Submission to the
Office of the Privacy Commissioner of Canada

Consultation on Consent and Privacy

Submitted by:

Samuel E. Trosow, (Associate Professor, University of Western Ontario, Faculty of Law and Faculty of Information and Media Studies)

Scott Tremblay, J.D. Candidate 2017 (University of Western Ontario, Faculty of Law)

Daniel Weiss, J.D. Candidate 2018 (University of Western Ontario, Faculty of Law)

August 5, 2016
# Table of Contents

1. **Introduction** ........................................................................................................................................... 1  

2. **The foundational principles of the purpose-consent model are outdated** ......................... 2  
   2.1 General Changes ................................................................................................................................. 2  
      2.1.1 Efforts to de-personalize information are becoming increasingly futile. ............................ 2  
      2.1.2 The increased potential for aggregation and analytics undermines the traditional  
            sensitive/insensitive dichotomy ........................................................................................................ 3  
      2.1.3 The purpose-consent model is not appropriate where data collection and analysis is  
            the purpose ........................................................................................................................................ 4  
      2.1.4 Adherence to the data minimization principle has become less effective. .............................. 4  
      2.1.5 Many IoT devices capture information from third parties ....................................................... 5  
      2.1.6 Quality of consent has been eroded by technological advances and business  
            practices ............................................................................................................................................. 5  
   2.2 Internet-of-Things (IoT) Specific Challenges .................................................................................. 6  
   2.3 Summary ............................................................................................................................................... 6  

3. **Enhancing informed consent to be meaningful in the digital networked environment** ........... 7  
   3.1 Consent needs to be informed ............................................................................................................. 7  
      3.1.1 Background ................................................................................................................................... 7  
      3.1.2 Discussion of Purpose for the Collection ....................................................................................... 8  
   3.2 Third parties ......................................................................................................................................... 9  
   3.3 Problems with the purpose-consent model ....................................................................................... 9  
   3.4 Proposed Solutions ............................................................................................................................... 10  
      3.4.1 Reinforcing Consent ...................................................................................................................... 10  
      3.4.2 Establishing opt-in and opt-out procedures for superfluous collections .................................. 11  
      3.4.3 Deeming IoT Data to be personal and sensitive ........................................................................ 13  

4. **Stronger accountability and enforcement measures are needed to ensure that PIPEDA  
   maintains the balance it was designed to uphold** .............................................................................. 14  

Appendix A: examples of Consent Clauses ...................................................................................... 15  
Appendix B: Proposed Revisions to 4.3 Principle 3 - Consent .......................................................... 16
1. **INTRODUCTION**

We are submitting this paper to the Office of the Privacy Commissioner as part of the 2016 consultation on consent and privacy. We are pleased to see a government agency take a proactive approach to such a compelling and timely policy problem, and we welcome the opportunity to participate.

We believe that the current consent model is inadequate to protect the legitimate privacy interests of individuals in a time of increased technological complexity. Measures to strengthen consent need to be taken to ensure that consent is meaningful. Many of the historical conditions and assumptions underlying the adoption of the current consent model have become outdated, and we agree with the statement in the discussion paper that “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.”[1] However, we reject the assertion that consent requirements should be relaxed, as this would be detrimental to the fundamental privacy rights of individuals and it would fail to achieve the goals of PIPEDA. The purpose of PIPEDA is to establish a framework of data-collection rules

> “that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.”

Essentially this framework is based on a set of balancing principles, and a purposive approach should be taken in re-calibrated these principles from time to time. Instead of relaxing consent requirements, the consent model should be improved, and we will suggest several ways of strengthening it in order to keep pace with technological, economic and social developments. We agree with the viewpoint of the European Union that “the right to data protection and the right to privacy are two distinct human rights”[3] and we think these values are appropriate in the Canadian context.

---

[1] Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information protection and Electronic Documents Act at


[2] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 3 [PIPEDA].

