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*

*Prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada*

# Table of Contents






30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

# Introduction

Consent is considered to be the cornerstone of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[1] Organizations are required to obtain individuals' consent to lawfully collect, use and disclose personal information in the course of commercial activity. Without consent, the circumstances under which organizations are allowed to process personal information are limited. PIPEDA is based on a technologically neutral framework of ten principles, including consent, that were conceived to be flexible enough to work in a variety of environments. However, there is concern that technology and business models have changed so significantly since PIPEDA was drafted as to affect personal information protections and to call into question the feasibility of obtaining meaningful consent.

Indeed, during the Office of the Privacy Commissioner's (OPC's) Privacy Priority Setting discussions in 2015, some stakeholders questioned the continued viability of the consent model in an ecosystem of vast, complex information flows and ubiquitous computing. PIPEDA predates technologies such as smart phones and cloud computing, as well as business models predicated on unlimited access to personal information and automated processes. Stakeholders echoed a larger global debate about the role of consent in privacy protection regimes that has gained momentum as advances in big data analytics and the increasing prominence of data collection through the Internet of Things start to pervade our everyday activities.

Some have argued for relaxing requirements for consent around the collection of personal information, and instead advocate focusing on accountability and ethical use of personal information and/or on a risk-based approach. [2] In their opinion, "(u)nderstanding how our personal information is being used in this environment is becoming increasingly difficult if not impossible for the average person. Thus, expecting individuals to take an active role in deciding how their personal information is used in all instances is increasingly unrealistic."[3]

Others hold an opposing view. They believe that measures should be introduced to strengthen consent, including increased transparency and mechanisms that enhance individual control. In their words, "removing consent from the equation risks undermining fundamental individual rights, protections and freedoms." [4]

The OPC has decided to take a closer look at the consent model as part of our strategic priority work on the Economics of Privacy. We have committed to identifying and exploring potential enhancements to the consent model in response to concerns raised both by individuals and organizations. This discussion paper aims to provide an overview of the landscape, key issues and potential solutions to stimulate dialogue and solicit suggestions for improvements or alternatives to the consent model as currently formulated.

Readers of this paper are encouraged to keep in mind the roles of the various players involved—individuals, organizations, regulators and legislators—as they reflect on the relative merits of the various potential solutions we've outlined. In assessing which solution, or combination of solutions, may be best suited to address the consent dilemma, it is important to bear in mind who is best placed to use the proposed tools and who they serve. Ultimately, the goal is to help strengthen the privacy protection of individuals.

# Why consent?

In PIPEDA, consent functions as a way for individuals to protect their privacy by exercising control over their personal information – what personal information organizations can collect, how they can use it, and to whom they can disclose it. Professor Alan Westin, in his seminal 1967 book *Privacy and Freedom*, described privacy as being rooted in personal autonomy, which in turn underpins our democratic system. Westin states, "In democratic societies, there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth…and in the need to maintain social processes that safeguard his sacred individuality."[5]

Professor Westin defined privacy as the desire of individuals to choose freely how much of themselves to expose to others. The notion of privacy as individual control over personal information was echoed in the 1972 report of the Departments of Communications and Justice Task Force on Privacy and Computers, which lay the foundation for Canada's privacy legislation. In relation to privacy in the information context, the report states, "all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit…He may decide to make it available to others in order to obtain certain benefits…Nevertheless he has a basic and controlling interest in what happens to this information and in controlling access to it."[6] This principle was reaffirmed some 20 years later when Justice Gérard La Forest of the Supreme Court of Canada quoted Professor Westin, stating, "Privacy is at the heart of liberty in a modern state…Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual." [7]

Respect for individual autonomy was the backdrop in the drafting of PIPEDA. Not only is individual autonomy a foundation for the consent principle, but it figures in other aspects of the law as well. For example, the drafters decided to avoid differentiating between "sensitive" and other kinds of data. According to those involved, "It is extremely difficult to determine *a priori* what is sensitive information, for people tend to have different views on what they consider most sensitive, and the matter can vary from one context to another. It was thought safest to let individuals decide what is sensitive and in which circumstances by giving them control of the information based on the right of consent."[8]

While privacy or the protection of personal information are not specifically mentioned the *Canadian Charter of Rights and Freedoms*, the Charter nonetheless affords privacy protection under Section 7 (the right to life, liberty and the security of the person), and Section 8 (the right to be secure against unreasonable search or seizure). In *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers , Local 401*,[9] the Supreme Court of Canada stated that data protection legislation has a quasi-constitutional status given the important interests it protects.

# Consent under PIPEDA

The purpose of PIPEDA is to establish rules that 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 the purposes that a reasonable person would consider appropriate in the circumstances.[10]

PIPEDA relies on knowledge and consent as a requirement for the collection, use and disclosure of personal information. Organizations are required to inform individuals about what personal information they will collect, how they plan to use or disclose that information, and for what purposes, to enable individuals to decide whether or not to provide consent. This aims to provide individuals with control over how their information will be collected, used and disclosed.


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

In order for consent to be considered meaningful under PIPEDA, individuals should have a clear understanding of what will be collected, how their personal information will be used, and with whom it will be shared. Consent 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.[11]

Recognizing organizations' need to collect, use and disclose personal information for reasonable purposes, PIPEDA also contains a number of exceptions to the requirement for knowledge and consent, based on the reality that obtaining individuals' consent may not be appropriate in every circumstance. For example, information may be used or disclosed without consent in an emergency that threatens the life, health or security of an individual. Some other exceptions include investigating a breach of an agreement or contravention of a law where seeking consent might compromise an ongoing investigation. Such exceptions recognize that individual consent, and the autonomy it protects, do not override all other interests, but rather that there needs to be a balance between privacy and competing values which individual consent might undermine.[12] In this sense, as is discussed below, PIPEDA already recognizes, and accommodates, both limitations inherent in the consent principle. Certain statutory obligations apply even if consent is not required. For example, subsection 5(3) of PIPEDA limits the purposes for which an organization may collect, use or disclose personal information to those that "a reasonable person would consider are appropriate in the circumstances." This helps ensure that individuals remain protected from inappropriate collection, use and disclosure of their personal information even if an individual consents or where consent is not required.[13] All other PIPEDA principles, such as safeguards and accountability, also continue to apply even where consent is not required.

PIPEDA requires that the purposes for which an individual's information is to be collected, used or disclosed be explained in a clear and transparent manner. Consent must be obtained before or at the time of collection, or when a new use of personal information has been identified. Organizations may not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information *beyond* that required to fulfill an explicitly specified and legitimate purpose. At the same time, individuals should be informed of the consequences of withdrawing consent, particularly if they are withdrawing consent to a collection, use or disclosure of their personal information that is essential to the service they are signing up for.

PIPEDA recognizes that the form of consent can vary, taking into account the sensitivity of the information and the reasonable expectations of the individual. Express consent is the most appropriate and respectful form of consent to use generally, and is required when sensitive[14] information is at issue. Implied consent can be acceptable in strictly defined circumstances.[15]

# The role of consent in other jurisdictions

## 1) European Union

In the European Union, the right to data protection and the right to privacy are two distinct human rights recognized in the *Charter of Fundamental Rights of the European Union*, the *Treaty on the Functioning of the EU*, and in two legal instruments of the Council of Europe, to which all the EU Member States are parties.

The EU Data Protection Directive 95/46 (EU Directive) governs the processing of personal data in both the public and private sectors. It was designed to achieve two basic objectives: to protect the fundamental right of data subjects to control their personal data; and to ensure the free flow of personal data in the internal market.

Article 6 of the EU Directive provides that personal information may only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." It should be "adequate, relevant and not excessive" in relation to the purposes for which data is collected and/or further processed and "accurate as well as, where necessary, kept up to date". This is comparable in many respects to subsection 5(3) of PIPEDA.

Within the boundaries of Article 6, consent of the data subject is one of the six legal grounds on which personal data can be processed. The other grounds are: enabling the performance of a contract, enabling the controller to comply with a legal obligation, protecting the vital interests of the data subject, performing a task for the public interest or in the exercise of an official authority vested in the controller, and to support the controllers' legitimate interests provided they are not overridden by the fundamental rights and freedoms of the data subject. Consent is not singled out as the preferred ground for data processing. Rather, it is placed on an equal footing with the other legal grounds. EU member states, which also have their own country-specific privacy legislation, recognize consent as a legal ground for processing but lend varying weight to its importance.[16]

When consent is being relied on for the lawful processing of data, consent must be a "freely given, specific and informed indication"[17] of an individual's wishes. Moreover, consent should be unambiguous and explicit in certain circumstances. For example, explicit consent is required for the processing of special categories of data, such as ethnic origin, genetic data, and political affiliation. Individuals also have the right to withdraw consent to the processing of their data.

The new General Data Protection Regulation (GDPR), which is expected to come into effect in 2018, and replaces the EU Directive, will require that consent be freely given, specific, informed and unambiguous. Businesses will need not rely on consent if they can prove that the data processing is "necessary for the purposes of the legitimate interests pursued by [a private party], except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."[18] The GDPR will also introduce restrictions on the ability of children to consent to data processing without parental authorization.

While the EU Directive allows implied consent in some circumstances, the GDPR will require that consent be expressed through a statement or another clear affirmative action, such as ticking a box on a website or choosing a technical setting. The GDPR explicitly states that silence or inactivity should not constitute consent. Individuals have the right to withdraw consent at any time. Once consent is withdrawn, data subjects will have the right to have their personal data erased and no longer used for processing.


