Canadian Journal of Law and Technology

Volume 17 | Number 1 Article 2

6-1-2019

Privacy and Connected Objects

Nicolas Karsenti

Recommended Citation

Nicolas Karsenti, "Privacy and Connected Objects" (2019) 17:1 CJLT 34.

Privacy and Connected Objects

Nicolas Karsenti

INTRODUCTION

Our society perennially seeks to multiply its connectivity in the name of greater efficiency. Over the past few years, several devices that had previously been quite basic have been made "smarter" in order to facilitate a consumer's life. A recent study highlights that some of the most common reasons for using "smart" objects are home automation and remote control.[1] Thus, convenience is driving companies, particularly appliance makers, to connect their devices to the internet in order to make them "smart".[2] These range from intelligent thermostats, smart fridges, connected pacemakers, smart watches and personal assistants (PAs) such as Alexa, Siri or Cortana, which exist within most devices of their parent companies. While innovation is the engine of the future, one has to wonder whether these recent advancements bring us too close to the Dickian and Orwellian futures we have been warned about for decades. The fear was never that we would get too advanced, since technological advancements are usually inherently positive, but rather that our penchant for an ever-present connection would strip us of our intimacy. The paper explores the privacy concerns that emerge from connected objects. More specifically, it examines how these objects fit within the framework of Quebec's privacy legislation, as well as Canada's federal privacy legislation. It also seeks to highlight the current flaws in the application of this framework to connected objects.

1. TECHNICAL OVERVIEW OF CONNECTED OBJECTS AND DATA COLLECTION

a. Definition

The first step in understanding the flaws in current privacy legislation is to define a smart object. Although there are varied definitions of a smart object, this paper relies on the version used by Mattern and Floerkemeier:

> Objects which using sensors, are able to perceive their context, and via built-in networking capabilities would be able to communicate with each other, access Internet services and interact with people.[3]

[1] Eric Zeng, Shrirang Mare & Franziska Roesner, "End User Security and Privacy Concerns with Smart Homes" (Paper included in the Proceedings of the Thirteenth Symposium on Usable Privacy and Security, July 2017) 65 at 68.

[2] Peter Milley, "Privacy and the Internet of Things" (2017) SANS Institute Information Security Reading Room at 3.

[3] Friedemann Mattern & Christian Floerkemeier, "From the Internet of Computers to the Internet of Things" in Kai Sachs, Ilia Petov & Pablo Guerrero, eds, *From Active Data*

Through the study of these objects, we will see that there exists a lack of compatibility with the current privacy framework. Smart objects can perform numerous tasks, and their "connected" status stems from their ability to communicate with each other, identify each other, locate themselves, transform electrical signals into real-life movement, and even store conversations to sharpen the effectiveness of future interactions (and publicity).[4] Underlining these functions is the ability to perceive their surroundings, to take decisions based on the data they collect, and to transmit this data.[5] Recently, IBM's CEO put forward the idea of a "Smart Earth" where every resource is connected for maximum efficiency.[6] But technology comes at a price.

b. Data Collection

A further study of how connected objects obtain data provides insight into the potential conflicts with the current privacy framework. Smart objects are built with sensors to interact with the environment and have the capability to cater to consumer needs.[7] Sensors process information and then store a smaller record of it on the cloud — through a technique called edge computing.[8] This cloud is often protected by very basic security measures.[9] As inconsequential as the data may seem, even the most innocuous information can be intrusive and dangerous. Ranger summarizes it best:

> Take the smart home: it can tell when you wake up (when the smart coffee machine is activated) and how well you brush your teeth (thanks to your smart toothbrush), what radio station you listen to (thanks to your smart speaker), what type of food you eat (thanks to your smart oven or fridge), what your children think (thanks to their smart toys), and who visits you and passes by your house (thanks to your smart doorbell).[10]

Management to Event-Based Systems and More (Berlin, Germany: Springer, 2010) 242 at 242.

[4] *Ibid.*

[5] Md Mahmud Hossain, Maziar Fotouhi & Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things" (Paper included in the Proceedings of the IEEE World Congress on Services, June 2015) 21.

[6] Ivan Ganchev, Zhanlin Ji & Mairtin O'Droma "A Generic IoT Architecture for Smart Cities" (Paper included in the Proceedings of the Joint 25th IET Irish Signals & Systems Conference and China-Ireland International Conference on Information and Communications Technologies, June 2014) 196.

[7] Hossain, *supra* note 5 at 2.

[8] Xio Technologies, "IoT Edge Computing: Architected for Performance and Reliability", White Paper (June 2017) at 2.

[9] Stephen Ornes, "Core Concept: The Internet of Things and the Explosion of Interconnectivity" (2016) 113:40 *Proceedings of the National Academy of Sciences* 1059.