Before turning to specific proposals, Section 2 will briefly outline some of the technological developments we think provide the context for requiring substantial changes to the current consent model. In terms of the Possible Solutions outlined in the OPC Discussion Paper, Section 3 will focus on “enhancing informed consent.” Making privacy policies more understandable and giving users and consumers better ways to understand and express their privacy preferences is a necessary component of any reform package. But while improving informed consent is a necessary step towards achieving the overall policy goals of protecting privacy, it is by no means a complete solution. So we will discuss further accountability and regulatory measures that will supplement making privacy policies more understandable in Section 4. These measures will include “stronger accountability mechanisms for organizations to demonstrate compliance with their current legal obligations”⁴ and also discuss ways to “strengthen regulatory oversight to ensure that proposed solutions are effective in protecting privacy.”⁵ We will conclude with a proposal for several textual revisions to PIPEDA Principle 4.⁶

2. **THE FOUNDATIONAL PRINCIPLES OF THE PURPOSE-CONSENT MODEL ARE OUTDATED**

2.1 **GENERAL CHANGES**

PIPEDA was conceived with the purpose of striking a balance between the interests of individuals in their personal information and the need of organizations to collect, use or disclose personal information. However, many of the historical assumptions and conditions underlying the striking of that balance have become outdated and need to be revisited. In particular, it should be emphasized that several of the old dichotomies (personal vs non personal information; sensitive vs non-sensitive information) are collapsing.

2.1.1 **Efforts to de-personalize information are becoming increasingly futile.**

In a case involving a database of information about suspected adverse reactions to health products, the Federal Court ruled that information is personal “where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.”⁷ However, recent advances in technology have made it difficult or

---

⁴ *OPC Discussion Paper* at 10 (3⁰ bullet).
⁵ *OPC Discussion Paper* at 11.
⁶ Attached as Appendix B.
impossible to predict what data may be aggregated with other available data such that it may be identified to a particular person once again. Seemingly impersonal data can be aggregated with other seemingly impersonal data to the extent of re-personalization. As such, the Office of the Privacy Commissioner of Canada found that the traditional method of binning information into the discrete categories of personal and non-personal is no longer appropriate.\(^8\) The concept of privacy should be thought of as both dynamic (constantly changing with the source’s social environment) and scaling (different data sets are more invasive or bear more risk if used improperly) in order to reflect the reality of today’s privacy landscape.

When PIPEDA was designed, the risk associated with the collection of information was apparent, and it was based on the type of data which was being collected. The risk in collecting one’s address was that the data subject’s address could be discovered. In the more recent context of the Internet of Things\(^9\) (IoT), data is collected continuously and generally combined (or combinable) with other data. Consequently the IoT generated data can be used to generate predictive assumptions about an individual that can reveal other information such as their socioeconomic status or other traditionally personal information such as ethnicity and age.

2.1.2 The increased potential for aggregation and analytics undermines the traditional sensitive/insensitive dichotomy.

The same statistical analysis technology which has created the risk that any data might be “repersonalized” (either purposefully or accidentally) has also rendered the distinction between sensitive and non-sensitive data irrelevant. In the same way that non-personal data can be re-identified, non-sensitive data can be used to draw what become sensitive inferences. In one

\(^8\) Policy and Research Group of the Office of the Privacy Commissioner of Canada, *The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments* (Gatineau: Office of the Privacy Commissioner of Canada, February 2016) at 20.

instance, the purchasing records of a Target customer allowed the company to infer her pregnancy status.\textsuperscript{10}

\textbf{2.1.3 The purpose-consent model is not appropriate where data collection and analysis is the purpose.}

The purpose limitation principle consists of two separate parts. First, data must only be collected for a specified explicit purpose, and no superfluous data should be collected (purpose specification). Second, data may not be further processed in a way that is incompatible with the purpose of the initial collection (compatible use).

The concept of “purpose limitation relies on the premise that it is possible to decide on the purpose of a certain data processing beforehand.”\textsuperscript{11} However, the value of data collection in many circumstances now “resides in the potential to uncover new correlations for potential new uses once the data have been collected.”\textsuperscript{12} The commercial reality today is that the primary purpose of data collection is to collect that data. Data collection is the purpose rather than being a means to an identifiable end.\textsuperscript{13}

Therefore, when “the purpose coincides with data collection and analysis,”\textsuperscript{14} the purpose limitation principle no longer limits what types of data may be collected. No data can be superfluous to that purpose. Consent to collection for this purpose opens up the consumer to having \textit{any} data collected about them, and used for nearly any purpose.