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

## 2) United States

In the U.S., privacy is protected by a patchwork of laws at the state and federal levels. Many are sector-specific and reflect the U.S. harm-based approach to privacy regulation. The Fair Information Practice Principles (FIPPs) serve as the basis for privacy protections, with "notice and choice" as one of the elements. The Federal Trade Commission (FTC) has been active in promoting consumer privacy using its powers to address "unfair and deceptive practices" under the *Federal Trade Commission Act*.[19] "Notice and choice" in the context of privacy policies and terms of service can be a factor in the FTC's findings under the FTC Act in that companies have an obligation to inform individuals of their privacy practices and give them a choice whether to consent to those practices.

The FTC also regulates children's privacy under the *Children's Online Privacy Protection Act* (COPPA).[20] COPPA requires that verifiable parental consent be obtained by operators of websites, online services and mobile applications that collect the personal information of children under 13. Notwithstanding COPPA, consent is not universally required before collecting or using personal information of individuals in the U.S. However, sectoral laws and enforceable codes of conduct often contain a user choice requirement either on an opt-in or opt-out basis.[21] Sensitive information, such as medical or financial data, generally requires users to opt-in.

In 2012, the FTC published a report calling for "broad, baseline privacy legislation that would establish privacy as a basic right." [22] The same year, the White House issued the so-called "Privacy Blueprint" report to address what it described as a lack of a "sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models." [23] The Privacy Blueprint proposes a Consumer Privacy Bill of Rights based on overarching principles that include individual control, transparency and respect for context.

"Respect for context" is a key principle of the proposed Consumer Privacy Bill of Rights under which "consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." [24] According to the Privacy Blueprint, this principle is derived from the broadly recognized FIPPs of "purpose specification" and "use limitation", and includes the following elements:

- Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise; and
- If companies will use or disclose personal data for other purposes, they should provide heightened transparency and individual choice by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection.

In February 2015, President Obama released the draft of a proposed *Consumer Privacy Bill of Rights Act*.[25] Under the bill, organizations are required to provide individuals with reasonable means to control the processing of their personal information that is proportionate to the privacy risks. Individuals have the right to withdraw their consent subject to specific exceptions, such as fraud prevention. If an organization processes personal data in a manner that is not reasonable in light of context, it must conduct a privacy risk analysis and take reasonable steps to mitigate any privacy risks identified as a result. Such steps must include providing "heightened transparency and individual control" over processing. At the time of writing, no further developments have occurred with regard to the bill, which has been criticized by some privacy advocates[26] as having weak enforcement provisions.

# Challenges to meaningful consent

## 1) New technologies and business models

The consent model of personal information protection was conceived at a time when transactions had clearly defined moments at which information was exchanged. Whether an individual was interacting with a bank or making an insurance claim, transactions were often binary and for a discrete, or limited, purpose. They were often routine, predictable and transparent. Individuals generally knew the identity of the organizations they were dealing with, the information being collected, and how the information would be used. Today, with cloud computing, big data and the Internet of Things (IoT), the environment is radically different. Further, traditional point-to-point transfers of data are being replaced with data flows through distributed systems, making it difficult for individuals to know which organizations are processing their data and for what purposes.

Though special care was taken to make the principles behind Canada's private sector privacy laws technology neutral, the complexity of today's information ecosystem is nonetheless posing challenges to obtaining and providing meaningful consent. As we saw in the OPC's research on predictive analytics[27] and IoT,[28] new technologies and business models have resulted in a fast-paced, dynamic environment where unprecedented amounts of personal information are collected by, and shared among, a myriad of often invisible players who use it for a host of purposes, both existing and not yet conceived of. Binary one-time consent is being increasingly challenged because it reflects a decision at a moment in time, under specific circumstances, and is tied to the original context for the decision, whereas that is not how many business models and technologies work anymore.

### a) Big data

Significant technological advances in the ability of organizations to collect, store and analyze unprecedented amounts of information have led to "big data." Big data can be described as data sets so large, lacking in structure, and changeable from one moment to another that traditional methods of data analysis no longer apply. Complex algorithms are used to find correlations in these data sets in order to solve problems and generate value and benefits for organizations, individuals and society. Many of the algorithms are opaque to individuals and regulators as organizations consider them proprietary.[29]

Big data analytics has led to many advances in all areas of the economy, including scientific research, resource management and manufacturing, and its benefits for society are substantial. Without big data analytics, tailored treatment of diseases, optimization of traffic flows, and personalized education may not be possible. Nonetheless, big data analysis does not always lead to positive outcomes. The potential exists for information to be used in ethically questionable ways, for example, discriminatory pricing based on attributes assigned to consumers [30] or advertisements based on racial profiling.[31] The FTC's report summarizing its public workshop *Big Data: A Tool for Inclusion or Exclusion*, elaborates on the concerns expressed by participants that while big data analytics can lead to numerous improvements for society, "potential inaccuracies and biases might lead to detrimental effects for low-income and underserved populations."[32]


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

Big data analytics is attractive to business because value is created from information that on its own might be worth much less. With storage costs of data decreasing and big data algorithms becoming more powerful, organizations do not have a strong incentive to dispose of information. Instead, many retain it in case it might prove useful in the future. Indeed, advances in technology are opening up new data uses that defy our imagination and it is becoming increasingly difficult to anticipate uses that will be made of the data down the road. This poses the risk that personal data will be used in new ways to which the individuals did not consent nor would ever have reasonably expected to consent at the time their information was collected.

There is also the issue of being able to distinguish between non-personal and personal information, as non-personal data does not typically fall under privacy regulation and thus does not require consent. The purpose of big data algorithms is to draw correlations between individual pieces of data. While each disparate piece of data on its own may be non-personal, by amassing, combining and analyzing the pieces, the processing of non-personal information may result in information about an identifiable individual. Big data analytics has the ability to reconstitute identities that have been stripped away.[33] It is difficult if not impossible to know in advance when an algorithm will re-identify an individual or what pieces of data will allow it to do so.[34] In the past, the question of whether information is about an identifiable individual, and thus is personal information has traditionally been as a yes or no question. However, some have more recently suggested a more nuanced and risk-based approach. [35] The question arises at which tipping point data becomes personal, requiring an organization to seek individuals' consent, or whether there should be a tipping point at all.

Big data analytics is also able to draw new and possibly *sensitive* inferences about individuals from discrete pieces of information that alone may be non-personal or may, if personal information, nonetheless be non-sensitive. Under PIPEDA, uses of sensitive data require express consent which, in a big data environment, may not have been obtained at the time of collection. Some believe[36] that the requirement to go back to individuals for their amended consent may discourage organizations from pursuing new uses of information because of the costs of obtaining new consent, thus undermining the drive for innovation. Yet, PIPEDA specifically requires new consent.

At their 2014 annual conference, the International Data Protection and Privacy Commissioners passed a resolution on big data[37] that reaffirms fair information principles, including consent. The Commissioners acknowledge the societal benefits of big data in areas such as medicine and environmental protection while noting that "(b)ig (d)ata can be perceived to challenge key privacy principles, in particular the principles of purpose limitation and data minimisation."[38] At the same time, however, the Commissioners underscore the importance of maintaining privacy protections as safeguards against the harms of extensive profiling, such as discriminatory outcomes and infringements on the right to equal treatment. They encourage organizations involved in big data analysis to, among other things, be transparent about their practices, obtain individuals' consent, and safeguard privacy through Privacy by Design and anonymization where appropriate.

In the OPC's research paper on predictive analytics, the point is made that "big data and intelligent predictive analytics could, on the one hand, help advance research, innovation, and new approaches to understanding the world and make important and socially valuable decisions in fields such as public health, economic development and economic forecasting. On the other, advanced analytics prompt increased data collection, sharing and linkages, as well as having the potential to be incredibly invasive and intrusive, discriminatory, and yet another underpinning of a surveillance society."[39]

## b) Internet of Things (IoT)

The growing dominance of IoT infrastructure is presenting unique challenges to consent-based privacy protection frameworks. IoT is a term used to describe an environment of physical objects that collect data using sensors and share it over telecommunications networks. While this technology has existed for decades, it was generally in use away from the public consciousness, for example, in manufacturing to monitor the condition of equipment and to track parts. More recently, IoT devices have become part of everyday life and consumer products, giving rise to a number of privacy implications and drawing the interest of privacy regulators. For example, the European Commission's Article 29 Data Protection Working Party adopted an opinion on IoT[40] where they concluded that data collected by IoT devices is so high in quantity, quality and sensitivity, that such data should be regarded and treated as personal data.

As discussed in the OPC's IoT research paper,[41] collection of IoT information is motivated by a desire to understand individuals' activities, movements and preferences, and inferences can be drawn about individuals. The OPC has demonstrated elsewhere that powerful insights about an individual can be gleaned from information such as IP addresses,[42] metadata[43] and web tracking data.[44]

The IoT provides individual and societal benefits through increased automation and monitoring of all aspects of the environment, potentially leading to better management of resources, increased efficiencies and added convenience. IoT applications include connected cars, health and fitness trackers, and smart home devices. IoT can be used to lower home energy costs by running appliances when electricity is cheaper or managing traffic flow by monitoring the number of vehicles through road-embedded sensors. To organisations, value lies not in the revenue from selling devices but in the data that is generated and processed through big data algorithms. Information collected by sensors within objects that are connected to each other in the IoT environment can yield a tremendous amount of data that can be combined, analyzed and acted upon. Much of this data may be sensitive, or be rendered sensitive by combining data from different sources. For example, combining data generated by an individual carrying a smart phone, wearing a fitness tracker, and living in a home with a smart meter can yield a profile that can include physical location, associates, likes and interests, heart rate, and likely activity at any given time.

