifiers to review the personal information kept about them, how it has been used and disclosed, and request corrections or deletion.

Comparison with similar proposals

This is somewhat similar to the proposal outlined in The White House Report entitled Big Data and Privacy: A Technological Perspective.[41] In that proposal, individuals associate themselves with standards established by intermediaries, who will vet apps against those profiles. That proposal carries the benefit of creating a marketplace for the negotiation of better privacy protections between intermediaries and online businesses. However, our proposal also gives individuals an opportunity to have different preferences across sites and allows sites to provide greater privacy protection for users who request it.

This approach is an evolution of the "Do Not Track List" we proposed in our 2009 report, "A 'Do Not Track List' for Canada."[42] That paper proposed to require that businesses check an individual's identifier against a central registry of persons wishing not to be tracked online. The new approach does not require individuals to be uniquely identified and gives individuals great flexibility in allowing some collection use and disclosure of their personal information on selected sites

Precautions to ensure the preferences reflect meaningful consent

Many precautions will have to be taken to keep the system from being used to avoid seeking consent.

Privacy must be the default. Our surveys found that 70% of Canadians would definitely or probably sign up for a do-not-track list, so maximum privacy reflects Canadian's preferences. It also respects the underlying principles of consent: people must select the privacy preference in order for it to provide meaningful consent. Furthermore, we found that 75% of Canadians surveyed preferred an "opt-in"

---

[40] World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage* (2013), online: <http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf>.

[41] Executive Office of the President President's Council of Advisors on Science and Technology, Big Data: A Technological Perspective (2014), online: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf> at 40-41.

[42] https://www.piac.ca/our-specialities/tracking-consumers-online-behavioural-targeted-advertising-and-a-do-not-track-list-in-canada/

consent model to allow tracking by particular websites.[43] American surveys similarly show that most consumers are uncomfortable with online tracking and do not want tailored advertising.[44]

The standard privacy preferences must be defined in plain language by an independent body. Otherwise, industry defined standard preferences would likely arise to pressure customers into accepting lengthy privacy policies granting them free rein to collect, use, and disclose personal information.

There must be a clear higher threshold for organizations to demonstrate consent to collection, use, or disclosure of personal information not permitted by the user's standard set of privacy preferences. Without a higher threshold, business will be free to continue attempting to rely on click wrap and browse-wrap to legalistic privacy policies. The rationale for requiring a higher threshold is that, through their privacy preference, the user has already indicated a general preference not to allow a particular collection, use, or disclosure of personal information. Specific and informed consent is required to overcome that general indication.

Alternatives to Consent

We are concerned that many of the proposed "Alternatives to Consent" are means of allowing online businesses to collect, use, and disclose personal information against the wishes of consumers. If obtaining consent is not practicable because consumers are unwilling to provide their consent, the consent mechanism is working exactly as it was intended to.

Businesses could get by collecting, using, and disclosing far less data. They could also do much more to obtain informed consent.

The state of online consent is somewhat similar to the state of medical consent in the early 1980s. In 1980, the Supreme Court of Canada raised the standard for medical consent to true informed consent. Doctors were suddenly required to inform patients of general and specific risks information that they knew of should have known would be relevant to the patient's decision, and to obtain consent despite that explanation of the risks, instead of merely meeting the standards of the profession.[45] After this dramatic change in the law, the medical community initially responded slowly. By 1984, still only 84% of doctors were aware of the decision. Of those who knew the case, 20% could recall nothing about it and 45% could only recall the specific facts. [46] Even though the change in the law was clear, it took a long time for the new standard to be implemented. PIAC views this situation as akin to the one that online businesses and marketers now face: PIPEDA clearly requires informed consent. Twelve years ago, the

---

[43] Public Interest Advocacy Centre, *A Do Not Track List for Canada?* (Ottawa: PIAC, 2014), online: <https://www.piac.ca/our-specialities/tracking-consumers-online-behavioural-targeted-advertising-and-a-do-not-track-list-in-canada/> at 12.

[44] Public Interest Advocacy Centre, *A Do Not Track List for Canada?* (Ottawa: PIAC, 2014), online: <https://www.piac.ca/our-specialities/tracking-consumers-online-behavioural-targeted-advertising-and-a-do-not-track-list-in-canada/> at 13-4.

[45] *Reibl v Hughes*, [1980] 2 SCR 880.

[46] Gerald B Robertson, *Informed Consent in Canada: An Emperical Study* (1984) 22:1 Osgood Hall LJ 139 at 144.

Federal Court of Appeal held that "Principle 3 [of PIPEDA] requires informed consent."[47] Last year, Parliament amended PIPEDA to add s 6.1, which specifies that "6.1 For the purposes of clause 4.3 of Schedule 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 they are consenting." This is an even clearer statutory requirement for informed consent.