[10] Steve Ranger, "What is the IoT? Everything You Need to Know about the Internet of

In line with this idea, recent studies have demonstrated that regular items not usually associated with tremendous security risks, such as lightbulbs or smoke detectors, are extremely vulnerable to attacks.[11] This suggests that significant privacy issues emerge from connected objects. Some stem from the potential misuse by a company,[12] but others stem from the fact that the information on these devices is often protected by a flawed security system.[13] Until recently, companies would install only the most basic security, such as using "guest" for the login and password,[14] largely based on the fact that most consumers do not know how to secure their smoke detector or their thermostat, if the option even exists. This tendency stems from a market failure for investment in cybersecurity.[15] Consumers bear the brunt of the costs when a breach occurs, while companies face few costs for failing to provide a secure environment and obtain very little return on investment when they do.[16] Verizon published a report which demonstrated that almost all of the vulnerabilities exploited had been made public for more than a year.[17]

Excellent examples of flawed security practices have emerged in recent years, particularly in the United States. A company named TRENDnet sold home cameras connected to smart phones and the internet. [18] Their security system was so basic that at one point anyone with the IP address of one of their cameras could, with a little tweaking, view a live feed and listen into the consumer's house.[19] Another camera maker, D-Link, had hardcoded the username and password of every camera to be "guest", had left a private key code to access their system on a publicly available website for six months, and had forgotten to encode users' credentials on their mobile app, leaving this information as a clear readable packet.[20] In a different area of connected objects, ASUSTek Computing

Things Right Now" (21 August 2018) ZDNet, online: < www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ > .

[11] Zeng, *supra* note 1 at 68.

[12] Kaivan Karimi & Gary Atkinson, "What the Internet of Things (IoT) Needs to Become a Reality" (2014) White Paper of Freescale Semiconductor, Inc. and ARM, Inc. at 4, online: < www.mouser.com/pdfdocs/INTOTHNGSWP.PDF > .

[13] Milley, *supra* note 2 at 3.

[14] *Federal Trade Commission v. D-Link Corporation & D-Link Systems Inc.*, 2018 WL 6040192 (N.D. Cal. 2018) ["*D-Link*"].

[15] Michael Kende, "Global Internet Report 2016" (Internet Society: 2016) at 18, online: < www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf > .

[16] *Ibid.*

[17] Verizon, "2016 Data Breach Investigations Report" (Verizon: 2016) at 15-16, online: < enterprise.verizon.com/resources/reports/2016/DBIR_2016_Report.pdf >

[18] *TRENDnet Inc. v. Federal Trade Commission*, No. 12-CV-1223090 (N.D. Cal. 2013) ["*TRENDnet*"].

[19] *Ibid.*

[20] *D-Link*, *supra* note 14.

had similarly faulty security. They made smart routers.[21] These routers gave the consumers access to cloud computing, that it claimed was secure.[22] Yet, anyone could access the user's personal cloud when typing in the associated URL into a browser.[23] Furthermore, the router had a default setting that made "admin" the administrator's account username and password.[24] These are only a few examples of a recent trend of inadequate security for connected devices.

The data that a company gathers can be used to identify the user's habits,[25] and this information could be used or sold without the user's knowledge. One of the greatest risks is a hacker learning about a person's life habits, including how often they drink coffee or when they open their garage door, which could lead to major security issues.[26] Major privacy risks also lie within PAs.[27] PAs exist to simplify the most mundane of tasks, from ordering a pizza to changing the colour of your lightbulb.[28] They are activated by a keyword (be it 'Hey Siri' or 'Hey Google'), are directly connected to online marketplaces, and often have access to our credit cards or our calendars.[29] Although they are not always recording, they are constantly listening, potentially turning them into tiny spies within our homes for a malicious user who manages to activate their key word at a distance.[30] Since smart objects are a treasure trove of personal data on users, they must be properly secured and used by the companies that make them,[31] in order to protect them from hackers attracted to the potential of these simple machines, most recently as bots for sophisticated attacks.[32]

[21] *Re ASUSTeK Computer Inc*., Federal Trade Commission file no 142 3156 (settled 2016), online: < www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter > ["*ASUSTeK*"].

[22] *Ibid.*

[23] *Ibid.*

[24] *Ibid.*

[25] Ruby R Dholakia & Nikhilesh Dholakia, "Scholarly Research in Marketing: Trends and Challenges in the Era of Big Data" (2013) William A Orme Working Paper Series No 2013/14 10, online: < web.uri.edu/business/files/Encycl-Communication-DataMining-n-Marketing-.pdf > .

[26] Alexandra Gheorghe, "The Internet of Things: Risks in the Connected Home" (2016) Bitdefender Research Paper, online: < www.bitdefender.com/files/News/file/Bitdefender-2016-IoT-A4-04_en.pdf > .

[27] Xinyu Lei et al, "The Insecurity of Home Digital Voice Assistants — Amazon Alexa as a Case Study" (2018) arXiv Paper No 1712.03327v2, online: < arxiv.org/pdf/1712.03327.pdf > .

[28] *Ibid.*

[29] *Ibid.*

[30] Hyunji Chung et al, "Alexa, Can I Trust You?" (2017) 50:9 Computer 100.

[31] Aliya Ramji et al, "Managing Big Data Privacy and Security" (2017) 46:1 Int'l L News 1.

[32] Chung, *supra* note 30 at 7.

2. QUEBEC-CANADA LEGISLATIVE FRAMEWORK FOR CONNECTED OBJECTS

We dissected the legal framework in Quebec for private organizations into two parts. The Canadian federal government has a privacy law, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[33] Similarly to other provinces, which are not the subject of this paper, Quebec has adopted a privacy law of its own, *The Act Respecting the Protection of Personal Information in the Private Sector*.[34] In 2002, the Government of Canada published the *Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council*.[35] This exempted organizations from *PIPEDA* when they were subject to provincial legislation that was judged to be *substantially similar* to *PIPEDA* with respect to the collection, use or disclosure of personal information occurring within that province. *PIPEDA* continues to apply in cases of a federal work, or when the data is collected outside the province. Thus, we will study the regulatory compliance of connected objects with regard to both of these laws.