Data collection in the IoT environment is often invisible to individuals. There is no interface between consumers and organizations where data would be exchanged in a visible and transparent way. Instead, data collection and sharing occurs device to device, without human involvement, as a result of routine activities.

A major challenge in this environment is how to convey meaningful information about privacy risks in order to inform the user's decision whether or not to provide consent. In the Mauritius Declaration on the Internet of Things,[45] International Data Protection and Privacy Commissioners highlighted transparency as a key concern, stating that consent obtained on the basis of existing privacy policies, which are often lengthy and complex, is not likely to be informed. Research[46] funded by the OPC on the connected car found privacy information provided to consumers to be so woefully inadequate as to make meaningful consent impossible. Wearable computing, which the OPC examined in a research paper,[47] also compounds the challenge of reaching users with relevant information at the right time and in a form and format that they can access and understand.

In its staff report[48] on the IoT, the FTC identified ubiquitous data collection and the potential for unexpected uses of data as two of the most serious privacy risks of the IoT. The FTC focused on the importance of notifying individuals of companies' data management practices, recommending that organizations notify consumers about how their information will be used, particularly when the data is sensitive or data use is beyond consumers' reasonable expectations.


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

## 2) Human behaviour

PIPEDA's requirement for knowledge and consent places responsibility on individuals to inform themselves of an organization's privacy management practices and to understand the nature, purpose and consequences of consenting to have their information collected, used and disclosed by the organization. Though this may, on the surface, seem like a straightforward proposition, in practice it can be fraught with risks and challenges. This is not just due to the complexities of the digital ecosystem but also paradoxes of human behaviour and the practical realities of having limited time and energy to fully engage with privacy policies.

Even before information technologies and business models evolved to their current state, the consent model was criticised as being overly theoretical. In their 2009 article "Soft Surveillance, Hard Consent," Professor Ian Kerr and his colleagues argued that "(i)f privacy legislation is to provide people with meaningful control over their personal information, it must employ a model of consent that accurately reflects people's behaviour."[49]

There is evidence that human behaviour undermines the efficacy of the consent model. Many studies have found that people who say they care about privacy at the same time may disclose vast amounts of personal information online. For example, a 2015 TRUSTe study[50] found that while 54 percent of parents say they are concerned about their children's privacy, 66 percent post their children's pictures online. In a 2015 AIMIA Institute survey,[51] 70 percent of respondents who take defensive action to protect their data also have a positive attitude toward sharing their data.

Behavioural psychologists have brought insight to this seemingly contradictory behaviour by identifying a number of factors that affect individuals' ability to make privacy decisions. Professor Alessandro Acquisti and his colleagues suggest[52] that people's privacy behaviour is influenced by three main factors:

- Uncertainty about the nature of privacy trade-offs – People do not have a clear and complete understanding of what happens to their information once organizations collect it. As a result, they are uncertain about how much information to share;
- Context dependence – People's sensitivity to privacy varies depending on the situation and is influenced by factors such as physical environment of the individual, website design, and degree of disclosure of others on the website; and
- The malleability of privacy preferences – People are easily influenced as to the type and amount of information they disclose. For example, default privacy settings are often interpreted as recommendations thus different default settings will lead to different privacy behaviours.

Researchers[53] have found that it is very difficult to quantify privacy risks when compared to the concrete rewards of disclosing one's information online. Individuals may not realize the implications of what they are disclosing, particularly over time as small disclosures lead to a bigger picture when information is combined. Individuals are also easily distracted by the illusion of privacy. Research[54] shows that simply posting a privacy policy increases users' comfort level that the site is protecting their personal information.

People's general attitude about the world around them also plays a role in privacy disclosures. A survey [55] conducted by the Annenberg School for Communication in the University of Pennsylvania explored the idea that people give out information about themselves online as a trade-off for benefits they receive. The researchers found "that more than half do not want to lose control over their information but also believe this loss of control has already happened" and so, by virtue of their resignation to their belief that there is no other way, will make trade-offs.

In light of these technological and human challenges to the consent model, the next section outlines possible solutions.

## Possible Solutions

We have seen how the digital information ecosystem poses consent challenges for both individuals and organizations. We have also seen how individuals face cognitive biases and practical constraints when making privacy decisions, and are tasked with the responsibility of understanding a very complex environment. Left entirely to their own devices, individuals can hardly be expected to demystify complex business relationships and complicated algorithms to make informed choices about when to provide consent to the collection, use and disclosure of their personal information. The burden of understanding and consenting to complicated practices should not rest solely on individuals without having the appropriate support mechanisms in place to facilitate the consent process.

Organizations, however, are confronting the practical difficulties of trying to explain their personal information management practices, particularly in the mobile environment and in light of the highly competitive and quickly evolving nature of online services. In order to be competitive in the global economy, organizations are under pressure to innovate quickly and would benefit from mechanisms that help them meet the consent requirement more efficiently.

Consent should not be a burden for either individuals or organizations, nor should it pose a barrier to innovation and to the benefits of technological developments to individuals, organizations and society. But how do we best preserve this important control given the current landscape and achieve a balance between the individual's right to privacy and the organization's need to manage personal information for reasonable business purposes, furthering the very purpose and objectives of PIPEDA? What tools would be effective and who is best placed to implement them? This paper is the OPC's first step towards helping identify mechanisms that could help make consent more meaningful while enabling innovation in a digital economy, with roles and responsibilities of the key players being an essential consideration.

A range of solutions have been proposed by various stakeholders to solve some of the privacy challenges of new technologies and business models, including:

- Enhancing informed consent through more understandable and useful ways of explaining information management practices to individuals as well as more user-friendly ways of expressing privacy preferences;
- Alternative solutions that might introduce certain limited permissible uses without consent or introduce certain "no-go zones" of prohibited uses;
- Stronger accountability mechanisms for organizations to demonstrate compliance with their current legal obligations, including third party assurances of undertakings on which users rely in giving consent;
- New accountability mechanisms that introduce broader notions of fairness and ethics in the assessment of purported uses that will be made of individuals' personal information as a supplement to, or in some circumstances, a substitute for, informed consent as traditionally understood; and


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

- Strengthening regulatory oversight to ensure that proposed solutions are effective in protecting privacy.

Some of these solutions re-emphasize the importance of the existing FIPPs. They challenge organizations, researchers and technologists to be more creative in how they present information to individuals and use technology to build in privacy protections with a view to making consent more meaningful for individuals. Others propose alternatives to consent for circumstances where consent might not be practicable. The governance solutions place the onus on organizations to evaluate and mitigate risk and to make judgements around the reasonableness of various uses of personal information.

There are advantages and disadvantages to each of these solutions. If consent can be a great tool to address the power imbalance between organizations and individuals in the information economy, do some of these solutions give enough, or too much, control to individuals? Do some place too much power into the hands of organizations which have a vested interest in the commercial value of personal information? If so, how can risk be mitigated?

Underlying the discussion about solutions is the key question of how responsibility for privacy protection should be apportioned to organisations, individuals, regulators and legislators. Ideally, organizations should implement practical solutions that provide meaningful choice to individuals, who in turn would engage in thoughtfully exercising their privacy preferences. But where consent is not practicable or meaningful, what reasonable substitutes should be permitted? What mechanisms could help regulators maintain the right balance between individual privacy interests and the needs of organizations to use personal information and ensure that a baseline of privacy protections is being respected?

Below, we present an array of options that, while not a complete inventory, at minimum describes the types of approaches being contemplated. It is doubtful that any one solution could serve as the proverbial "silver bullet." However, the right combination of solutions might help individuals achieve greater control over their personal information in the digital realm. Questions at the end of each section, as well as at the end of this discussion paper, are intended to stimulate dialogue on preferred solutions to the issues we have identified as challenging consent.

# 1) Enhancing consent

The current consent-based model of privacy protection can no doubt be strengthened through the implementation of mechanisms aimed at improving individuals' practical ability to exercise meaningful consent. Greater transparency in privacy policies and notices, simpler ways for individuals to manage their privacy preferences, and enhancing technical and governance approaches all have the potential to support the consent model in continuing to function as intended. Some of these mechanisms for enhancing consent are outlined below.

## a) Greater transparency in privacy policies and notices

In the digital environment, flows of personal information have multiplied and diversified between individuals and organizations. However, the vehicle for conveying information about privacy practices, i.e. the privacy policy, has not evolved at the same pace as the ecosystem.

When organizations use a single document to describe complex privacy practices to reduce their exposure to legal liability and to comply with privacy laws in multiple jurisdictions, it is not surprising that the result may not be particularly useful. Privacy policies have been the subject of much criticism for their opaque and

legalistic language, and the effort required to read them. Widely cited research[56] from 2008 found that Internet users would need 244 hours per year to read, much less understand, the privacy policies of the sites they visited. Presumably today that number would be even higher.

Professor Helen Nissenbaum suggests[57] that the main limitation of privacy policies is the "transparency paradox." If privacy policies try to comprehensively describe organizations' practices, this will result in a long complex document that the average user will not read or understand. If a privacy policy is short and simple, it cannot cover the complexity of information flows in sufficient detail to allow for informed consent.

Various practical solutions have been proposed to lessen the burden on individuals to inform themselves of complex information management practices. Privacy regulators, including the OPC,[58] advocate that in addition to clear and comprehensive privacy policies, organizations should endeavour to convey privacy information at key points in the user experience to help users overcome the challenges of trying to understand complex information flows.