\textbf{2.1.4 Adherence to the data minimization principle has become less effective.}

The reason for the implementation of the data minimization principle is increasingly inconsistent with emerging practices. Many IoT devices, by their very nature, collect huge and indiscriminate data sets. Devices such as fitness trackers continuously collect data so long as they are powered on, and home security devices are intended to be always on and always monitoring the surrounding environment Of course, it is in this continuous data collection that these products


\textsuperscript{12} Moerel at 7.

\textsuperscript{13} Moerel at 7

\textsuperscript{14} Moerel at 8.
find their value. While collection of this sort is indiscriminate, it is allowable because it is as restricted as possible while achieving the goal of the product.

The ultimate result of this reality is that even while adhering to the data minimization principle, the combination of inherent value from continued data collection in devices such as fitness trackers, and the extremely broad identified purposes described above in 2.1.3 have the effect of ensuring that there is much more data in the marketplace about an individual than there previously was.

2.1.5 Many IoT devices capture information from third parties
Most devices can only collect information from the user or a person who intentionally uses the device. However, other IoT devices are designed such that they will inevitably collect information from third parties without their knowledge. In some newer devices such as the Amazon Echo, always-on microphones record all sounds in a room. This raises the inevitability that a third party (or child) could have their voice or other data recorded without even knowing that there is a data-collecting device in the room.

2.1.6 Quality of consent has been eroded by technological advances and business practices
Quality consent must be both informed and voluntary. It is difficult for consumers to give informed consent about the use of collected data because of the possibility of its aggregation with other data to accomplish more than the data sets can do separately. This has made the “purpose limitation principle” much harder to enforce in recent years.

First, consent has become woefully uninformed. The primary means of acquiring consent from end-users of technology is by means of a Privacy Policy or Terms of Use document. These are typically not ready by the end-user. Further, the use of the data may be fairly complicated to the extent that even if a user fully reads the policy, she may not fully understand how her data is being used and the consequences of that use.

Second, consent has become less voluntary in many circumstances. Many devices require the user to accept the privacy policy in order for the device to function.15 This forces users to part with personal information as part of the payment for access to a device or service. The user may

---

15 The traditional framework is that consumers agree to a Terms of Service contract when using a product and this ToS is associated with a Privacy Policy that the user is required to accept.
not access important services like Google search, or Facebook without consenting to the privacy policy – whatever that policy might entail.

Consent used to be the end-all of evidence that a person understood, and decided that a certain use of her information was in her interest. However, since consent is now often uninformed, and often given under threat of not being able to use a desired service, it no longer carries the weight that it used to.

2.2 **INTERNET-OF-THINGS (IoT) SPECIFIC CHALLENGES**

Wasser *et al.* describe how the advent of the IoT affects the privacy environment. This article describes a heightened risk of harm; increased sensitivity of personal information; more vulnerabilities and difficulty of patching; and vulnerabilities created by third parties.\(^\text{16}\)

Furthermore, while loss of privacy, injury or property damage may result solely from the failure of an IoT device, in other cases it may result from a combination of IoT device vulnerabilities and the intentional malicious exploitation by a third party. In 2015, various media reported on demonstrations conducted by attackers who were purportedly able to disable brakes and interfere with steering on Internet connected vehicles.\(^\text{17}\) Other media have reported on security experts being able to hack into a secured wireless network through "smart" light bulbs.\(^\text{18}\) While there has been debate about the practicality of specific exploits, it is reasonable to expect that an expanding base of Internet integrated devices will attract an expanding base of individuals looking to exploit those systems for nefarious purposes.\(^\text{19}\)

2.3 **SUMMARY**

To summarize this section, the foundation of modern privacy law relies on a balance struck between the privacy interest of each member of the public, and the ability of businesses to innovate and compete in an increasingly global economy. Some of the factors weighed in

---


striking the current balance have changed both qualitatively and quantitatively since then, so it is necessary that we re-calibrate this balance.

The ability to aggregate and recombine data sets has greatly diminished the relevance of the distinction between personally identifiable and anonymous data. It has also undermined the dichotomy between sensitive and non-sensitive personal information. While it is difficult to predict whether seemingly unassuming data might become personal or sensitive once aggregated with other available sets, new privacy and consent policies must recognize this problem.

3. **ENHANCING INFORMED CONSENT TO BE MEANINGFUL IN THE DIGITAL NETWORKED ENVIRONMENT**

Considering how much the founding assumptions of the current privacy law regime have changed, it is no surprise that the law based on those assumptions is outdated in some respects and needs to be revisited.