In 2000, the Canadian law on privacy, *PIPEDA*, was passed.[36] It was created to protect people's personal information when it is collected, used or disclosed by organizations, while also acknowledging the need for them to do so at times.[37] The act applies to any *commercial activity* where *personal information* is used, collected or disclosed.[38]

The privacy framework of Quebec is set out in the *Act respecting the protection of personal information in the private sector* (the Act).[39] This Act must be read hand-in-hand with article 4 of the *Charter of human rights and freedoms*, articles 35 to 40 of the *Code civil du Québec* (*CCQ*),[40] as well as the *Act to establish a legal framework for information technology*.[41] The Court of Appeals has affirmed,[42] and reaffirmed,[43] the quasi-constitutional status of the Act,[44] and

[33] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ["*PIPEDA*"].

[34] *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c. P-39.1 ["QC *Private Sector Privacy Act*"].

[35] *Process for the Determination of Substantially Similar Provincial Legislation by the Governor in Council* (2002) Canada Gazette 2385.

[36] *PIPEDA*, *supra* note 33.

[37] *PIPEDA*, *supra* note 33 at s. 3.

[38] *PIPEDA*, *supra* note 33 at s. 4(a).

[39] QC *Private Sector Privacy Act*, *supra* note 34.

[40] *Code Civil du Québec*, C.Q.L.R. c. CCQ-1991 at ss. 35-41 ["*CCQ*"].

[41] *Act to establish a legal framework for information technology*, C.Q.L.R. c. C-1.1.

[42] *Québec (Commission d'accès à l'information) c. ArcelorMittal Montréal inc.*, 2016 QCCA 1336, 2016 CarswellQue 7704 (Q.C. C.A.) ["*ArcelorMittal*"].

[43] *Drouin c. 9179-3588 Québec inc.*, 2013 QCCA 2146, 2013 CarswellQue 12649 (Q.C. C. A.) ["*Drouin*"].

[44] *ArcelorMittal*, *supra* note 42 at para 52; *Drouin*, *supra* note 43 at para 51.

the Supreme Court has recognized the quasi-constitutional status of privacy laws.[45] As stated above, it was deemed to be "substantially similar" to *PIPEDA* by the Governor in Council, in accordance with s. 26(2)(b) of *PIPEDA*.[46] This exempts organizations that fall under the purview of the Act from complying with *PIPEDA* while collecting, using or disclosing information within the province of Quebec.[47] Many of the principles found in *PIPEDA* are also present in the Act, therefore they will be presented side by side in an effort to avoid repetition, as well as to highlight the differences and their impact on connected objects.

In *PIPEDA*, a commercial activity is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character [. . .]."[48] The test, laid out by the Supreme Court in *Regional Assessment Commisioner v. Caisse Populaire de Hearst*, is "whether it [the organization] has as its preponderant purpose the making of a profit."[49] As the parent companies and manufacturers of these connected objects easily fit within this definition, there is no need to delve further into its complexities.

While *PIPEDA* employs the notion of commercial activity, the Act uses the *CCQ*'s concept of organized economic activity.[50] This notion is larger, as it also applies to unions, lawyers and physicians.[51]

Personal information is defined, in the context of *PIPEDA*, as "information about an identifiable individual."[52] This creates "a very elastic definition"[53] which encapsulates a lot of information. The key component to information fitting in this definition is identifiability,[54] the "data elements must be attributable to a specific individual."[55] In the Gordon case,[56] the Federal Court accepted the following test, submitted by the Privacy Commissionner:

[45] *Douez v. Facebook, Inc*, 2017 SCC 33, 2017 CarswellBC 1663 (S.C.C.).

[46] *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374; *PIPEDA*, *supra* note 33 at s. 26(2)(b).

[47] *Ibid.*

[48] *PIPEDA*, *supra* note 33 at s. 2(1).

[49] *Ontario (Regional Assessment Commisioner) v. Caisse Populaire de Hearst Ltée*, [1983] 1 S.C.R. 57 at 70, 1983 CarswellOnt 563 (S.C.C.).

[50] *CCQ*, *supra* note 40 at art. 1525(3).

[51] Michael Power, *The Law of Privacy in Canada*, 2nd ed (Toronto: LexisNexis Canada, 2017) at section 4.5.4.

[52] *PIPEDA*, *supra* note 33 at s. 2(1).

[53] *Citi Cards Canada Inc. v. Pleasance*, 2011 ONCA 3, 2011 CarswellOnt 6 (O.N. C.A.) at para 22.

[54] Power, *supra* note 51 at s. 4.1.2.A.

[55] Power, *supra* note 51 at s. 4.1.2.A.

[56] *Gordon v. Canada (Health)*, 2008 CarswellNat 522, [2008] F.C.J. No. 331, 2008 FC 258 (F.C. T.D.).

> 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 available information.[57]

The courts have also used the same test negatively, asking whether "a person will be identifiable if the information disclosed, together with other publicly available information, would tend to or possibly identify them".[58]

The Act has a similar scope, as it applies to any personal information collected, used, disclosed or communicated in the course of an enterprise within the meaning of the *CCQ*.[59] It defines personal information as "any information which relates to a natural person and allows that person to be identified".[60] This has been clarified by the courts, and the *Commission d'accès à l'information*, as any information which: "(i) permits someone to learn something; (ii) relates to a natural person; and (iii) is capable of identifying the person."[61] The Act excludes from its scope information which is made publicly available by law.[62] Information about an object relating to the person is not necessarily personal information as it can only identify indirectly,[63] but the combination of information on the object and the person can bring it under the scope of the Act.[64]

When considering the case for the personal data collected by connected objects, we look at previously identified areas of personal information. The Privacy Commissioner has found that personal information encapsulates: IP addresses (in certain cases);[65] device identifier information;[66] mobile subscriber

[57] *Ibid* at para. 34-35.