Layered privacy policies have been popular in recent years, in an attempt to make privacy policies both comprehensive and readable. Creative options also warrant exploring to make consent more appropriate to changing circumstances and preferences and to minimize decision overload. For example, organizations could be enhancing their privacy policies with dynamic, interactive data maps and infographics, or short videos. Icons can also be useful in supplementing privacy policies to allow individuals to know at a glance how their information is being used. "Privacy Icons"[59] are an example of a symbols-based approach to presenting attributes of privacy policies including data retention, third party use of data, and whether law enforcement can access data.

Keeping consumers informed is not only a regulatory requirement but also contributes to the overall success of the organization. A 2015 Consumers Council of Canada report[60] warns that complex terms and conditions statements, including privacy policies, may undermine trust between consumers and businesses. The report recommends best practices for organizations, including posting a summary of salient points of a privacy policy, highlighting changes from the previous versions, and providing definitions of key concepts.

## b) Managing privacy preferences across services

The White House Report entitled *Big Data and Privacy: A Technological Perspective*[61] suggests that responsibility for using personal data in accordance with the user's preferences should rest with the organization, possibly assisted by a mutually accepted intermediary. Individuals would associate themselves with a standard set of privacy preference profiles offered by third parties. The third party websites would then vet apps and services based on the user's privacy profile.

A similar suggestion appears in the 2013 World Economic Forum (WEF) report *Unlocking the Value of Personal Data: From Collection to Usage*.[62] The WEF proposes tagging all collected data with metadata that includes the individual's preferences for how the data could be used. An audit function would be built in to verify whether actual usage is consistent with the hard coded preferences. There has been some technical work to implement this idea of tagging data with preferences or rules (sometimes referred to as creating "smart data"). The "eXtensible Access Control Markup Language" (XACML) is a standard for creating conditions and obligations for controlling data access. XACML has been extended to create schemes for "sticky" privacy policies where personal data is stored in packages or envelopes that control how it is released and used.[63]


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

Both these approaches could simplify the consent process as they obviate the need for individuals to fully understand all of an organization's privacy practices and decide whether or not to provide consent every single time they want to use a new digital service. They would also help account for consent when big data analysis leads to new uses of data after consent to collecting the data had already been obtained.

## c) Technology–specific safeguards

Closely related to transparent explanations and mechanisms for more easily managing privacy preferences are proposals around ways to address the requirement for meaningful consent when personal information is processed by specific technologies. For example, the unique characteristics of the IoT environment make it a perfect candidate for this type of approach.

In Europe, the Article 29 Working Party advocates[64] building compliance mechanisms into IoT devices and services to get around the "poor fit" of traditional consent mechanisms. The WP29 states that IoT devices and services need to include functionality that enables users to withdraw consent at any time, including withdrawing consent without being penalized economically or in terms of being able to access the device's capabilities.

In its staff report[65] on the IoT, the FTC lists a number of promising solutions being implemented to improve the effectiveness of privacy messaging in the IoT environment. These include:

- Codes on the device, such as QR codes, that lead consumers to more in-depth information;
- Privacy choices during set-up of the device, taking advantage of set-up wizards to explain and select privacy settings;
- Management portals or dashboards that include privacy settings consumers can set up and revisit; and
- Out-of-band communications that allow individuals to receive privacy information through another device, such as e-mail.

The Online Trust Alliance[66] (OTA) developed the Internet of Things Trust Framework[67] aimed at manufacturers, developers and retailers of connected home devices and health and fitness wearables. The framework consists of best practices such as:

- Disclosing prior to purchase a device's data collection policies, as well as the impact on the device's key features if consumers choose not to share their data; and
- Disclosing if the user has the ability to remove or make anonymous all personal data upon discontinuing the device or device end-of-life.

## d) Privacy as a default setting (Privacy by Design)

Privacy by Design[68] (PbD) aims to ensure that privacy is considered throughout the development and implementation of initiatives that involve the handling of personal information. It imposes obligations on companies to account for privacy when creating their products and systems to ensure that privacy protections, including meaningful consent, are "baked in." In other words, privacy is embedded as the default, making it an inherent component of the program or system.

The concept underlying PbD is holistic in that it incorporates technical measures as well as principles of governance. Privacy should be integral not only to technology but also to organizational priorities, project objectives, and overall planning of operations. This proactive approach to privacy protection fosters trust on

the part of individuals that their data will not be used in unanticipated ways and without their consent. It also enables organizations to enhance their accountability and take ownership of their privacy obligations.

PbD is recognized internationally. In 2010, the International Conference of Data Protection and Privacy Commissioners adopted a resolution on PbD[69] acknowledging PbD as an essential component of privacy protection. They also called on data protection and privacy regulators to promote the adoption of PbD principles in the formulation of privacy policy and legislation. The Commissioners endorsed PbD principles in a number of subsequent resolutions, including the 2014 resolution on big data.[70]

In the US, the FTC 2012 report *Protecting Consumer Privacy in an Era of Rapid Change*[71] proposed a framework for organizations and policy makers with PbD as a core value. In 2015, the European Union Agency for Network and Information Security (ENISA) published[72] an inventory of existing PbD approaches, strategies and technical mechanisms in order to promote ways of operationalizing the principles contained in privacy legislation.

Also in the EU, the new General Data Protection Regulation (GDPR) requires that organizations incorporate PbD principles into the development of business processes for products and services. In the European model, governance is layered on to the technical framework of PbD. For example, the obligation to obtain explicit consent and to be able to demonstrate that consent has been given puts the onus on organizations to design and implement a consent mechanism that meets those criteria.

### Questions for Reflection

1) What measures have the potential to enhance consent and how should their development/adoption be promoted?

2) What incentives should exist for organizations to implement greater transparency and privacy preference mechanisms to enhance individuals' ability to provide consent?

3) How should PbD be treated in the context of Canada's privacy law framework? Should this concept merely be encouraged as a desirable aspect of an accountability regime? Or should it become a legislated requirement as it will soon be in Europe?

## 2) Alternatives to consent

In seeking to find solutions to the challenges of the consent model in the digital realm, it may be that consent is simply not practicable in certain circumstances. In this section, we contemplate alternative approaches to protecting privacy that have the potential to supplement consent in those cases. In evaluating the merits of these approaches, we should consider what changes need to be implemented in order for the approaches to function effectively. Some, like de-identification, could fit into the current legislative framework. Others, like expanding the grounds for legitimately processing personal information without consent, are a potential shift from the current norm and would require legislative change.


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

## a) De-identification

A number of related terms are used to describe the spectrum from completely anonymized to fully identified information. Anonymized data, as defined by the UK Information Commissioner's Office (ICO), is "(d)ata in a form that does not identify individuals and where identification through its combination with other data is not likely to take place."[73] Pseudonymised data falls somewhere on the spectrum between anonymized and fully identified data in that it carries varying degrees of risk of re-identification. According to the International Standards Organization (ISO), the process of pseudonymisation "allows for the removal of an association with a data subject. It differs from anonymization…in that it allows for data to be linked to the same person across multiple data records or information systems without revealing the identity of the person."[74] Pseudonymised data can be said to be a subset of de-identified data, which is data from which "the association between a set of identifying data and the data subject" has been removed. [75]

Privacy and data protection laws treat anonymized information as non-personal information that is not subject to privacy protections. The EU GDPR specifically excludes anonymized data from its scope. It recognizes pseudonymised data as a method of reducing privacy risk for individuals and as a safeguard to help data controllers meet their privacy obligations. "Pseudonymisation" is defined in the current version[76] of the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person."

A key aspect of de-identification is the assessment of the risk of re-identification. If de-identified data is generally at risk for re-identification, should the degree of privacy protection given to de-identified data be commensurate with the degree of risk of re-identification? In other words, the higher the risk of re-identification, the higher the level of protection that should be provided?

PIPEDA's provisions apply to personal information, defined as information about an identifiable individual. The OPC's interpretation of personal information has also been very broad. For example, in the OPC's guidance on Online Behavioural Advertising, we take the position that information collected for the purpose of OBA will generally be considered as personal information. In Canada, the Courts have ruled that "information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information."[77] This suggests that pseudonymised data could be personal information under PIPEDA and subject to all provisions of the Act.

There is an ongoing debate as to the value of de-identification as a privacy protection mechanism in today's environment of large data sets, personalized services and persistent tracking. Professor Paul Ohm[78] and others believe that information can never be truly de-identified, for the simple reason that too much secondary data is available which, when combined with the de-identified data, can enable the identification of individuals. For example, in the famous Netflix re-identification study, researchers were able to identify individual Netflix users in a supposedly "anonymized" dataset, by knowing when and how users rated as few as six[79] movies.

Some experts caution against the ad hoc nature of many de-identification techniques, and suggest that many released data sets can be re-identified with basic programming and statistics skills.[80] They also argue that the risk of re-identification of de-identified data sets grows over time as re-identification techniques become more effective and more data sets become available for matching.

Others, such as the Article 29 Working Party, believe in the value of de-identification as a strategy to mitigate the risks to individual's privacy while acknowledging the difficulty of creating a truly de-identified dataset that retains enough value to enable organizations to achieve their purposes. The WP29 is of the view that de-identification techniques can serve to protect privacy but only if they are rigorously engineered and risks of re-identification are monitored and mitigated on an ongoing basis.[81] For example, Article 38 of the GDPR provides for codes of conduct on the use of pseudonymisation as a means of safeguarding the processing of personal data.

Dr. Khaled El Emam argues that de-identification can be a useful privacy enhancing tool because following established procedures for de-identification will greatly minimize the risk of re-identification. He has demonstrated[82] that de-identification is particularly useful in health research because it allows the use of very sensitive personal information for the greater public good, such as advancing health research and improving the quality of health care, where consent may not be practicable. Dr. El Emam advocates a risk-assessment approach to de-identification that evaluates the risk of re-identification and optimizes the de-identification to ensure that the risk is below an acceptable threshold.