3.1 **CONSENT NEEDS TO BE INFORMED**

3.1.1 **Background**

The “reality of today’s data-driven society is that individuals often do not know which data are being processed about them, how they are being assessed and categorized by the data controllers, and what the consequences of this might be for them.”\(^{20}\) This is in part because even when they are supposedly informed, they are generally not properly informed. Moerel and Prins argue that “[i]f the information provided is shorter, citizens are not properly informed, but if proper information is provided, hardly anybody will read it.”\(^{21}\) They add that “[i]t is an illusion to suppose that by informing individuals better about which data are processed and for which purposes, we enable them to make more rational choices and to better exercise their rights.”\(^{22}\) This dilemma about the length and complexity of privacy policies presents a troubling paradox. The paradox of informed consent arises because if the information provided is shorter, a person is not fully informed, but if the full information is provided it is too long to reasonably expect a person to fully read and understand it.

---

\(^{20}\) *Moerel*, at 8.

\(^{21}\) *Moerel*, at 9, footnote 35.

\(^{22}\) *Moerel*, at 9.
Contractual Terms of Use (including Privacy Policies) are the standard method of informing data-subjects about how their data is being used, and to gain their consent. As these provisions are generally thought to be legally binding, they substantially affect the rights and obligations of the parties. Since these provisions are rarely read and even more rarely fully understood, this is a problem for consumers as well as data-collecting organizations.

To complicate matters, the growing complexity of data networks are so riddled with algorithms that in many instances it is unrealistic to expect that a person could understand. Further, in many contractual Terms of Service, the identified purposes are so broad that they become meaningless. The purpose typically declared in the ToS is “to provide the service that the device was designed and marketed to provide.” We feel this language is not only overbroad, but also circular. Our initial review of these provisions in popular consumer IoT applications reinforces these worries.\footnote{See attached Appendix A.} This purpose identification is of little value to consumers who wish to determine how their data is practically being used.

To compound the issue, even where the use and consequences of contractual provisions can be understood, it is unrealistic to assume that the reasonable person will have the time or inclination to read all of the privacy policies associated with all of the devices, services, and apps to which they subscribe and understand how they might interact with one another.

In sum, consent acquired under the current model is a legal fiction. It does not make sense to acknowledge that privacy policies are not being read and fully understood, while also pretending that the user is informed. Such constructive notice is not adequate to support a consent model in which consent must be both informed and meaningful. But how should this paradox be remedied?

3.1.2 Discussion of Purpose for the Collection

The reasons for establishing a purpose for the collection of data are twofold. First, it ensures that the data-subject is aware of how the data will be used, and this will inform their level of consent. Second, it sets a reasonable limit on the type of data that can be collected, and the use of that data in the future (to delineate the scope of the consent).
When an organization is collecting data as a means to achieve some other end purpose, an arm's-length and neutral third party arbiter (such as the OPC) is needed to objectively evaluate whether a sufficient relationship exists between the stated purpose and the data collected. A complaint that came before the OPC in 2005 provides a good example of how this limit operates. In that case, the OPC was able to draw clear connections between the extensive personal information that a bank collected in a credit card application (including date of birth; date, time, and location of transactions; purchase history; employer; repayment history on loans) with specific end results (including maintaining the integrity of the credit granting system; complying with various anti-money laundering legislation; protecting the bank from fraud). In the Internet of Things context where data collection is a more central purpose, the logic becomes circular.

3.2 THIRD PARTIES

Further issues of consent exist where the data is collected by the user about another person (such as by a body camera) and that third party does not know that the data is being collected. How can they have consented to the collection of personal information if they do not know that it has been collected? An increasing number of IoT devices risk capturing data from third parties, and they warrant further scrutiny.

3.3 PROBLEMS WITH THE PURPOSE-CONSENT MODEL

Once an organization has justified the collection of data, it must undertake to meet the operational principles on an ongoing basis. In the IoT context, these principles can be thought of as terms that the consumer is deemed to be entitled to enforce.