Given time and regulatory pressure, online business will adapt to the requirement of informed consent, much like the medical community in the 1980s. Dire predictions of the loss of innovation, efficiency or "business" should be gauged by this yardstick: companies can adapt to privacy; privacy need not adapt to companies' practices.

Derivations from the principle of consent should only be allowed in the clearest of cases, such as to contact the user in the event of an emergency. The current exceptions in PIPEDA already strike an appropriate balance in this regard.

Consent for the collection, use, and disclosure of de-identified data

In our opinion, individual's consent should be required regardless of whether or not the information is identifiable and therefore constitutes personal information subject to PIPEDA.

Professor Shoshana Zuboff of Harvard University characterizes the data created from use of online services as a "behavioral surplus" which is processed and resold as a tool for predicting and manipulating consumer behavior. She argues that such data should not be used as a free raw material.[48] Users should have the right to control the data they generate, and businesses should have to bargain for the right to collect, use, and resell that data.

The question of whether individuals should have a right to limit the collection and use of anonymous data about themselves can be considered relative to the theories of privacy mentioned above. One reason we protect privacy is to foster social relationships, specifically by giving people confidence in providing the personal information they need to fully participate in the digital economy. People may be uncomfortable with the collection and use of anonymous data, or may even be harmed by the collection and use of such data, undermining their confidence when choosing to provide personal information. Such concerns were raised in relation to the disclosure of aggregated data from Ontario's sex offender registry, where the Ministry of Community Safety and Correctional Services expressed concern that even disclosure of geographically aggregated data would deter sex offenders from registering because "[w]hile identification of an individual could lead to [the harms referred to in the law enforcement exemptions], these consequences can happen in circumstances where no one has been identified.

---

[47] *Englander v Telus Communications Inc*, 2004 FCA 387, [2005] 2 FCR 572.

[48] Shoshana Zuboff, *The Secrets of Surveillance Capitalism* (2016) in Frankfurter Allgemeine Zeitung, online:<http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616-p2.html?printPagedArticle=true>.

Community unease and vigilantism can arise from concern about the presence in the neighbourhood of any registered sex offender regardless of his identity."[49]

In terms of privacy protecting the individual from the state, the collection and use of anonymized data may be abused by the state, as for example city-block level totals of the number of Japanese-Americans were used to locate Japanese-Americans for internment during the Second World War.[50]

As a matter of informational self-determination, anonymized data is constantly used to make generalizations about groups.

Finally, our surveys show that most Canadian consumers do not want to be tracked at all, and think that tracking should be opt-in. So, limiting the collection and use of anonymous data would reflect Canadian's preferences both as consumers and as citizens.[51] Consumers should be able to chose whether to "feed the beast" of big data – even with "anonymized" data.

PIAC is of this view because consent for the collection and use of some de-identified data may already be required by law. At the time data is collected it is usually identified, identifiable, or at least potentially identifiable. Consequently, the user's consent is required for the data collection. Further processing of the data to de-identify it is a use of the data. The user's consent is therefore required for that use. Needless to say, the user's consent would also be required for further disclosure of this anonymized or aggregated information.

A user's consent may also be required when a website stores information on a user's own device, such as in a cookie. Such data is "collected" in the sense of being recorded and in the sense of being kept for the use and benefit of the website.

Nevertheless, there is sufficient uncertainty in this area that the Office of the Privacy Commissioner could consider whether guidelines or legislative amendments are needed to clarify the circumstances under which data can be collected, and then purportedly "anonymized" and used or further disclosedwithout consent.

Criteria for assessing risk of re-identification

The scope of information which should be considered "identifiable" and therefore personal information needs to be better developed. PIAC would consider information personal if:

1. From a statistical perspective, there is a reasonable possibility of information being revealed about any protected individual, either by cross-referencing with data which is or is expected to

---

[49] *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 at 39, [2014] 1 SCR 674.

[50] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (2010) 57 UCLA Law Review 1701, online <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006> at 1756.

[51] Public Interest Advocacy Centre, *A Do Not Track List for Canada?* (Ottawa: PIAC, 2014), online: <https://www.piac.ca/our-specialities/tracking-consumers-online-behavioural-targeted-advertising-and-a-do-not-track-list-in-canada/>.

be publically available or by using personal knowledge, with sufficient certainty that it may affect the individual.

2. From a broader perspective, there is a reasonable possibility of re-identification being attempted taking into account: the time and cost required to identify the individual, the purpose for which the information is being provided, incentives for re-identification, and undertakings by confidential recipients.