Privacy expert Robert Gellman[83] proposes protecting privacy by controlling the re-identification of de-identified data through contractual means. Under his proposal, where de-identified information is being shared between parties, the parties would enter into a voluntary contract formalizing an agreement not to re-identify the data and offering remedies if privacy protections are not upheld. Based on the premise that technical methods of de-identification reduce but do not eliminate the risk of re-identification, the contractual solution provides additional protection by holding accountable those who commit to not re-identifying information.

The Future of Privacy Forum (FPF) promotes de-identification as a method of ensuring privacy while retaining the commercial and scientific value of large data sets. The FPF is working to establish a framework for applying privacy protections to de-identified data factoring in nature of data, and risk of re-identification, as well as the presence of any additional administrative safeguards and legal protections, such as data protection policies or contractual terms that restrict how third parties can use the data.[84]

## Questions for Reflection

1) What are the criteria for assessing and classifying risk of re-identification?

2) Should consent be required for the collection, use and disclosure of de-identified data? If so, under what conditions?

3) Is there a workable, risk-based approach that can vary the stringency of the consent requirement with the risk of re-identifiability of data?

4) What role should contractual backstops play? Are there other ways to protect de-identified data?


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

## b) "No-Go Zones"

A "No-Go Zone" is a prohibition on the collection, use or disclosure of personal information in certain circumstances. It can be based on a variety of criteria, such as the sensitivity of the type of data, the nature of the proposed use or disclosure, or vulnerabilities associated with the group whose data is being processed. A true "No-Go Zone" creates a full prohibition against processing. However, a variation on this idea is a "Proceed with Caution Zone" in which additional substantive or procedural requirements are imposed in certain circumstances before collection, use or disclosure can occur.

### i) True "No-Go Zones"

Under PIPEDA, subsection 5(3), which imposes an over-arching limit on all processing, regardless of the presence of consent, constitutes a form of prohibition against inappropriate processing. In restricting an organization's collection, use and disclosure of personal information to purposes a reasonable person would consider appropriate in the circumstances, s.5(3) of PIPEDA forbids processing that could be considered inappropriate in a given context.

An organization may not proceed with collection, use or disclosure of personal information that conflicts with that standard of appropriateness, regardless of whether the individual has consented. This provision requires a relative comparison between the proposed use or disclosure and the surrounding circumstances. The contextual nature of s.5(3) lends it a certain flexibility as a restraint on inappropriate processing of data. For example, in the OPC's policy position on Online Behavioural Advertising,[85] this Office imposed two restrictions, or "No-Go Zones", at a best practice level: namely, organizations may not use methods of tracking that individuals cannot control, for example, device fingerprinting; and organizations should avoid knowingly tracking children and tracking on websites aimed at children. The first reflected the need to ensure individuals were able to exercise control over the technologies used to track them online; the latter reflected the difficulty of obtaining informed consent to such practices from children. Recently, the OPC found that a web site whose business model involved republishing court decisions without redacting the personal information they contain and allowing them to be indexed by search engines was acting contrary to s.5(3) of the Act. In that case, the OPC concluded that the organization's main purpose in posting this information was to incentivize individuals to pay for the removal of their personal information from the web site, a purpose the OPC considered "inappropriate."

"No-Go Zones" can also be established in relation to certain types of data, either in general terms, or in relation to particular uses of that data. For example, Bill S-201 attempts to do that by prohibiting the collection of genetic test results as a requirement for providing goods and services or entering into a contract. It is worth considering whether, even absent proposed legislation, Principle 4.3.3 and subsection 5(3) of PIPEDA would operate to restrict the collection and use of genetic test results in similar circumstances. However, since these PIPEDA provisions are broadly framed and subject to interpretation, would introducing specific and clear "No-Go Zones" be desirable?

### ii) "Proceed with Caution Zones"

Privacy legislation sometimes establishes enhanced procedural protections for certain categories of information, types of processing or in order to protect more vulnerable groups.

PIPEDA's approach to the question of the appropriate form of consent is an example of this. Under PIPEDA, the form of consent sought by an organization may vary, depending on the circumstances and type of information. The sensitivity of the information and the reasonable expectations of the individual in the circumstances are both relevant considerations in this assessment. Where information is sensitive, express consent will normally be required (such as with medical or financial records).

The GDPR relies on enhanced procedural protections for particular kinds of information and processing. Sensitive categories of data (including data relating to race or ethnic origin, religion or beliefs) is placed under a general prohibition on processing, which is then subject to a number of exceptions, including if the affected individual expressly consents to the processing. The GDPR establishes a similar prohibition in relation to automated decision-making about individuals: individuals have the right not to be subject to a decision based solely on automated processing, including profiling, if the decision could have a direct legal or similar impact on the individual. Again, this prohibition is subject to a range of exceptions, including the express consent of the individual.

The proposed U.S. *Consumer Privacy Bill of Rights Act* establishes a tiered system for processing of personal information by means of the principle of "respect for context." Under the U.S. bill, if an organization processes personal data in a manner that is not reasonable in light of the context in which the data was originally collected, it must conduct a privacy risk analysis and take reasonable steps to mitigate any privacy risks identified as a result. Such steps must include providing "heightened transparency and individual control" over processing. When organizations use or disclose data in ways that respect context, they are more likely able to infer consent to processing. When a proposed use or disclosure does not respect context, increased transparency and measures to facilitate individual choice would be required. Under this model, no substantive restrictions are placed on the purposes for which information can be collected, used or disclosed; the tiered system only impacts the level of procedural due diligence imposed on the organization.

The principle of "respect for context" bears some conceptual resemblance to the idea of "consistent use" employed in the federal *Privacy Act*, in which a use or disclosure that is consistent with the purpose for which the information was originally collected may not require the individual's consent. Key to employing either concept is the way in which the original "context" or original "use" is defined, since this will determine how broad a range of other uses can be considered "respectful" or "consistent."

The White House Report entitled *Big Data: Seizing Opportunities, Preserving Values*[86] suggests that if regulation shifted focus to responsible *uses* of data, consideration could better be paid to the balance between socially beneficial uses of big data and the harms to privacy. One way of operationalizing this would be to develop a taxonomy of data processing that would distinguish between purposes that would be permitted without consent, purposes that would be permitted only with express consent, and purposes that would be prohibited under *any* circumstances. Such an approach would appear to combine tiered procedural protections for different forms of processing with an absolute prohibition on certain uses or disclosures.


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

## Questions for Reflection

1) If subsection 5(3) can offer the possibility of true prohibitions, what should some of these prohibitions be?

2) Is subsection 5(3) sufficient or do we need further rules regarding "No Go Zones" for collection, use and disclosure, such as those involving potentially discriminatory practices or when children are involved?

3) Under PIPEDA, context and sensitivity help determine whether express or implied consent can be relied on. Should there be further rules depending on certain types of information or uses?

### c) Legitimate business interests

Under PIPEDA, meaningful consent is required for the collection and processing of personal information, with limited exceptions, which recognize that some situations do not lend themselves to individual consent. The notion that consent is not always workable is reflected in the new EU framework, which relies on several legitimate grounds for processing of data although the EU framework requires consent when information is sensitive.

PIPEDA's exceptions to consent align with several of the EU's grounds for lawful data processing. For example, the EU permits processing that is necessary for compliance with a legal obligation to which the controller is subject, while PIPEDA allows for collection, use or disclosure of personal information without consent as "required by law."

However, in the EU, legitimate interests can be used as a ground for lawful processing without consent. Specifically, data processing is lawful if it is necessary for the purposes of the "legitimate interests" pursued by the controller or third party, except where fundamental rights of the individual outweigh such interests, in particular where the data subject is a child. In other words, processing without consent is lawful subject to a balancing test weighing the organization's interests vis-à-vis the interests of the individual. The balancing can be a complex process, taking into account factors such as the nature of the data, the public interest, and the reasonable expectations of the individual.[87]

Given the challenges to the consent model in the digital environment, particularly with respect to big data and IoT, does PIPEDA's current reliance on consent need to be rethought in circumstances where other means might be used to achieve the desired balance between the organization's business needs and the individual's privacy rights? Broadening permissible grounds for processing under PIPEDA to include legitimate business interests subject to a balancing test might be one solution. Creating further exceptions under PIPEDA, which would need to be defined, might offer another possibility. If this route were to be considered, other frameworks, such as Ontario's *Personal Health Information Protection Act*, could help inform pre-conditions that would have to be met before processing personal information without consent. While these pre-conditions are in the context of health research and the public good, they may nevertheless offer a path forward.

## Questions for Reflection

1) In the absence of consent, what grounds for lawful processing could authorize the collection, use and disclosure of personal information?

2) How do we ensure a fair and ethical assessment of grounds for lawful processing that ensure the proper balance is achieved?

3) What would be the role of regulators in assessing grounds for lawful processing?

# 3) Governance

In this section, we identify possible solutions based on accountability as a means to ensure strong privacy protections. Some of the proposed solutions serve to enhance consent, some are alternatives to consent, and some may belong in a self-regulatory framework.

PIPEDA's accountability principle requires organizations to develop and implement policies and practices to uphold the FIPPs, including the obligation to obtain meaningful consent. Taken as a whole, these policies and practices constitute a privacy management program, the necessary elements of which are described in guidance[88] issued by the OPC together with our British Columbia and Alberta counterparts.