[58] *Girao v. Zerek Taylor Grossman Hanrahan LLP*, 2011 FC 1070, [2011] F.C.J. No. 1310 (F.C. T.D.) at para 32.

[59] QC *Private Sector Privacy Act*, *supra* note 34 at s. 1.

[60] QC *Private Sector Privacy Act*, *supra* note 34 at s. 2.

[61] Power, *supra* note 51 at s. 4.5.5.

[62] *Champagne c. Caisse populaire Desjardins de la Vallée du Gouffre*, 2002 QCCAI 186, 2002 CarswellQue 3772 (C.A.I. Qué.).

[63] *Cie d'assurances ING du Canada c. Marcoux*, 2006 QCCQ 6387, 2006 CarswellQue 6142 (C.Q.) at para 27.

[64] *J.C. c. SSQ, société d'assurances générales inc.*, 2017 QCCAI 129, 2017 CarswellQue 13061 (C.A.I. Qué.) at para 37.

[65] Office of the Privacy Commissioner of Canada, *Assistant Commissioner Recommends Bell Canada Inform Customers about Deep Packet Inspection*, *PIPEDA* Report of Findings #2009-010 (September 2009), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/2009_010_rep_0813/> ["OPC re Bell Canada"].

[66] Office of the Privacy Commissioner of Canada, *Investigation into the Personal Information Handling Practices of WhatsApp Inc.*, *PIPEDA* Report of Findings #2013-001 (15 January 2013), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/*PIPEDA*-2013-001/>; Power, *supra* note 51 at s. 4.1.2.A.

ID;[67] mobile network and country code;[68] payload data from unsecured wireless networks collected inadvertently;[69] the individual's name[70] and email address.[71] Of particular interest for connected objects, especially PA's, is that the Privacy Commissioner considers the characteristics of a person's voice to be personal information.[72] It is seen as biometric information, and is thus more sensitive, similarly to a fingerprint or an iris pattern.[73]

Another important qualification is with regard to Online Behavioural Advertising. In the Privacy Commission's *Policy Position on Online Behavioural Advertising*, the position taken was that while most of the information captured (third-party tracking cookies, IP addresses, browser settings) is not personal, the cumulative effect of this mass of information could make it identifiable, and thus personal.[74] The vast quantities of data gathered by connected objects, which can highlight several key aspects of an individual's life, offer strikingly similar parallels. Indeed, as the *Privacy Engineer's Manifesto* suggests, "if you can access, correlate, and associate identity and activity in the IoT, you will pretty much be able to write a biography that will shock mothers and end marriages".[75] Thus, the information gathered by connected objects could be considered personal information because of its range.[76]

[67] *Ibid.*

[68] *Ibid.*

[69] Office of the Privacy Commissioner of Canada, *Google Inc. WiFi Data Collection*, *PIPEDA* Report of Findings #2011-001 (20 May 2011), <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/*PIPEDA*-2011-001/>.

[70] Office of the Privacy Commissioner of Canada, *Bank Provides Former Employee with Insufficient Access to his Personal Information*, *PIPEDA* Report of Findings #2013-004 (18 July 2013) at paras 82-87, online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/*PIPEDA*-2013-004/>.

[71] Office of the Privacy Commissioner of Canada, *Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, *PIPEDA* Report of Findings #2016-005 (22 August 2016) at paras 146-149, online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/*PIPEDA*-2016-005/>.

[72] *Turner v. Telus Communications Inc.*, 2005 FC 1601, [2005] F.C.J. No. 1981 (F.C.) at para. 22.

[73] *Ibid* at para 12.

[74] Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising" (December 2015), online: <www.priv.gc.ca/en/privacy-topics/advertising-and-marketing/behaviouraltargeted-advertising/bg_ba_1206/>.

[75] Michelle Dennedy, Jonathan Fox & Thomas R Finneran, *The Privacy Engineer's Manifesto*, (New York: Apress, 2014) at 17.

[76] 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: <www.priv.gc.ca/media/1808/iot_201602_e.pdf> ["OPC on IoT"].

Before diving further into the core principles of these laws, a last point is of note. With regard to *PIPEDA*, the Privacy Commissioner has no extraterritorial powers per se. Initially, the pursuit of investigations regarding companies outside of Canada was seen as outside the scope of the Commissioner's purview.[77] In 2007, the Federal Court ruled that the Privacy Commissioner did have the power "to investigate complaints relating to the transborder flow of personal information".[78] This reasoning was based on the Canadian component of the information collected, in order to create a psychological profile.[79] The data had been sculpted in the US, but it had originated from Canada, and thus the Privacy Commissioner had the right to investigate whether this data collection complied with *PIPEDA*.[80] The "real and substantial link" theory was used broadly in the case of an online foreign organization by the court in *A.T. v. Globe24h.com*[81] for the purposes of applying *PIPEDA*. This principle could also apply to connected objects where Canadian data is uploaded to foreign servers.