The Achilles’ heel of the purpose-consent model is the fact that it says very little about the legitimacy of the purposes. PIPEDA only requires that the purpose be “explicitly specified, and legitimate.” The way this works in practice is that a purpose is considered legitimate if it is one that “a reasonable person would consider … appropriate in the circumstances.” This essentially translates into a two-part test for the legitimacy of the purpose. First, there should be a “rational

---

24 Re PIPEDA Case Summary No 296 (2005), 2005 CarswellNat 6721 (OPC).
25 If, indeed, they are thought of this way, an inference may be drawn that PIPEDA severely restricts the use of choice-of-law clauses.
26 PIPEDA, Schedule 1, Clause 4.3.3.
27 PIPEDA, s 5(3); Re PIPEDA Case Summary No 296, 2005 CarswellNat 6721 (OPC).
connection” between the data that was collected and the ends to be achieved.\textsuperscript{28} Second, the organization collecting data must balance the costs and benefits of using the specified data as a means to achieve the desired result. The OPC has set out some factors to consider such as: whether the method is likely to be effective, whether a less-intrusive means exists, and whether the benefit gained by the data-collector is proportional to the loss of privacy suffered by the data-subject.\textsuperscript{29}

Applying this test for the legitimacy of purposes does not make sense in the IoT context. The problem is that a purpose that underpins the data collection must be directed at some kind of tangible result. When the purpose and end result are both the data collection itself, PIPEDA does not provide any mechanism to evaluate whether the purpose is legitimate or not.

3.4 PROPOSED SOLUTIONS

We would like to propose multiple solutions to the problems delineated above. First, it is our position that reinforcing the current consent doctrine is necessary, but is not sufficient to uphold the goals of PIPEDA. Second, we would like to propose a new approach that might replace or work in tandem with the purpose-consent model.

3.4.1 Reinforcing Consent

Reducing the amount of information that’s found in privacy policies and presenting it in a way that makes sense to the ordinary person is the next step toward informed consent. While many corporations have attempted to write their privacy policies without legal jargon,\textsuperscript{30} and this is certainly desirable, these texts must still address a whole range of legal clauses. As such, they are still too long to expect the average person to read and fully understand.

One mechanism which might avoid the current paradox of informed consent (the paradox whereby if the information provided is shorter, a person is not fully informed, but if the full information is provided it is too long to reasonably expect a person to fully read and understand it) is to filter out information which is already assumed by the user. In practice, the average person may be comfortable skipping over privacy policies because they have faith that government regulations (or industry standards or privacy watchdogs or the fear of bad press)

\textsuperscript{28} Re PIPEDA Case Summary No 114, 2003 CarswellNat 5826 (OPC).
\textsuperscript{29} Re PIPEDA Case Summary No 114
\textsuperscript{30} See attached Appendix A.
already prevent those policies from having objectionable clauses. If those unobjectionable clauses can be identified and filtered out of privacy policies, then what remains is simply the information required for the user to determine how this particular product or service strays from their privacy expectations.

In practice, this would mean creating a standardized best practices privacy policy to be implied by statute, subject to reasonable contractual modifications. Privacy policies would not need to address any areas imposed by statute unless the policy-writer wished to stray from the standardized best practices. Since all of the basics of a typical privacy policy would be implied by default, a privacy policy under this regime would generally be quite short, displaying only those areas where the device or service strays from the standard privacy policy (which should come to reflect the user’s expectations). This approach is in line with the legal theory that contractual terms which are particularly unusual or onerous necessitate a higher level of notice, and it has many practical benefits.

First, the number of privacy policies presented to users on an ongoing basis would be dramatically reduced, assuming that most products do not deviate from the standard policy and would therefore not need to give additional notice to users. This may sound like reducing the consent requirement of the privacy regime, but it is not. To make this change would simply bring the law into synchronicity with how people are already behaving, and it would introduce a baseline level of certainty into the process.

Second, when a user is presented with a privacy policy, she would know that the policy-writer is proposing an unusual use of her data and might be more inclined to read the shorter, less cluttered text.

3.4.2 Establishing opt-in and opt-out procedures for superfluous collections

One issue that we have identified with the current model is that data is often collected for the purpose of data collection, which leaves the user vulnerable to any data being collected. Something that we feel is important in order for users to maintain control over their personal information is the ability to opt in to or opt out of unwanted data collections and uses which are
not necessary for the individual device, service, or app to function, and that this ability be without penalty to the consumer.