While an internal privacy management program is a good starting point for an organization, a more transparent and demonstrable approach is required to help give Canadians the assurance that organizations are holding themselves to responsible personal information management practices they profess to have and/or are obligated to have. The requirement for demonstrable accountability is gaining prominence in other jurisdictions, notably the EU, where the GDPR will require that organizations be able to demonstrate compliance with the law. Below are some examples of practical applications of accountability-based approaches that can help level the playing field for organizations and individuals in terms of seeking and providing meaningful consent to complex business practices.

## a) Codes of practice

Codes of practice are commonly used tools that provide practical guidance with respect to industry best practices on a range of activities, including regulatory compliance. On the privacy front, codes of practice can help promote transparency and openness with respect to how privacy obligations are met and addressed. Around the world, several data protection authorities (DPAs) and private sector organizations have


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

participated in the development of codes of practice that align with the requirements of data protection principles or laws. Depending on the legislation in place, these are either voluntary best practices developed by industry or are developed by DPAs to serve as an enforcement tool.

For example, in the UK, the Information Commissioner can encourage the development of codes of practice, or initiate one, following consultations with industry and the public. In Australia, credit reporting bureaus can develop codes of practice to be registered by the Commissioner. A breach of a registered code of practice can be investigated by the Commissioner.

In the U.S., the White House *Consumer Privacy Bill of Rights* promotes the idea of enforceable codes of conduct for specific markets or business contexts in order to provide consumers with more consistent privacy protections by standardizing privacy practices within sectors.

In Canada, paragraph 24(c) of PIPEDA mandates the OPC to encourage organizations to adopt instruments such as policies and codes of practice in line with PIPEDA requirements. We have not yet fully explored this provision. When it comes to consent, some might argue that codes of practice in particular sectors could provide an added measure of predictability and consistency for companies in terms of understanding their obligations around meaningful consent and appropriate limits on data processing. It might also be argued that codes of practice would offer greater clarity for individuals that their information is being processed in a transparent and fair manner in line with their expectations.

### Questions for Reflection

1) Could sectoral codes of practice indeed enhance consent and/or privacy protection?

2) How should they be enforceable?

3) Who should be involved in developing sectoral codes? Who should be responsible for overseeing compliance with sectoral codes?

## b) Privacy Trustmarks

Privacy seals, like codes of practice, can be a useful accountability mechanism for organizations to help ensure compliance with privacy laws and to demonstrate a commitment to privacy. Like codes of practice, these can be operated by privacy regulators or organizations, depending on the jurisdiction.

In France, la Commission nationale de l'informatique et des libertés (CNIL) operates an accountability seal program for companies that comply with the CNIL's standard for what accountability means in practice. The U.K. ICO recently introduced a privacy seal program[89] whereby the ICO will endorse third party operators to deliver the program. The operators will then be responsible for the day-to-day management of the program.

U.S.-based TRUSTe is one of the best known privacy seal programs. It has been operating since 1997 and primarily certifies websites. In Europe, EuroPriSe offers certification to manufacturers and vendors of IT

products and IT-based services. Its European Privacy Seal certifies that "data processing resulting from interactions between a web server and a user's browser conform to European data protection law."[90]

In a similar example of a scheme where third party agents are responsible for certifying adherence with privacy standards, the APEC Cross-Border Privacy Rules use accountability agents to help ensure that participating companies are compliant with privacy and security standards required under the APEC Privacy Framework.[91]

For a privacy seal program to function effectively in Canada, there would need to be an objective mechanism in place to evaluate how well the program aligns with legislated privacy requirements as well as an independent audit function to ensure continued upholding of standards. It would be necessary to consider whether PIPEDA should be amended, including the OPC's role, if privacy seals were to be pursued as part of a regulatory framework.

### Questions for Reflection

1) Under what conditions are trustmarks a sensible and reliable tool for protecting consumer privacy in the evolving digital environment?

2) How would a privacy seal program operate alongside PIPEDA?

## c) Ethical Assessments

Several initiatives are under way that aim to supplement or replace the consent model, in the context of big data and the like, by integrating the notions of fairness and ethics when balancing the organization's needs to process data for legitimate business purposes with the individual's right to privacy. These initiatives ultimately place the onus on organizations to make judgements on the benefits and risks of processing data for the organization, the individual, and society at large.

### i) Centre for Information Policy Leadership (CIPL)

The U.S.-based CIPL is developing an approach to protecting privacy in the age of big data that focuses on enhanced accountability, improved risk management and a new interpretation of core privacy principles and concepts. In a series of white papers,[92] CIPL suggests that organizations need to adopt enhanced accountability to deal with contexts where "express consent and granular individual control about specific data processing activities are not possible." The enhanced accountability model would incorporate more developed risk management and transparency as well as operationalizing fair processing and data ethics. The aim is to have a framework in place for protecting privacy either through informed consent "where possible and appropriate and through other mechanisms where necessary and appropriate." [93]

As for improving risk management, CIPL calls for developing and incorporating "a framework of privacy harms or other negative impacts, a framework for analyzing benefits resulting from data processing" and for recognizing risk management as a critical element of data protection concepts and tools. In particular,


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

better risk management will, in CIPL's view, enhance the privacy protection effectiveness of legitimate interest processing, fair processing, transparency tools and a renewed focus on context and data use.[94]

### ii) Future of Privacy Forum (FPF)

The work of the FPF on the use model as an alternative to consent is an example of a next generation accountability model that suggests replacing consent in appropriate circumstances. The 2014 FPF White Paper on big data[95] outlines a framework for organizations to guide them in evaluating the merits of big data projects by recognizing the interests of organizations as well as individuals, and allowing organizations to weigh big data benefits against privacy risks.

### iii) Information Accountability Foundation (IAF)

The IAF, which is also U.S.-based, is working on approaches to data protection in the age of big data through a series of interrelated projects aimed at developing solutions to issues such as evaluating the fairness of innovative data uses and identifying and mitigating risks to individuals. The IAF's Unified Ethical Frame[96] is a process for reaching an ethical position on whether a big data analytics project is appropriate by building on core data protection values to incorporate fundamental rights.

The IAF's Holistic Governance Project aims to improve the overall effectiveness of data protection by better aligning the responsibilities of the participants in information flows. For example, individuals would only consent where their consent is meaningful, and not consent when it is not, for example, in the case of a new use that is consistent with the original purpose. Organizations would expand risk assessment, transparency and accountability so that regulators are more informed about business practices.[97] According to the IAF, the Holistic Governance Project recognizes that both data collection and use should be part of an effective governance structure.

As part of their efforts, the IAF is working in Canada on a governance project for ensuring privacy protections where consent is not practicable and exploring how to effectively create a mechanism that functions similarly to legitimate interests as a means to use data beyond the expectations of reasonable persons.[98]

The work of CIPL, the FPF and the IAF raises the question of who will determine whether uses of data are ethical, fair, or appropriate and, in a Canadian context, whether these solutions would require changes to the legislative framework. Regarding the first issue, one could look to the scientific research community, which pioneered the creation of independent research ethics boards to review proposed research projects for ethical implications. Ethics review boards weigh the potential benefits of research against potential risks to research participants. Lately, academics and businesses have begun to posit whether an equivalent mechanism is needed to help guide commercial organizations wanting to exploit big data in order to conduct research into consumer behaviour. The concept of consumer ethics boards serving in an advisory capacity to corporations has been proposed as a means of helping them evaluate the broader implications of using personal information, particularly in a big data environment.

To some observers, the issue will be whether it is appropriate that organizations, even with advice from boards of ethics, be authorized to decide how to use the personal information of individuals, particularly if such boards are not truly independent nor have any meaningful veto power. These observers will want to know how individuals' rights can be protected and how the balance required under PIPEDA can otherwise be achieved. It is important to understand more clearly what might happen to the role of consent under these proposals and how they square with existing PIPEDA provisions.

Proponents explain their proposals either as a supplement to consent, as a substitute for consent, or as a means to balance an organization's needs to process data for legitimate purposes with the right to privacy of individuals. Each of these would have different implications for PIPEDA depending on how they are operationalized.

### Questions for Reflection

1) To what extent are the suggestions by CIPL, FPF and IAF helpful and practicable in assessing ethical uses?

2) To what extent can businesses be expected to self-regulate in a manner that protects individual privacy in the new digital age?

3) How should such ethics boards be created, composed and funded? Who should they report to, and what should be their decision-making authority?

## 4) Enforcement Models

The accountability-based solutions mentioned in this paper rely on organizations to develop and implement measures to respect their privacy obligations, including obtaining meaningful consent. PIPEDA's purpose is to balance the privacy rights of individuals with organizations' legitimate needs to collect, use and disclose personal information. While there are positive aspects to the ethical framework proposals discussed above, the process remains internal to an organization and the organization's interests remain paramount. Independent oversight bodies are intended to ensure this balance is maintained so that individuals' privacy interests are protected. The need for such independent oversight may be even more compelling where consent is impracticable and organizations take on a greater role in deciding what appropriate uses can be made of personal information.

In order for the OPC to be truly effective as an oversight body capable of protecting the privacy rights of individuals, what should be its attributes and authorities beyond independence? It may be worthwhile to contemplate engaging in proactive enforcement activity (either through the existing regulatory model or supplemented by third party assistance), in addition to enforcement based on complaints, as is typically the case under the current model. For example, if certain kinds of uses or disclosures were to be authorized by means other than consent (e.g. based on a legitimate business interest, using "respect for context" or through a technical tool such as de-identification) or be placed off-limits due to the enactment of a "No-Go Zone", not only might such alternatives to consent require organizations to be able to demonstrate compliance but they might also warrant enforcement or softer compliance engagement by the regulator at an earlier stage than is currently undertaken (e.g. spot checks or compliance reviews). That said, implementation of a more proactive compliance model should avoid imposing too much of a regulatory burden on organizations and if


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

implemented properly, could lead to organizations avoiding the significant costs associated with the introduction of a non-compliant program or of being subject to a formal investigation. At the same time, imposing a resource burden on the regulatory body should also be avoided.