This test, outlined and explained in the author's paper, *Government Data Sharing*, would include some "de-identified" or "anonymous" data.[52]

At the first stage, it includes some situations where attribute disclosure, totals, or probability reveal information about an individual. It includes situations where any individual is identifiable, even if the vast majority are not. It includes situations where information which may be publically available in the future could facilitate identification. Where the information relates to small groups, it includes information which would be identifiable through personal and tacit knowledge. It includes false information and probabilistic information if there is sufficient certainty to affect the individual.[53]

At the second stage, this approach sets a higher threshold for anonymization of valuable or desirable data, and for data that is easily processed data. It includes all data kept for the purpose of identifying individuals. It gives greater lenience where there the data recipient is a trusted party with appropriate safeguards in place and no interest in identifying individuals. Conversely, it gives less lenience where information is being sold to an untrusted party.

Almost any individual level of data and some aggregate data are subject to some risk of re-identification and should be considered personal information subject to PIPEDA.[54]

While de-identification is not a substitute for consent, it can be a useful precaution, if done carefully and correctly, for minimizing privacy risks where personal information is to be collected, used, or disclosed.

Finally, we note that even de-identified information that cannot be associated with an identifiable individual can be used in a discriminatory fashion against particular individuals, likely based on prohibited factors such as race, ethnicity, age, etc. The EU Article 29 Working Party has recognized this risk and has proposed expanding the definition of personal information to state "a natural person can be

---

[52] Ben Segel-Brown, "A Principled Approach to Identifiability", online: <https://www.researchgate.net/publication/305698898_Government_Data_Sharing> at 10.

[53] This applies to both the certainty of identification and certainty of information. To illustrate, in one case Target "guessed" when a female customer has become pregnant and sent her targeted marketing based on that assumption. The advertising was discovered by the women's father, and the probabilistic information revealed (that woman was likely pregnant) forced the woman to reveal her pregnancy. Kate Crawford and Jason Schultz, *Big Data and Due Process: Towards a Framework to Redress Predictive Priacy Harms* (2014) 55:93 Boston College Law Review 93, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784>.

[54] Take as an example, the Ontario's Privacy Commissioner found in Order PO-2713 that Toronto Law Student's grade distributions were personal information – despite being perfectly anonymous. This conclusion can by justified through this test on the basis that top and bottom students could be identified based on personal knowledge, re-identification was almost sure to be attempted, and revelations of student's grades could seriously impact their social standing, job prospects, and so on.

considered identifiable when, within a group of persons, he or she can be distinguished from other members of the group and consequently be treated differently" to control this possibility.[55] The OPC should consider this concept for further study and possible inclusion into PIPEDA's definitions.

Contractual backstops

Contractual controls on attempts at re-identification can similarly reduce the risk of re-identification being attempted. Such contractual controls should be implemented where personal information must be provided in the context of a transaction, such as where a third-party handles payment. Like de-identification, such contracts are not a substitute for obtaining the consumer's consent to the disclosure of the information to the third party. Each disclosure entails new risk, and the consumer may not be able to pursue remedies against the third-party receiving the information for misuse of the data.

This may pose challenges for data users who are too small or new to be entrusted with personal information. We suggest that accredited reputable data brokers bound by contractual backstops could hold data and run non-identifying analysis on behalf of such data users.

No-Go Zones

No-go zones could help to rein in the application of overreaching privacy policies by preventing uses of personal information which no individual could reasonable have intended to consent to, or for which there is no meaningful opportunity to refuse consent. Examples might include:

1. Recording sound from user's microphone or camera, except in where a user is using the microphone or camera as part of obtaining services from the site;
2. Recording a general key-log;
3. Discriminating against user's on the basis of a prohibited ground;
4. Attempting to re-identify a user in anonymized data;
5. Publication of user-submitted intimate images or videos without proof of the consent of the subject of those images or videos (Already criminalized by the *Protecting Canadians from Online Crime Act*, SC 2014, c. 31, 162.1);
6. Publishing personal information for the purpose of incentivising individuals to pay for the removal of their information.

These prohibitions are not, on their own, however, likely to be very effective. Paul Ohm notes that banning re-identification is unlikely to be effective because it happens in the shadows and is very difficult to detect.[56] The same could be said of most of these no-go zones. But where such infringements are detected, specifying these no-go zones would make it easier for victims to seek remedies. The OPC should at the least consider Guidelines clearly denouncing such practices, which may have a deterrent effect and could be cited by individuals in privacy complaints to strengthen their complaint.

---

[55] Article 29 Data Protection Working Party, Opinion 08/2012 providing further input on the data protection reform discussions, (Adopted on 05 October 2012) 01574/12/EN, WP199. Online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf

[56] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (2010) 57 UCLA Law Review 1701, online <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>.

Proceed with Caution Zones

More specific and informed consent should be required in situations where there is a greater risk of harm.