Presented in combination with a filtered-down privacy policy, this provides users with a powerful tool to control their personal information. Under this proposed model, a user who purchases an IoT device would be presented with a very simple privacy policy. Its elements would be:

a) A statement noting that the device, service, or app complies with the standard privacy policy except for a certain number of exceptions;

b) A list of those clauses which deviate from the standardized policy, but which are necessary for the individual device, service, or app to function;

c) A list of those clauses which are not necessary for the individual device to function paired with the option to opt in or out of these collections or uses without penalty.

While this method also provides corporations with a powerful tool for data collection, it lowers the risk to consumers of being coerced to given consent. While mandated to draw attention to practices which do not conform with the OPC-approved policy, this method retains some flexibility for corporate collection policies. If a map application really wants to use your GPS location for the purposes of targeted advertising in a completely different service offered by the same company – it needs to ask, and the consumer is free to agree or decline. It could provide separate consideration for the consumer’s provision of this additional information. What this limits is situations where users are giving uninformed consent, or else consenting under the threat of losing access to a desired (and perhaps necessary) service.

---

31 It is possible that circumstances exist where a collection or use is not necessary for the individual device to function, but it would impede the functionality of all such devices if everyone were to opt out. Google maps, for example, collect your GPS information to determine traffic patterns to advice other users of ideal routes. We propose that in these circumstances the user should have the ability to opt out nevertheless.

32 A health app, for example, might need to move your data to its own servers in order to analyze that data and provide the output for the user – but if the corporation has chosen to host that personal information on servers outside of the country to save money, it might not comply with the standardized privacy model and therefore require notice and consent.

33 For example, the user of a search engine may find that the search engine wishes to use their search history in order to better target advertisements. This is not necessary for the service to function, so there should be an option to opt-out without disruption of the service.
Additionally, determining data collection and use based on whether it is necessary for the product to function rather than on whether it is connected to a potentially vague pre-determined purpose solves the issue of overbroad terms in privacy policies.

3.4.3 Deeming IoT Data to be personal and sensitive

The dichotomies between personal information and non-identifiable information as well as that between sensitive and non-sensitive data have been rendered effectively irrelevant because of the power of complex algorithms. These algorithms are getting stronger, not weaker, and it is necessary to acknowledge this reality in any proactive privacy regime. In the context of IoT data, we believe that it is necessary to presume that all IoT data is sensitive unless that presumption is rebutted, and to deem all IoT data as personal even after it has been allegedly depersonalized. This is due to the highly increased risk of repersonalization, and the ability of powerful algorithms to make sensitive inferences from otherwise insensitive information.

“[T]he European Commission’s Article 29 Data Protection Working Party adopted an opinion on IoT40 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”; that by combining even depersonalized 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.”

The law needs to reflect this change in technology. The current law was created when depersonalized information would generally stay that way, and non-sensitive information was just that – not sensitive. Now that the default has changed in reality, it should also change in the eyes of the law.

---

34 OPC Discussion paper at 8.

35 In light of the significance of above discussion, we do not support the creation of “No-Go Zones” as we do not think they would be necessary. “No-Go Zones” are the solution to the problem that people are consenting to collections and uses of their data that they should not be consenting to. We believe that this can be remedied by re-establishing the meaningfulness of choice (consent) through increased information and voluntariness rather than limiting each person’s freedom to choose altogether.
4. **Stronger Accountability and Enforcement Measures are Needed to Ensure that PIPEDA Maintains the Balance It was Designed to Uphold**

A twenty first century society ought to guarantee privacy in a way that is genuinely meaningful for its citizens. Maintaining privacy as a fundamental freedom means that there must be “real opportunities” for people to create a certain degree of space for themselves. “…every individual in a society must be able to exercise real freedom and have genuine opportunities to make choices and act on the basis of those choices.” In this context, this means that consent is only meaningful if it is truly voluntary.

Finally, in order to accomplish the purposes we have discussed, the OPC will need to have clear order making powers along with the ability to impose fines and penalties.