The transparency mechanisms discussed in this paper require large-scale implementation if they are to make a measurable difference. Given the ongoing confusion individuals experience in understanding organizations' privacy practices, what are the incentives for organizations to invest in transparency? Should the consequences for non-compliance with PIPEDA be stronger than the ability to "name and shame"? Financial penalties are one way of ensuring that organizations accept greater responsibility for informing individuals what they plan to do with their personal information. The ability to levy fines exists in certain current EU country data protection laws as well as in the new EU GDPR.

Currently, the Privacy Commissioner can only make non-binding recommendations and has no power to make orders. This is in contrast to counterparts in provinces with substantially similar privacy legislation, as well as regulators in the EU and the U.S., who have order-making powers. The question of enhancing the Privacy Commissioner's powers under PIPEDA was explored in depth in a report by Professors Houle and Sossin in 2010.[99] These experts observed that provincial commissioners who have this power use it sparingly, preferring to resolve complaints through mediation, conciliation and other informal means. Nevertheless, order-making power was seen as a strong incentive for the parties to settle on reasonable terms. Houle and Sossin observed, "(l)ooking to the experience of provincial regulators in Canada, as well as to the American and European experience, the ability to levy fines and other order-making capabilities can lead to additional compliance and serve as an important deterrent even if not used often."

### Question for Reflection

1) What additional powers, if any, should be given to the OPC to oversee compliance and enforce new or enhanced consent rules?

# Conclusion

It is a daunting task to identify and implement mechanisms to support the consent model in the face of big data, the Internet of Things and future privacy challenges. This requires a systemic approach to privacy protection, involving a range of policy, technical, regulatory and legal solutions.

In tackling the issue of consent, we want to find solutions that will reduce the burden individuals face of having to understand complex business processes and that will provide individuals with a more meaningful way of exercising their privacy preferences. Consent remains an important means of controlling one's personal information, and more broadly to express one's dignity and autonomy. However, we also want to acknowledge that the current and future technological environments make it increasingly difficult to seek and provide informed consent. In that context, does the solution lie only in giving individuals better information and mechanisms by which to make informed choices, or must we find other ways to protect their interests?

Organizations also face challenges in fulfilling the requirement to obtain meaningful consent from individuals. Their need for innovation would be supported by greater clarity as to acceptable purposes for data processing in the absence of express consent and internal mechanisms that would guide them in balancing benefits to the organization against privacy risks to the individual. The challenge of such mechanisms lies in ensuring that the privacy risks are assessed independently and that the individual's interests are protected.

As part of the search for solutions, we need to ensure that the appropriate balance is being struck. The regulator's role and responsibilities as well as the overall privacy framework require regular review to ensure they are aligned with the new environment. Are legislative changes required to bolster the work of the regulator in holding organizations accountable and adequately representing the individual? What is the appropriate role of sectoral codes of practice, trustmarks, and third party certifiers in an effective compliance regime?

## Consultation Questions

We invite stakeholders to join in this discussion by contributing their views on the viability of the consent model and proposing solutions to improve individual control over personal information in the commercial environment. While we welcome views on all consent-related topics, we are particularly interested in answers to questions we posed earlier as well as the following:

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

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

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

4) What, if any, legislative changes are required?


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

[1] *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) Online at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[2] Fred H. Cate, Peter Cullen, and Victor Mayer-Schönberger. "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines." March 2014. Online at http://www.repository.law.indiana.edu/facbooks/23/; See also Eloïse Gratton, *Understanding Personal Information: Managing Privacy Risks*, LexisNexis, 2013 which advocates for an approach focusing on the risk of harm, which would have the result of reducing the burden of the notification obligation (and concurrently, the consent obligation).

[3] Center for Information Policy Leadership. "The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society." Discussion draft. October 21, 2015.

[4] Ann Cavoukian, Alexander Dix, and Khaled El Emam. "The Unintended Consequences of Privacy Paternalism." March 5, 2014. Online at https://www.privacybydesign.ca/index.php/paternalistic-approach-privacy-will-deliver-unintended-consequences/ Dr. Cavoukian is the former Ontario Information and Privacy Commissioner and currently Executive Director of the Privacy and Big Data Institute at Ryerson University.

[5] Alan F. Westin. *Privacy and Freedom*. 1967. New York: Atheneum. p. 33.

[6] Departments of Communications and Justice. "Privacy & Computers." 1972. P.14.

[7] *R v Dyment*, [1988] 2 SCR 417 at para 17. Online at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/375/index.do

[8] Stephanie Perrin, Heather H. Black, David H. Flaherty and T. Murray Rankin. *The Personal Information Protection and Electronic Documents Act*: An annotated guide. Irwin Law. 2001. p. 23

[9] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers , Local 401, 2013 SCC 62,* at para. 22

[10] Section 3 of PIPEDA

[11] Section 6.1 of PIPEDA

[12] Lisa M. Austin. "Is consent the foundation of fair information practices? Canada's Experience under PIPEDA." University of Toronto Legal Studies Series, Research Paper No 11-05. November 2005. Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=864364

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

[14] The sensitivity of information depends on the nature of the information and the context in which it is being collected, used or disclosed.

[15] Office of the Privacy Commissioner of Canada." Interpretation Bulletin: Form of consent." Online at https://www.priv.gc.ca/leg_c/interpretations_07_consent_e.asp

[16] Article 29 Data Protection Working Party. "Opinion 15/2011 on the Definition of Consent." July 13, 2011. Online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[17] Article 6 of the EU Data Protection Directive

[18] GDPR, See Article 6 + recitals 38, 56 and 57

[19] US Code, Title 15, Subchapter 1, Federal Trade Commission. Full text online at https://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I

[20] US Code, Title 15, Chapter 91, Children's Online Privacy Protection. Full text online at https://www.law.cornell.edu/uscode/text/15/chapter-91

[21] 37th International Privacy Conference Amsterdam 2015. "Privacy Bridges: EU and US privacy experts in search of transatlantic privacy solutions." Online at https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf

[22] Federal Trade Commission. *Protecting consumer privacy in an era of rapid change: Recommendations for Businesses and Policymakers*. March 2012. Online at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

[23] The White House. *Consumer Data Privacy In a Networked World: A Framework for protecting privacy and promoting innovation in the global digital economy*. February 2012. Online at https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[24] *Ibid.*page 1

[25] Administration Discussion Draft: *Consumer Privacy Bill of Rights Act of 2015*. Full text online at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf

[26]See for example, the Centre for Democracy and Technology post "Analysis of the *Consumer Privacy Bill of Rights Act*." March 2, 2015. Online at https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/

[27] Office of the Privacy Commissioner of Canada. "The Age of Predictive Analytics: From Patterns to Predictions." August 2012. Online at https://www.priv.gc.ca/information/research-recherche/2012/pa_201208_e.pdf

[28]*Office of the Privacy Commissioner of Canada*. The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments." February 2016. Online at https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp

[29] Danielle Keats Citron and Frank Pasquale. "The Scored Society: Due Process for Automated Predictions." University of Maryland Francis King Carey School of Law, Legal Studies Research Paper, No. 2014-8. . (2014) 89 *Wash. L.Rev* 1]

[30] The White House. *Big Data: Seizing Opportunities, Preserving Values*. May 2014. Online at https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[31] Latanya Sweeney. "Discrimination in Online Ad Delivery." Harvard University. January 28, 2013. Online at http://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf

[32] Federal Trade Commission Report. *Big Data: A toll for Inclusion or Exclusion?*January 2016. Online at https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

[33] Paul Ohm. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review, Vo. 57, 2010. Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

[34]Kate Crawford and Jason Schultz. "Using Procedural Due Process to Redress Big Data's Privacy Harms", New York University School of Law. October 2013.

[35] See Ira Rubinstein and Woodrow Hartzog, "Anonymisation and Risk" August 17, 2015. Washington Law Review, Vol. 91, No 2, 2016; Eloïse Gratton, "If Personal Information is Privacy's Gatekeeper, then Risk of Harm is the Key: A proposed method for determining what counts as personal information." Albany Law Journal of Science & Technology, Vol. 24, No. 1, 2013; Paul Schwartz & Daniel Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." 2011. 86 N.Y.U. Law Review 1814.