This is not necessarily captured in the distinction between implied and express consent. Implied consent may be very informed and specific. For example, when an individual sends a message via Facebook messenger, this provides very informed and specific implied consent to convey that message to the listed recipient. In contrast, clicking "I agree" to Facebook's lengthy terms and conditions provides, at best, uninformed and vague consent. This is particularly the case for applications the user would not have contemplated even if they had read those terms and conditions, such as Facebook experimenting with how it can manipulate user's emotions through the content posted in their newsfeed as part of "user experience research" authorized under their terms and conditions.[57] However, express consent will generally be required where personal information is not being collected, used, or disclosed for a purpose obviously required for the task the user is trying to perform.

It is difficult to say, for all people, what information is sensitive and creates a risk of harm for them. However, some examples gleaned from OPC findings and guidance include:

1. Seeking information about medical procedures or conditions;
2. Expressions of political and religious belief and association;
3. Expressions of the individual's sexuality;
4. Intimate messages, images, and videos;
5. Information on individuals' financial situation;
6. Recording biometric information used to authenticate a user on a device;
7. Genetic data.

All of these areas have been found in past OPC findings or guidance to be, *prima facie*, sensitive personal information requiring opt-in or explicit consent.

We contend that for at least the above categories, that businesses should know that such content requires a higher standard of consent. Indeed, given the very nature of some online business operations, such as a dating website – it is foreseeable that very specific and informed consent should be required for nearly every function on that website. This in turn can be augmented by the age or vulnerability of the likely users of the website,[58] to which we now turn.

Age restrictions

The Office of the Privacy Commissioner of Canada's *Guidelines on Privacy and Online Behavioural Advertising* states that:

---

[57] Robert Booth, *Facebook reveals news feed experiment to control emotions* (2014) in The Guardian, online: <https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds>.

[58] PIPEDA Report of Findings #2012-001, Social networking site for youth, Nexopia, breached Canadian privacy law (29 Feb 2012). Online: https://www.priv.gc.ca/cf-dc/2012/2012_001_0229_e.asp

> PIPEDA requires meaningful consent for the collection, use and disclosure of personal information. It is difficult to ensure meaningful consent from children to online behavioural advertising practices. Therefore, as a best practice, organizations should avoid tracking children and tracking on websites aimed at children.

This broad restriction needs to be implemented in a more concrete manner and rigorously enforced. It is particularly problematic that the guidelines do not define who is a child by age and do not address the particular challenges posed by social networks.

To address these deficiencies, PIAC researched the capacity of children to understand online privacy. Based on that research, we have developed guidelines specific to three age brackets: under 13, 13 to 15, and 16 to the age of majority. We have also developed specific guidelines for seeking consent to retain information upon the child reaching the age of majority, and for consent to social media.

PIAC supports specific age thresholds rather than a capacity test. At common law, legal minors are considered to be under a legal incapacity. Adults must exercise legal minors' rights on their behalf, and must do so in the minors' best interests.

While informed minors are allowed to provide medical consent, such consent is only accepted where a judge is convinced that "the young person's physical, mental, and emotional development will allow for a full appreciation of the nature and consequences of the proposed treatment."[59]

It is unlikely children will have the requisite capacity. The Eurobarometer survey suggests that even large numbers of adults struggle to understand the privacy choices they are making: 38% of adults do not read privacy policies at all, and 24% say they read them without fully understanding them.[60]

While a child's technical understanding of a privacy policy online might be tested over the internet, it would be much more difficult to conclude whether they are emotionally mature enough to make privacy decisions. If capacity tests are designed and implemented by self-interested corporations, those tests could undermine any protection of children's privacy.

While the loss of privacy can carry severe consequences, refusal to disclose personal information merely keeps minors from being able to use some online services. Given the risks and benefits involved, it is appropriate to allow businesses to rely on online tests suggesting minors' capacity in lieu of age thresholds.

PIAC recommends a prohibition on the collection, use, and disclosure of all personal information from children under age 13.[61] PIAC's research found that up to age 13, children are not able to understand

---

[59] Kenneth G. Evans, *Consent: A guide for Canadian physicians* (2006), online: <https://www.cmpa-acpm.ca/-/consent-a-guide-for-canadian-physicians> at "Age of Consent".

[60] European Commissions, *SPECIAL EUROBAROMETER 359: Attitudes on Data Protection and Electronic Identity in the European Union (Report)* (2010), online: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> at 112.

[61] John Lawford and Mani Taheri, *All in the Data Family: Children's Privacy Online* (2008), online: <https://www.piac.ca/wp-content/uploads/2014/11/children_final_small_fixed.pdf> at 5.

the privacy choices they are making. For example, while children recognized risks involved in providing information online to other individuals, they did not perceive there to be the same risk provided with posting personal information in public online spaces like Facebook. While they were aware of web tracking, they didn't understand that they were being tracked individually, thinking that only aggregate behavior was being tracked.[62] Children under age 13 rarely read privacy policies and did not really understand them if they tried.[63]

For teens aged 13-15, websites should be permitted to collect and use personal information only with:

1. the consent of the teen and
2. the explicit consent of a parent
3. for the benefit of the child and
4. solely in relation to that website or service

Businesses should not be permitted to further disclose their personal information.