Also, s. 5(1) of *PIPEDA* obliges organizations to comply with Schedule 1 of *PIPEDA*.[82] This schedule is a series of principles that come from the *CSA Model Code for the Protection of Personal Information*.[83] We discuss these principles further below. Additionally to these constraints, s. 5(3) of *PIPEDA* subjugates the collection, use and disclosure of personal information to "purposes that a reasonable person would consider are appropriate in the circumstances".[84] This obligation is one of the most significant in the act.[85] It subjugates the consent of a person towards their information to an objective standard of reasonableness.[86] This standard was set out by the Court in *Eastman v. Canadian Pacific Railway*.[87] The test was created by the Privacy Commissioner to determine whether there was a violation of s. 5(3).[88] The four questions are :

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?[89]

[77] *Lawson v. Accusearch Inc*., 2007 FC 125, [2007] 4 F.C.R. 314 (F.C.) at para 14.

[78] *Ibid* at para 51.

[79] *Ibid* at paras 38-43.

[80] *Ibid.*

[81] *A.T. v. Globe24h.com*, 2017 FC 114, 2017 CarswellNat 184 (F.C.) at paras. 47-64.

[82] *PIPEDA*, *supra* note 33 at s. 5(1).

[83] Canadian Standards Association, *Model Code for the Protection of Personal Information*, (1996) CAN/CSA-Q830-96.

[84] *PIPEDA*, *supra* note 33 at s. 5(3).

[85] Power, *supra* note 51 at s. 4.1.6.

[86] Power, *supra* note 51 at s. 4.1.6.

[87] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, [2004] F.C.J. No. 1043 (F.C.).

[88] *Ibid* at para 13.

Subsequent cases have used this test, or variants of it, when facing allegations of s. 5(3) violations.[90]

The 10 principles outlined in Schedule 10 are the core of *PIPEDA*.[91] They do not focus on preventing the collection, use and disclosure of personal information, but rather on the purposes for which this information is used.[92] For the purpose of this paper, we have targeted certain fundamental categories of privacy law that would be most affected by connected objects and the IoT.

The first category is consent, which is the core and first step of any privacy legislation. This is represented by s. 4.3 of *PIPEDA*.[93] The second category is collection, especially limiting its breadth, represented by principles 4.4.[94] The third is safeguarding the information, which is especially difficult to uphold in a connected world. It is represented by s. 4.7 of *PIPEDA*.[95] The penultimate category is exactitude, which requires both the accuracy of the information and access to it. It is highlighted by ss. 4.6 and 4.9 of *PIPEDA*.[96] The last category, accountability, is overarching, as it applies to every step of the privacy cycle. It is part of s. 4.1 of *PIPEDA*.[97]

Consent

Consent is the act of accepting that an organization may collect some data for specified purposes.[98] Consent is always required except in rare circumstances that will not be discussed here. Furthermore, consent cannot be given to explanations that are too vague and sweeping,[99] since the individual cannot "reasonably understand how the information will be used or disclosed".[100] Many consumers are completely unaware of the data collected by their connected

[89] *Ibid.*

[90] As an example of the same test see Office of the Privacy Commissioner of Canada, *Law School Admission Council Investigation: Executive Summary*, *PIPEDA* Case Summary #389 (29 May 2008), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/exec_080529/ > ; for a variation on this test see *Turner*, supra note 72 at para 23.

[91] Power, *supra* note 51 at s. 4.1.

[92] *Englander v. Telus Communications Inc.*, 2004 FCA 387, [2005] 2 F.C.R. 572 (F.C.A.) at para 42.

[93] *PIPEDA*, *supra* note 33 at sched. 1 s. 4.3.

[94] *Ibid* at sched. 1 s. 4.4.

[95] *Ibid* at sched. 1 s. 4.7.

[96] *Ibid* at sched. 1 ss. 4.6, 4.9.

[97] *Ibid* at sched. 1 s. 4.1.

[98] Ibid at sched. 1 s. 4.3.

[99] Office of the Privacy Commissioner of Canada, *Bank Adopts Sweeping Changes to its Information Collection Practices*, *PIPEDA* Case Summary #2002-97 (30 September 2002), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/*PIPEDA*-2002-097/ > .

[100] *PIPEDA*, *supra* note 33 at sched. 1 s 4.3.2.

objects.[101] Indeed, the trend is towards smaller objects, bracelets and lightbulbs for example, that do not possess the interface to communicate the consent of the user yet amass mountains of data.[102]

An organization cannot require consent to data collection in order to use the product or service, beyond what is required to fulfill legitimate purposes. Thus, obtaining the SIN of a person cannot be a requirement to obtaining internet[103] or banking services.[104] This limit is nuanced by organizational security concerns, and the utility of more sensitive information in enhancing security measures.[105]

Consent can either be implicit or explicit.[106] Consent to collect can thus be opt-in or opt-out. Opt-in requires express consent to gather data. Opt-out requires positive action for the gathering to cease. For an organization to use opt-out consent, it must pass a four-part test.[107] The organization must demonstrate that the information is not sensitive "in nature and context".[108] The information-sharing situation must be well-defined and regulated in terms of the scope of the personal information that could be shared.[109] The purposes "must be limited and well-defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected".[110] Lastly, the opt-out process must be convenient.[111]

[101] Yvonne O'Connor et al, "Privacy by Design: Informed Consent and Internet of Things for Smart Health" (2017) 113 Procedia Computer Science 653 at 653-656.

[102] > Eloïse Gratton, "Beyond Consent Based Privacy Protection" (11 July 2016) *Eloïse Gratton* (blog) at 16, online: < www.eloisegratton.com/files/sites/4/2016/07/Gratton_-Beyond-Consent-based-Privacy-Protection_-July2016.pdf > .