[36] Fred H. Cate and Viktor Mayer-Schönberger. "Notice and Consent in a World of Big Data: Microsoft Global Summit Summary Report and Outcomes." November 2012. Online at http://www.microsoft.com/en-ca/download/confirmation.aspx?id=35596

[37] 36th International Conference of Data Protection and Privacy Commissioners. "Resolution on Big Data." October 2014. Online at http://www.privacyconference2014.org/media/16602/Resolution-Big-Data.pdf

[38] 36th International Conference of Data Protection and Privacy Commissioners. "Resolution on Big Data." October 2014. Online at http://www.privacyconference2014.org/media/16602/Resolution-Big-Data.pdf

[39] Office of the Privacy Commissioner of Canada. "The Age of Predictive Analytics: From Patterns to Predictions." August 2012. Online at https://www.priv.gc.ca/information/research-recherche/2012/pa_201208_e.pdf

[40] Article 29 Data Protection Working Party. "Opinion 8/2014 on Recent Developments on the Internet of Things", September 16, 2014. Online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[41] *Office of the Privacy Commissioner of Canada*. "The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments" February 2016. Online at https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp

[42] Office of the Privacy Commissioner of Canada. "What an IP Address Can Reveal About You." May 2013. Online at http://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp

[43] Office of the Privacy Commissioner of Canada. "Metadata and Privacy: A technical and legal overview." Online at https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.asp

[44] Office of the Privacy Commissioner of Canada. "Policy Position on Online Behavioural Advertising." Online at https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp

[45] 36th International Conference of Data Protection and Privacy Commissioners. "Mauritius Declaration on the Internet of Things." October 14, 2014. Online at http://privacyconference2014.org/media/16596/Mauritius-Declaration.pdf

[46] BC Freedom of Information and Privacy Association. "The Connected Car: Who is in the Driver's Seat?" 2015. Online at https://fipa.bc.ca/connected-car-download/


30 Victoria Street – 1st Floor, Gatineau, QC K1A 1H3 • Toll-free: 1-800-282-1376 • Fax: (819) 994-5424 • TDD (819) 994-6591
www.priv.gc.ca • Follow us on Twitter: @privacyprivee

[47] Office of the Privacy Commissioner of Canada. "Wearable Computing – Challenges and opportunities for privacy protection." January 2014.
[48] Federal Trade Commission Staff Report. *Internet of Things: Privacy & Security in a Connected World*. January 2015. Online at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[49] Ian Kerr, jennifer barrigar, Jacquelyn Burkell, Katie Black. "Soft Surveillance, Hard Consent." From *Lessons from the Identity Trail.* Oxford University Press, 2009, page 21. Online at http://idtrail.org/files/ID%20Trail%20Book/9780195372472_Kerr_01.pdf
[50] PR Newswire. "According to a Study, Parents of Pre-Teens Don't Always Protect Their Children's Privacy Online." April 1, 2015. Online at http://news.sys-con.com/node/3319012
[51]Columbia Business School Center on Global Brand Leadership. "What is the future of data sharing?" 2015. Online at http://www8.gsb.columbia.edu/globalbrands/research/future-of-data-sharing
[52] Alessandro Acquisti, Laura Brandimarte and George Loewenstein. "Privacy and human behaviour in the age of information." Science vol 347 issue 6221,pp. 509-514. January 30, 2015. Online at http://www.sciencemag.org/content/347/6221/509.abstract
[53] Leslie John. "We say we want privacy online, but our actions say otherwise." *Harvard Business Review*. Online at https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise
[54] Chris Jay Hoofnagle and Jennifer M. Urban. "Alan Westin's Privacy Homo Economicus." 49 Wake Forest Law Review 261 (2014). Pp. 261-317. May 19, 2014. Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2434800
[55] Joseph Turow, Michael Hennessy and Nora Draper. "The Tradeoff Falacy: How Marketers Are Misrepresenting American Consumers And Opening Them up to Exploitation." Annenberg School for Communication, University of Pennsylvania. June 2015. Online at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf
[56] Aleecia M McDonald and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies." I/O Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review Issue. Online at http://aleecia.com/authors-drafts/readingPolicyCost-AV.pdf
[57] Helen Nissenbaum. "A contextual approach to privacy online."Dædalus, the Journal of the American Academy of Arts & Sciences. 140 (4) Fall 2011. Online at http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf
[58] Office of the Privacy Commissioner of Canada. "Guidelines for Online Consent." Online at https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp
See also "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps." Online at https://www.priv.gc.ca/information/pub/gd_app_201210_e.asp
[59] Maria Popova. "Mozilla's Privacy Icons: A Visual Language for Data Rights." BigThink.com. Online at http://bigthink.com/design-for-good/mozillas-privacy-icons-a-visual-language-for-data-rights
[60] Consumers Council of Canada. "Canadian Businesses and Consumers Both Face Risk from Poorly Understood Terms and Conditions Statements." October 2015. Online at http://www.consumerscouncil.com/improving-online-agreements-release
[61] The White House. *Big Data and Privacy: A Technological Perspective*. May 2014. Online at https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf
[62] World Economic Forum. *Unlocking the Value of Personal Data: From Collection to Usage*. Online at http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf
[63] Siani Pearson, Marco Casassa Mont. "Sticky Policies: An Approach for Managing Privacy across Multiple Parties." Computer, vol. 44, no. 9, pp. 60-68, Sept., 2011
[64] Article 29 Data Protection Working Party. "Opinion 8/2014 on the Recent Developments on the Internet of Things." September 16, 2014. Online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[65] Federal Trade Commission Staff Report. *Internet of Things: Privacy & Security in a Connected World. January 2015*. Online at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[66] The OTA is a non-profit industry group whose members include Microsoft, Symantec, ADT and TRUSTe.

[67] Online Trust Alliance. "OTA releases new Internet of Things Trust Network to Address Global Consumer Concerns." October 28, 2015. Online at https://otalliance.org/news-events/press-releases/ota-releases-new-internet-things-trust-framework-address-global-consumer
[68] For more information, see https://www.privacybydesign.ca/
[69] 32nd International Conference of Data Protection and Privacy Commissioners. "Resolution on Privacy by Design." October 2010. Online at https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf
[70] 36th International Conference of Data protection and Privcy Commissioners. "Resolution on Big Data." October 2014. Online at https://icdppc.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf
[71] Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*. 2012. Online at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers
[72] ENISA. "Privacy and Data protection by Design." January 12, 2015. Online at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design
[73] UK Information Commissioner's Office. "Anonymization: managing data protection risk code of practice." Online at https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
[74] International Standards Organization. "'Pseudonymization' – new ISO specification supports privacy protection in health informatics." March 10, 2009. Online at http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1209
[75] ISO/TS 25237:2008(E) Health Informatics – Pseudonymization, ISO, Geneva, Switzerland. 2008.
[76] Current as of the writing of this paper
[77] Gordon v. Canada (Health), 2008 FC 258 (CanLII)
[78] Paul Ohm. "Broken Promises of Privacy: Responding to the surprising failure of anonymization." UCLA Law Review, 57, 1701 (2009). Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006
[79] Arvind Narayanan and Vitaly Shmatikiv. "Robust de-anonymization of large sparse datasets" in *Proceedings of the 2008 IEEEE Symposium on Security and Privacy*, pp 111-125 (2008). Online at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf
[80] Arvind Narayanan, Joanna Huey and Edward Felten. "A Precautionary Approach to Big Data Privacy." March 19, 2015. Online at http://randomwalker.info/publications/precautionary.pdf
[81] Article 29 Data Protection Working Party. "Opinion 05/2014 on Anonymisation Techniques."April 10, 2014. Online at http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf
[82] Ann Cavoukian and Khaled El Emam. "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy." Office of the Ontario Information and Privacy Commissioner. June 2011. Online at https://www.ipc.on.ca/images/Resources/anonymization.pdf
[83] Robert Gellman. "The Deidentification Dilemma: A Legislative and Contractual proposal." Fordham Intellectual Property, Media and Entertainment Law Journal, Volume 21, Issue 1, 2011. Online at
[84] For more information, please see About De-Identification, Future of Privacy Forum. Online at https://fpf.org/issues/deid/
[85] Office of the Privacy Commissioner of Canada. "Policy Position on Online Behavioural Advertising." Online at https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp
[86] The White House. *Big Data: Seizing Opportunities, Protecting Values*. May 2014. Online at https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
[87] Article 29 Data Protection Working Party. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC." April 9, 2014. Online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[88] Office of the Privacy Commissioner of Canada. "Getting Accountability Right with a Privacy Management Program." Online at https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp
[89] UK Information Commissioner's Office Blog. "What you need to know about ICO Privacy Seals." January 28, 2015. Online at https://iconewsblog.wordpress.com/2015/01/28/what-you-need-to-know-about-ico-privacy-seals/
[90] EuroPriSe European Privacy Seal. Online at https://www.european-privacy-seal.eu/EPS-en/About-EuroPriSe
[91] The Asia Pacific Economic Cooperation Privacy Framework. Online at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

[92] As of the writing of this paper, drafts of the following white papers had been posted to the CIPL website: "The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Infomration Society" and "The Role of Risk Management." Online at https://www.informationpolicycentre.com/

[93] Centre for Information Policy Leadership. "The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society." Discussion draft. October 21, 2015.Online at https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/World_of_Big_Data_Accountability_and_Digital_Responsibility_Sustainable_Data-Driven_Economy_and_Information_Society.pdf

[94] Centre for Information Policy Leadership. "The Role of Risk Management." Discussion draft. February 16, 2016. Online at https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Protecting_Privacy_in_World_of_Big_Data_Role_of_Risk_Management.pdf

[95] Jules Polonetsky, Omer Tene and Joseph Jerome. "Benefit Risk Analysis for Big Data Projects." September 2014. Online at https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf

[96] The Information Accountability Foundation. "Unified Ethical Framework for Big Data Analysis: IAF Big Data Ethics Initiative, Part A, March 2015." Online at http://informationaccountability.org/wp-content/uploads/IAF-Unified-Ethical-Frame.pdf

[97] Information Accountablity Foundation. "Holistic Governance and Policy project: Introduction to the HGP Framework." October 29, 2015. Online at http://informationaccountability.org/wp-content/uploads/HGP-Overview.pdf

[98] Martin Abrams. "Information Impact Assessments Key to Protection with Innovation." IAF Blog. January 21, 2016. Online at http://informationaccountability.org/category/canada/

[99] France Houle and Lorne Sossin. "Powers and Functions of the Ombudsman in the *Personal Information Protection and Electronic Documents Act:* An Effectiveness Study." August 2010. Online at https://www.priv.gc.ca/information/research-recherche/2010/pipeda_h_s_e.asp