Websites should be permitted to collect and use personal information with the consent of teens between 16 and the age of legal majority (18 or 19 as defined by the province). Such websites should be permitted to disclose the personal information of the teen to a third party only with the opt-in consent of the teen and explicit consent of a parent.

Once children reach the age of majority websites that have collected and used personal information (or that have been transferred the child's personal information with explicit consent during this period) should no longer be permitted to retain the information gathered during the child's "legal minority" and should be required to remove the information immediately (a privacy "get out of information jail free card") unless the newly adult person gives his or her explicit consent (within a very short time frame) to the continued collection, use, and (should they agree) possible future disclosure of their personal information gathered during their minority. This allows new adults to undo uninformed choices they may have made with regard to their personal information while children.

These requirements are designed to avoid encouraging children to enter this "data family" until they are capable of appreciating, to a reasonable degree, the information that is being collected about them and the consequences it could have for them.

More specific rules are proposed for social networking sites, given these sites' attraction to teens and the immense amount of personal information they collect. Firstly, teen users would benefit from the strictest privacy settings available on such websites or apps by default. Second, the social networking site/app would be prohibited from allowing lookup services (even to members within a site) that were able to return lists of children. Third, children would be allowed to sign up for social networks/apps with a pseudonym. It might also be appropriate to delay the collection of information about home address, gender, and sexuality until the child reaches the age of majority.

---

[62] *Ibid.*
[63] *Ibid., at* 19

Social networking services would be unavailable until age 13, as before that time, the child's personal information could not be collected, used or disclosed, even with explicit consent, to any third party (including those who also were members of a social network). For teens aged 13-15, if a social networking site wished to post limited access profiles (accessible only to those approved by the teen within the website) they would be required to seek explicit consent to this limited internal use from the teen and parent. As well, social networking sites could not seek to fund their services for the 16-17 age group from third party advertising, unless the advertising were general demographic (non-targeted) in nature, or explicit consent had been obtained from the teen and a parent or guardian. These older teens could, however, sign up to and use social networking without their parent's consent.

Legitimate business interests exception

The entire regime of PIPEDA is intended to balance the rights of privacy of individuals with legitimate business interests. As stated in s 3 of PIPEDA:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

This provision already creates the "balancing" between business use and personal information protection that the "legitimate business exemption" purports to seek.

The proposed exemption is far too broad and vague. It has the potential to overwhelm the entire rest of the Act. It is unacceptable, and would gut PIPEDA.

In the context of the EU, legitimate business interests subject to the rights of the data subject, including their right to privacy and appears to be very narrowly understood to be related to ensuring network and information security.[64] Those legitimate interests must also have been disclosed at the time the data was collected.[65]

Business may have legitimate interests such as tracking their server load and processing orders. Such interests should be dealt with on the basis of de-identification or implied consent. Is maximizing the value of ad space a legitimate interest? Is the resale of personal information to third parties to support the costs of service delivered a legitimate business interest? Before answering these questions the OPC should consult with all stakeholders and not simply accept the unproven (and circular) logic of marketers and online businesses that these services are necessary to their business models and since they are necessary they must therefore be legitimate (business) interests.

---

[64] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, (2012) 2012/0011 (COD), online: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> at 38-39, 44.

[65] *Ibid.,* at Article 14(1)(b).

Creating an exception for "legitimate business interests" would essentially dispense with the entire balancing of interests struck by PIPEDA, relying instead on businesses to exercise good judgment. We urge the Office of the Privacy Commissioner to reject this proposal. It requires no further study.

Governance

Codes of practice

Industry codes of practice are no substitute for government regulation. Businesses have a strong vested interest in ensuring that they are able to collect, use, and resell as much personal information as possible. Self-regulation entails an inherent conflict of interest – all participating businesses stand to gain from lax enforcement.

By contrast, the Privacy Commissioner's Guidelines, including the "Guidelines for Online Consent" and "Guidelines on Privacy and Online Behavioural Advertising" seem to provide useful guidance for businesses about what they need to do to comply with PIPEDA. We would support making such regulator-created guidelines binding (to the extent possible) or associating a trustmark with demonstrated compliance with those guidelines. These guidelines could also be more fully fleshed out in consultation with industry and consumer advocacy groups and any other stakeholders, should the OPC wish to enlarge its guideline making process.

Any industry commitments to higher privacy standards should be in the form of a mandatory code, enforceable by the OPC, particularly where those commitments arguably might put businesses at a competitive disadvantage. Only independent enforcement and interpretation of such codes will ensure bad actors are caught ad good actors do not bear the costs of bad actors.