[103] Office of the Privacy Commissioner of Canada, *Company Asks for Customer's SIN as a Matter of Policy*, *PIPEDA* Case Summary #2001-22 (5 November 2001), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/*PIPEDA*-2001-022/ > .

[104] Office of the Privacy Commissioner of Canada, *Using SIN for Identity Verification Cannot be a Condition of Service, PIPEDA* Case Summary #2017-006 (20 December 2017), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2017/*PIPEDA*-2017-006/ > .

[105] Office of the Privacy Commissioner of Canada, *Movie Theatre Chain Strengthens Personal Information Handling Practices*, *PIPEDA* Case Summary #2005-304 (7 June 2005), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/*PIPEDA*-2005-304/ > ; *Individual Objects to Request for Information as Condition of Supply of Service*, *PIPEDA* Case Summary #2002-94 (2 December 2002), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/*PIPEDA*-2002-094/ > .

[106] *PIPEDA*, *supra* note 33 at sched. 1 s 4.3.6.

[107] Power, *supra* note 51 at s. 4.1.7.3.

[108] Office of the Privacy Commissioner of Canada, *Bank Does Not Obtain the Meaningful Consent of Customers for Disclosure of Personal Information*, *PIPEDA* Case Summary #2003-192 (23 July 2003), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/*PIPEDA*-2003-192/ > .

[109] *Ibid.*

[110] *Ibid.*

When information is likely to be considered sensitive, consent should be explicit, and thus opt-in.[112] Due to the very sensitive nature of the data captured by connected objects, especially in the case of connected homes,[113] explicit consent could be required more often. The use of customer data with usage information for targeted ads was found by the Privacy Commissioner to require opt-in consent. This could potentially apply to connected objects which collect data on usage, have personal customer information, and use this combined data for targeted advertisement.

Even when consent is given, "binary, one-time consent and traditional definitions of personal information are increasingly perceived as outdated".[114] Privacy law is trending towards requiring a flexible method of consent that can be given throughout the object's lifespan, and "simplistic, 'on/off' personal data management policies may be neither flexible, nor appropriate, in the fast-developing online environment".[115] Article 29 Working Party of the EU addressed the issue of consent in connected objects, noting that in the case of smart watches, the opacity of their data collection system caused "'low-quality' consent based in a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals".[116]

Provincially, consent is outlined in s. 14 of the Act. It differs from the consent required in *PIPEDA*, which has a dual opt-in and opt-out approach depending on the sensitivity of the information. The Act requires that consent be "manifest, free, and enlightened, and [. . .] given for specific purposes".[117] It must also be limited to the time necessary to accomplish the aforementioned goals.[118]

The high level of consent required is thus extremely hard to meet with implicit consent.[119] The *Commission d'accès à l'information* (CAI) wrote that an individual dealing with a bank had given manifest consent because it was written, specific, limited in time, and the objective of the data collection was well understood by the person and well-defined by the notice which they signed.[120] In the context of connected objects, this will make consent more difficult to obtain.

[111] *Ibid.*

[112] *PIPEDA*, *supra* note 33 at sched. 1 s. 4.3.6.

[113] Dholakia & Dholakia, *supra* note 25.

[114] OPC on IoT, *supra* note 76.

[115] *Ibid.*

[116] European Union, Article 29 Data Protection Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things" (2014) at 7, online: < www.dataprotection.ro/servlet/ViewDocument?id = 1088 > .

[117] QC *Private Sector Privacy Act*, *supra* note 34 at s 14.

[118] *Ibid.*

[119] *Syndicat de Autobus Terremont ltée-CSN c. Autobus Terremont ltée,* 2010 QCCA 1050, 2010 CarswellQue 5303, [2010] J.Q. no 5005 (C.A. Que.) at paras 99-100.

[120] *Allain c. Caisse populaire Laval-des-Rapides*, 2004 QCCAI 25, 2004 CarswellQue 12407 (C.A.I. Qué.) at para 18.

A recent Australian study highlighted the difficulties of obtaining "meaningful" consent with current connected objects.[121] Participants reported that most objects had mandatory opt-in policies in order to use them.[122] They also felt lost when trying to understand most consent forms, creating uncertainty as to the quality of their consent.[123] Recommendations were made to have "multiple points of consent with the ability to revoke earlier forms of consent or opt out if necessary along the data use life-cycle".[124]

For the consent to be complete, organizations must identify the purpose(s) of their data collection, and they must keep a trail of their collection for later justification, if need be.[125] The avowed goal of identifying the purposes behind the collection is to limit the capture of unnecessary data.[126] Organizations should communicate the reasons for the data collection to the individual, at the time of or before.[127] Inadequacy in communicating purposes is often cited by the Privacy Commissioner as a failure.[128]

For example, an airplane company had collected information for lost baggage.[129] The purposes identified were tracing the baggage and creating a basis for the claim.[130] The information sought included the person's Social Security number and employment situation.[131] This information was not *necessary* to the baggage tracing system, nor the claim's system.[132] Thus, this collection violated *PIPEDA*.[133] In 2009, the Commission found that Facebook's default privacy settings violated this principle because the purposes of the data collected through these settings was not properly explained to users.[134] The same syllogism could

[121] Rachelle Bosua et al, "Privacy in a world of the Internet of Things: A Legal and Regulatory Perspective" (2017) Networked Society Institute Research Paper No 6, online: < networkedsociety.unimelb.edu.au/__data/assets/pdf_file/0008/2640779/IoT-and-privacy-NSI-Disc-6.pdf > .

[122] *Ibid* at 10.

[123] *Ibid.*

[124] *Ibid* at 13.