Where a person were to discover that their data was “used” illegally, they must now put in substantial effort in order to rectify what will likely be a very small issue for them, and indeed likely a large collection of small issues for thousands of people. At the same time, large corporate collectors of personal information have much stronger incentives and resources to address these privacy issues from their perspective. This disparity creates an untenable balance, one that very sorely needs to be addressed. Given the changing nature of the technological, economic and social environments in which personal information is routinely exchanged, the Canadian OPC needs to take a more proactive, even aggressive role in maintaining the balance that PIPEDA is designed to promote. Without deliberate action, this balance will increasingly tilt away from the privacy interests of individual consumers.

---

37 Moerel, “Privacy for the homo digitalis” at 38, citing Amartya Sen 2009 (but did not include the citation).
## APPENDIX A: EXAMPLES OF CONSENT CLAUSES

<table>
<thead>
<tr>
<th>Device</th>
<th>Purpose of Data Collection</th>
<th>Link to Privacy Policy</th>
</tr>
</thead>
</table>
| **Fitbit**                      | Fitbit uses your data to provide you with the best experience possible, to help you make the most of your fitness, and to improve and protect the Fitbit Service. Here are some examples:  
  - Height, weight, gender and age are used to estimate the number of calories you burn.  
  - Contact information is used to send you notifications, allow other Fitbit users to add you as a friend, and to inform you about new features or products we think you would be interested in.  
  - Data and logs are used in research to understand and improve the Fitbit Device and Fitbit Service; to troubleshoot the Fitbit Service; to detect and protect against error, fraud or other criminal activity; and to enforce the Fitbit Terms of Service.  
  - De-identified data that does not identify you may be used to inform the health community about trends; for marketing and promotional use; or for sale to interested audiences. | [https://www.fitbit.com/ca/privacy](https://www.fitbit.com/ca/privacy) |
| **Nest**                        | We use this information to provide, develop and improve Nest Products and services, including to make assessments and recommendations about products, safety, or energy use. We may use your contact details to send you this information, or to ask you to participate in surveys about your Nest use, and to send you other communications from Nest. | [https://nest.com/ca/legal/privacy-statement-for-nest-products-and-services/](https://nest.com/ca/legal/privacy-statement-for-nest-products-and-services/) |
| **August Smart Lock**           | Personal Information is used for the following purposes:  
  (i) to provide, administer and improve our Services,  
  (ii) to better understand your needs and interests,  
  (iii) to fulfill requests you may make,  
  (iv) to personalize your experience,  
  (v) to provide Service announcements,  
  (vi) to provide you with further information and offers from August or third parties;  
  (vii) to administer rewards, surveys, sweepstakes, contests, or other promotional activities or events sponsored or managed by August or our business partners; and  
  (viii) to comply with our legal obligations, resolve disputes with users, enforce our agreements and to protect, investigate and deter against fraudulent, harmful, unauthorized or illegal activity | [http://august.com/legal/privacy-policy](http://august.com/legal/privacy-policy) |
| **GE Café Connected Appliances**| GE may use Connected Data to register your connected Appliances, improve the products and services we provide and to enhance your experience with the GE family of companies. GE may analyze the Connected Data and provide recommendations to you on how to optimize the use of your connected Appliance and provide you with, tips, maintenance, and repair programs related to GE's products and services. We also may use Connected Data for internal purposes which include, but are not limited to, administration of our websites, data analytics, market research purposes, identification and execution of sales, marketing and advertising opportunities and compliance with law or legal process and our policies and procedures. | [http://www.geappliances.com/privacy/privacy_policy_connected.htm](http://www.geappliances.com/privacy/privacy_policy_connected.htm) |
APPENDIX B: PROPOSED REVISIONS TO 4.3 PRINCIPLE 3 – CONSENT

Note that these are in MS Word “Revision Mode” format so that the changes may be easily visualized.

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where it is inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, a new and separate consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records, records collected through a device in a personal residence, records collected through a wearable device, and income records) is almost–always considered to be sensitive, any information can be sensitive, depending on the context. Since information that is not in itself sensitive may become sensitive when combined with other information, sensitivity will generally be presumed. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special interest magazines might be considered sensitive.
4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless express consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive—either by itself or in combination with other information. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

- (a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- (b) a checkoff box may be used to allow individuals to request consent that their names and addresses not may be given to other organizations. Individuals who do not check the box are assumed not to consent to the transfer of this information to third parties;
- (c) consent may be given orally when information is collected over the telephone provided a written confirmation of such consent is immediately sent to the consumer; or
- (d) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or reasonable contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.