Privacy Trustmarks

A privacy trustmark system could be helpful in a few ways. It could shift the burden onto companies to demonstrate that they are in compliance with PIPEDA – or some higher voluntary standard. It could also allow regulation of foreign online businesses that may not be subject to PIPEDA but who want to compete on equal footing with Canadian online businesses with regard to Canadians willingness to entrust personal information to them. Privacy trustmarks could also help distinguish businesses who have demonstrated compliance with PIPEDA from those who have not. Blackmarks could be used to warn users of disreputable sites, and sites against which privacy complaints have been upheld. This is a more public instance of the OPC's "name and shame" power, which largely has been neglected.

Privacy trustmarks would integrate well with standard privacy preferences as those preferences would allow Canadians to share more information with organizations which have demonstrated compliance and be warned of those that have not.

It is important that trustmarks be implemented by a credible organization independent of industry influence – either the Privacy Commissioner or an independent organization supervised by the Privacy Commissioner. Endorsement of independent organizations could allow the same organization accredit online business's compliance with the laws of many jurisdictions, simplifying compliance for businesses and making more trustmarked sites available for Canadian consumers.

While the government likely cannot outright prohibit industry trustmarks, it will be important to communicate to consumers that the trustmark is backed by the Privacy Commissioner, defined independent of industry influence and ensures a higher standard than industry trustmarks. Otherwise, consumers may be misled.

Ethical Assessments

Ethical assessments are no substitute for consent. Most consumers do not want to be tracked online and do not want any information disclosed to third parties. Canadian consumers also generally do not want behavioral marketing, the main application of data collected by online businesses. Substituting ethical assessments for consent would not be "overcoming the transaction costs" involved in explaining a use and seeking consent, it would be overcoming the will of consumers.

Ethical assessments might be considered by the Privacy Commissioner in deciding whether data analysis should be allowed on the basis that "it is used for statistical or scholarly study or research, purposes that cannot be achieved without disclosing the information".[66]

However, businesses have a strong vested interest in ensuring that they are able to collect, use, and resell as much personal information as possible. Consumers do not have the information or market power to choose businesses which better protect their privacy. Relying on businesses to make judgments on the benefits and risks of processing data for the organization, the individual, and society at large relies on businesses acting against their own financial best interests.

The templates for ethical assessment, such as that set out by the Future of Privacy Forum, are unrealistic in their overemphasis of the public benefits which are likely to result for using and disclosing data. Most often, a corporation will be weighing the financial gain from selling their data or from offering targeted marketing against the risk such behavior poses to their reputation. Corporations should conduct such assessments, but they are in no way a substitute for consent or regulation.

From an ethical perspective, it matters whether an individual chooses to share personal information or that information is expropriated without their knowledge or consent. Professor Zuboff argues that privacy is the right to make decisions about whether to keep something secret or to share it.[67] In other words, privacy requires that the individual make choices around their personal information. The mass collection, use, and disclosure of personal information for private profit expropriates this right to decide whether to let personal information be used for big data analysis. Accepting ethical assessments in lieu of consent would legitimize that expropriation. Furthermore, since our research shows individuals do not want to be tracked and do not want targeted advertising, it will be rare that the collection, use and disclosure of information can be justified on utilitarian grounds.

Enforcement Models

Consumers need readily available and binding remedies for breaches of their privacy rights.

---

[66] *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5, s 7(2)(c).

[67] Shoshana Zuboff, *The Secrets of Surveillance Capitalism* (2016) in Frankfurter Allgemeine Zeitung, online: <http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616-p2.html?printPagedArticle=true>.

To this end, the Privacy Commissioner should be empowered to make orders and impose fines. The Privacy Commissioner should also be empowered to award costs against a business for costs incurred by complainants in identifying and bringing forward their complaints.

As the vast bulk of all evidence of alleged privacy violations lies in the hands of the business, the evidentiary burden should be on the business to demonstrate compliance with PIPEDA where:

1. the Privacy Commissioner has received a complaint,
2. the complaint is made in good faith and it not duplicitous, frivolous or vexatious, and
3. the allegations set out in the complaint suggest a breach of PIPEDA has occurred.

Legislative changes should be implemented to clarify that the right to complain to the Commissioner and power of the Commissioner to make orders and impose fines is not barred by forum selection, mandatory arbitration, and anti-class action provisions in terms of service.

PIPEDA gives the Privacy Commissioner jurisdiction to investigate complaints relating to the transborder flow of personal information: *Lawson v. Accusearch Inc.*, 2007 FC 125, [2007] 4 FCR 314 at 51. The power to make orders and impose fines should similarly extend to any businesses collecting personal information from Canadians, or providing personal information to Canadians. Nevertheless, it may not be possible for the Commissioner to effectively investigate or enforce judgments against companies with little presence or assets in Canada. However, the OPC should have this option and weigh the effectiveness of targeted enforcement efforts on foreign-domiciled companies, especially social networks, cloud services, etc.