[125] Power, *supra* note 51 at s. 4.1.7.2.

[126] *PIPEDA*, *supra* note 33 at sched. 1 s. 4.2.2.

[127] *Ibid* at sched. 1 s. 4.2.4.

[128] Power, *supra* note 51 at s. 4.1.7.2.

[129] Office of the Privacy Commissioner of Canada, *Air Traveller Offended by Airline's Information Requirements for Baggage Claim*, *PIPEDA* Case Summary #2003-148 (9 April 2003), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/*PIPEDA*-2003-148/ > .

[130] *Ibid.*

[131] *Ibid.*

[132] *Ibid.*

[133] *Ibid.*

[134] Office of the Privacy Commissioner of Canada, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents*

be applied to connected objects. The purposes of the data collected through the default privacy settings, and through a change in them, would have to be explained to the user. If an organization identifies a *new* use for a particular information, the purpose sharing process must be repeated with the user.[135]

Provincially, according to the Act, an enterprise may only collect information for a "serious and legitimate reason".[136] There must be a "legitimate and justifiable link"[137] between the information gathered and the activities of the enterprise. The information must also be "necessary"[138] although the term "relevant" was also used with regard to Article 37 *CCQ*. "Necessary" was defined in opposition to what is "superfluous, without object nor pertinence".[139] When creating a folder of information on an individual, the enterprise's goal must be determined, articulated and recorded.[140] During the creation of the file, the enterprise must also communicate three elements to the person:

(1) the object of the file;
(2) the use which will be made of the information and the categories of persons who will have access to it within the enterprise;
(3) the place where the file will be kept and the rights of access and rectification.[141]

Collection

This principle requires that organizations only capture the information necessary to fulfill the purpose identified by them, and for which they obtained consent.[142] A failure to find appropriate purposes will result in a collection that also infringes on this principle.[143] In Quebec, an enterprise may only establish a file for a serious and legitimate reason.[144] Thus, the collection is limited to the motives behind the establishment of the file.[145] Information collected in violation of other privacy laws will not qualify as a collection under the act.[146]

Act" (16 July 2009) at paras 89-99, online: < publications.gc.ca/collections/collection_2010/privcom/IP54-31-2009-eng.pdf > ["Denham"].

[135] *PIPEDA*, *supra* note 33 at sched. 1 s. 4.2.4; Power, *supra* note 51 at s. 4.1.7.2.

[136] QC *Private Sector Privacy Act*, *supra* note 34 at s. 4; Power, *supra* note 51 at s. 4.5.6.

[137] Power, *supra* note 51 at s. 4.5.6.

[138] QC *Private Sector Privacy Act*, *supra* note 34 at s. 5; Power, *supra* note 51 at s. 4.5.6.

[139] *B.(P.) c. Lepage,* 2010 QCCQ 5982, 2010 CarswellQue 6968 (C.Q.) at para 91.

[140] QC *Private Sector Privacy Act*, *supra* note 34 at s. 4; Power, *supra* note 51 at s. 4.5.6.

[141] QC *Private Sector Privacy Act*, *supra* note 34 at s 8.

[142] *PIPEDA*, *supra* note 33.

[143] Power, *supra* note 52 at s. 4.1.7.4.

[144] QC *Private Sector Privacy Act*, *supra* note 34 at s. 4; Power, *supra* note 51 at s. 4.5.6.

[145] Power, *supra* note 51 at s. 4.5.6.

[146] *Drouin*, *supra* note 43 at para 27.

The idea of limiting the collection of data runs contrary to the purpose of connected objects. At their core, they seek to collect the most data possible. In an average supermarket, 544 TB of data per day could be collected.[147] Smart objects are filled with sensors that constantly collect data on their environment,[148] and this data is used to improve the decision-making skills of the machines (through neural networks and deep learning).[149] Problems emerge when a line has to be drawn between the information that is crucial to the purposes of the organization, and that which is superfluous. Almost anything can be included under umbrella purpose terms such as "improving the user's life", especially with the recent advances in machine-learning, which require large data-sets for the machine to become more effective in its interactions.[150]

Safeguards

This principle is a headache for technologists in the context of connected objects. It demands that personal information be protected by security safeguards equivalent to the *quality* of the information. The security measures required by *PIPEDA* are very similar to those included in the Act. Security proportional to the sensitivity, purpose and quantity of the information is also the rule.[151] With the multitude of sensors within connected objects, even the most minute details can be used to identify a person and their intimate habits.

Organizations are in a rush to market new products. Security "is often an afterthought in the architecture of many wide spread IoT devices".[152] Thus, at times, simple security measures are lacking from known household products. This has already enabled several hackers to take advantage of weak security systems to form botnets.[153] A recent study found that certain devices do not even use a Secure Socket Layer connection, a basic security standard for internet

[147] Shen Bin, "Research on Data Mining Models for the Internet of Things" (Paper included in the proceedings of the 2010 International Conference on Image Analysis and Signal Processing, 9 April 2010) at 1.

[148] Nguyen Luong et al, "Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: Survey" (2016) 18:4 IEEE Communications Survey & Tutorials 2546.

[149] Shuochao Yao et al, "Deep Learning for the Internet of Things" (2018) 51:5 Computer 32 at 33.

[150] Pedro Domingos, "A Few Useful Things to Know about Machine Learning" (2012) 55:10 Communications of the ACM 78.