One way to address this problem is to develop a trustmark certified by the Privacy Commissioner, or an independent body accredited and monitored by the Privacy Commissioner. The trustmark would indicate that a business is subject to the power of the Privacy Commissioner, in addition to any other requirements. To be eligible, a foreign business would have to either show it is bound by PIPEDA or enter into a contract making it subject to PIPEDA. Conversely, a black mark could be associated with disreputable websites, especially those against which an order or fine is outstanding, even if that fine or order would be hard to enforce due to the foreign domicile of the company.

What solutions have we not identified that would be helpful in addressing consent challenges and why?

Comfort letters

The Privacy Commissioner should be empowered to issue comfort letters, at a business's expense, providing its preliminary opinion whether a proposed practice would comply with PIPEDA.

We envision this being used to determine whether consent is meaningful. The comfort letter would have to take into account the overall transaction and compare the consent to the actual proposed collection use or disclosure. The comfort letter might offer suggestions for how consent could be made meaningful. This would allow business to reduce their regulatory risk and the Privacy Commissioner to

communicate what PIPEDA requires. Comfort letters should be made public and published online for reference by other business and review by other stakeholders once the proposed consent interface is implemented.[68] Because there would be no opportunity for stakeholders such as users and advocacy groups to make submissions at the initial comfort letter request stage and it may be difficult for the Privacy Commissioner to understand how an interface would work in context, these comfort letters should not be dispositive of future complaints.

This process might go some way to allaying concerns of online business that PIPEDA was retarding innovation.

Data portability

Users of privacy invasive websites with substantial market power, like Facebook, may feel that they have little choice but to provide whatever consent the service requires. With users "locked-in" to such sites, there may be limited scope for competition on the privacy terms. Such sites have market power because users value the content generated by their friends on that site and they have invested time and energy in developing their profile on that site.

The European Union is implementing a right to data portability as part of its Data Protection Reforms. The Office of the Privacy Commissioner should explore implementation an identical right to data portability in Canada.[69]

As a partial solution, PIPEDA Principle 8 (Openness) might be applied to require such sites allow a user to export a file containing all their personal information as it is kept in the social networks' servers, leaving the problem of importing such data to be addressed by competing platforms.

Right to be Forgotten

The European Union is implementing a requirement that data controllers delete an individual's personal data if that person explicitly requests deletion and there is no other legitimate reason to retain it. A request for the deletion is a withdrawal of consent to any further collection, use or disclosure of personal information, as these are necessary implications of deleting the data. As in the medical context, a refusal or withdrawal of consent is not required to be informed. The Office of the Privacy Commissioner should explore implementation a similar right to be forgotten in Canada.[70] We are aware of criticisms of the potential right in Canada (based largely on freedom of expression) but we believe that those speaking out against it are motivated by business interests and have not fairly examined the

[68] Publishing opinions immediately would be problematic for businesses hoping to gain a competitive advantage through user interface improvements.

[69] European Commission: Justice: Data Protection, *EU Data Protection Reform : What benefits for businesses in Europe?* (2016), online: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> at 5.

[70] European Commission: Justice: Data Protection, *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century* (2012), online: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0009&from=en> at 2.

potential to enhance individual's sense of personal privacy such a right would entail. We therefore do not think that the OPC or Canadians should "forget about a right to be forgotten".[71]

The OPC can now however, without change to PIPEDA, provide more detailed guidance for data retention. Currently, the OPC's "Getting Accountability Right with a Privacy Management Program" simply provides that:

> In order to minimize unauthorized collection, use and disclosures, organizations should not retain personal information that is no longer required for the delivery of their services. Organizations must also have a policy regarding the disposal or destruction of records. Customers have the expectation that an organization will dispose of their personal information when it is no longer needed. As such, organizations should securely dispose of customers' records in accordance with its policy.[72]

Many online businesses do not have a data retention policy despite having a business model relying solely on personal information and despite the requirement in PIPEDA to have such a policy.[73] Few businesses are securely disposing of customer's records that are no longer required for the delivery of their services. Data brokers are keeping large amounts of personal information entirely unrelated to the services in relation to which the data was collected. More specific guidance on the length of time data may be retained and the method of disposal of personal information is needed as are audits of online data retention practices.

International Data Flows

The European Union requires the consent of a data protection authority for the transfer of personal information to affiliates outside the EU. This leaves a substantial loophole in that consumers, while authorizing information to be shared with corporate affiliates, are inadvertently authorizing information to be disclosed to parties who may not be subject to PIPEDA. The Office of the Privacy Commissioner should explore implementation similar restrictions on the transfer of Canadian's personal information outside Canada.[74]

---

[71] See David Fraser, McInnes Cooper LLP, "You'd better forget the right to be forgotten in Canada" (26 April 2016), online: http://blog.privacylawyer.ca/2016/04/youd-better-forget-right-to-be.html and Eloise Gratton, Borden Ladner Gervais, "Challenges with the Implementation of a Right to be Forgotten in Canada" (28 April 2016), online: http://www.eloisegratton.com/blog/2016/04/28/challenges-with-the-implementation-of-a-right-to-be-forgotten-in-canada/

[72] Office of the Privacy Commissioner of Canada, *Getting Accountability Right with a Privacy Management Program* (2012), online: <https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp>.

[73] See for example, complaint issues 20-24 of the *Nexopia* finding, *supra*.

[74] European Commission: Justice: Data Protection, *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century* (2012), online: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0009&from=en> at 5.

What roles, responsibilities and authorities should the parties responsible for promoting the development and adoption of solutions have to produce the most effective system?

The Office of the Privacy Commissioner should:

1. Strictly enforce the existing requirement of informed consent;
2. Lead the implementation of standard privacy settings to convey informed consent;
3. Lead the implementation of privacy trustmarks and black-marks;
4. Enforce the new requirements of data tagging to indicate restrictions on use and disclosure;
5. Enforce the requirement to implements safeguards, including de-identification, contractual backstops and privacy by design more broadly;
6. Enforce the principle of Individual Access to counteract the market power of social networks;
7. Establish and develop guidelines, including industry-specific guidelines;
8. Establish no-go zones and caution zones;
9. Establish and enforce specific age restrictions;
10. Investigate consumer complaints and make orders and impose fines where appropriate.

The Parliament of Canada will:

1. Empower the Privacy Commissioner to make orders and impose fines;
2. Mandate the Privacy commissioner to develop and implement a standard privacy settings system, privacy trustmarks and privacy blackmarks;
3. Require that data be tagged to indicate restrictions on its use and disclosure;
4. Increase the funding for the Privacy Commissioner in line with its expanded role.

Online businesses will:

1. Seek to minimize the collection use and disclosure of personal data through privacy by design, de-identification and contractual backstops;
2. Demonstrate the compliance required to receive the trustmark established by the Privacy Commissioner;
3. Design online systems which respect individual's standard privacy preferences where possible and to seek informed consent;
4. Cease relying on tacit, implicit, drive-by, browser-wrap and click-wrap assent to privacy policies as a foundation for consent.

Consumers and consumer advocacy organizations will:

1. Support the implementation of standard privacy settings and trustmarks;
2. Provide input on the development of guidelines;
3. Monitor corporations' compliance with PIPEDA and bring forward complaints where required.

What, if any, legislative changes are required?

In our view, most organizations are not complying with their existing obligations under PIPEDA as they are failing to obtain informed consent for collection, use, and disclosure as required by Principle 4.3 and s. 6.1 of PIPEDA. Consequently, strengthening the Privacy commissioner's enforcement powers is essential.

Powers of the Privacy Commissioner

As mentioned above, the Privacy Commissioner should be empowered to make orders and impose fines. Those fines must be sufficient to ensure compliance with PIPEDA, rather than nominal amounts which can be written off as a cost of doing business. The Privacy Commissioner should also be empowered to award costs against a business for costs incurred by complainants in identifying and bringing forward their complaints.

Evidentiary burden

The burden should be on a business to demonstrate compliance with PIPEDA where:

1. the Privacy Commissioner has received a complaint;
2. The complaint is made in good faith and it not duplicitous, frivolous or vexatious;
3. The allegations set out in the complaint suggest a breach of PIPEDA has occurred.

This would also help address the problem of investigating complaints against non-responsive foreign businesses, as the Privacy Commissioner struggled with in *Lawson* v. *Accusearch Inc.*, [2007] 4 FCR 314, 2007 FC 125.

Establishing the Trustmark

The Privacy Commissioner should be given statutory authority and mandate to establish a trustmark, accredit third-party trustmarks and to publicize a trustmark. The same powers should be given in relation to the establishment of a black-mark.

Comfort letters

The Privacy Commissioner should be permitted to issue comfort letters, at a company's expense, providing a preliminary opinion on whether a proposed practice would comply with PIPEDA, provided those letters are made public online and are not dispositive of any related complaints.

Data tagging

Data should be required to be tagged to identify restrictions on its use. Businesses must tag information already collected in accordance with the principle of meaningful consent, which may require seeking new consent from users. A date should be set by which all untagged information must be destroyed.

Establishing Standard Privacy Preferences

The Privacy Commissioner should be given statutory authority to establish a standard privacy preference system.