[151] QC *Private Sector Privacy Act*, *supra* note 34 at s. 10; *Stacey c. Sauvé Plymouth Chrysler (1991) inc.*, 2002 CarswellQue 1310, [2002] J.Q. no. 1155, [2002] R.J.Q. 1779 (C.Q.) at para 102.

[152] Kishore Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV): IoT Botnets" (2017) arXiv Paper No 1702.03681v1, online: <arxiv.org/pdf/1702.03681.pdf>..

[153] Manos Antonakakis et al, "Understanding the Mirai Botnet" (Paper included in the Proceedings of the 26th USENIX Security Symposium, 16 August 2017), online: <www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf>.

navigation.[154] Most devices did not provide for the possibility of an update to face zero-day vulnerabilities, thus denying themselves the chance to patch their systems and re-secure their customers.[155] Another study found that most wearable connected objects did not change MAC addresses, enabling any bystander to persistently track the user.[156] Furthermore, many devices use the most basic combination of username and password, with the user being excluded from changing them, making these devices particularly vulnerable. The world was made brutally aware of this fact with the explosion of Mirai attacks.[157] Originally developed by an American college student, these intrusions were first used to hack 600,000 devices with a combination of 61 common usernames and passwords,[158] and have since been further complexified.[159]

Another important facet of security protection is the recent *Digital Privacy Act* (also known as Bill S-4).[160] A key component of this law is the creation of mandatory data breach reporting obligations,[161] which became a concern for the public following the Yahoo[162] and eBay[163] data leak scandals. When an organization experiences a breach in security safeguards that affects personal information under its control, it now faces certain requirements.[164] For these to be triggered, the incident must create "a real risk of significant harm to an individual".[165] This risk must be evaluated with regard to the quality of the

[154] Ahmed Elnaggar, "Secure Socket Layer" (Student paper presented at 2nd Assignment of Communication Systems & Computer NW, University of Alexandria, Egypt, October 2015), online: < www.researchgate.net/publication/283297122_Secure_Socket_Layer > .

[155] Mario Barcena & Candid Wueest, "Insecurity in the Internet of Things" (Symatntec: 2015) at 5, online: < www.symantec.com/content/dam/symantec/docs/security-center/white-papers/insecurity-in-the-internet-of-things-15-en.pdf > .

[156] Andrew Hilts et al, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security" (Open Effect: 2016) at 25, online: < openeffect.ca/reports/Every_Step_You_Fake.pdf > .

[157] Steve Ragan, "Here are the 61 Passwords that Powered the Mirai IoT Botnet" *CSO* (3 October 2016), online: < www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html > .

[158] Antonakakis, *supra* note 153 at 1.

[159] For a complete portrait of the evolution of these attacks: Constantinos Kolias et al, "DDoS in the IoT: Mirai and Other Botnets" (2017) 50:7 Computer 80.

[160] Bill S-4, *Digital Privacy Act*, S.C. 2015, c. 32, amending *PIPEDA*, *supra* note 33 ["*DPA*"].

[161] Adrienne Blanchard, *Blanchard Life Sciences in Canada*, 2nd ed (Toronto: Carswell, 2006) at ch. 16.

[162] Robert McMillan & Ryan Knutson, "Yahoo Triples Estimate of Breached Accounts to 3 Billion," *The Washington Post* (3 October 2017), online: < www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804 > .

[163] Gordon Kelly, "eBay Suffers Massive Security Breach," *Forbes* (21 May 2014), online: < www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#ace2f5f74920 > .

[164] Blanchard, *supra* note 161 at ch. 16.

information involved and whether "it is reasonable under the circumstances to believe"[166] it will be misused.[167] A real risk implies a risk which is never theoretical nor abstract.[168] When an organization determines that a real risk of significant harm exists, it must notify the affected individuals, as well as the Privacy Commissioner, "as soon as feasibly possible".[169]

An issue with the formulation of this component of the act is the lack of reporting with regard to small breaches which may pose no reasonable risk of harm to a single individual, but expose a more universal flaw with the system at hand.[170] This criticism is particularly relevant with regard to connected devices, which are more likely to contain inherent flaws and zero-day vulnerabilities. This could, in turn, lead to the systemic exploitation of flaws that did not meet the test, and thus were not initially reported.

In Quebec, the Act has no mandatory reporting obligations.[171] The CAI merely provides resources when breaches occur, as well as a voluntary reporting system.[172] Among its recommendations, there is a six-part checklist to deal with breaches, which essentially mirrors the obligations of Bill S-4.[173] The CAI identified the lack of legal reporting or notification obligations, beyond the general rules of civil responsibility,[174] as an issue that the government should address.[175] For now, consumers are at risk of being kept in the dark when their connected devices, and the data they contain, are breached. With the plethora of risks associated with stolen information,[176] this is a glaring wart on Quebec's privacy protection regime.

Another problem has emerged with regard to safeguards, in the form of third-party access and use of information. In a 2009 report by the Privacy

[165] *DPA*, *supra* note 160 at s. 10.1(1).

[166] *Ibid.*

[167] *Ibid*; Blanchard, *supra* note 161 at ch. 16.

[168] Chloé de Lorimier, "Revue des nouvelles obligations de la Loi sur la protection des renseignements personnels numériques" *La référence* (Octobre 2016), EY-B2016REP2055 at 8.

[169] *DPA*, *supra* note 160 at s. 10.1(2).

[170] Canadian Bar Association, "Bill S-4 — *Digital Privacy Act*" (2014) at 14, online: < www.cba.org/CMSPages/GetFile.aspx?guid = ab9dfd4e-a2a0-48fe-83e0-92900459e68e > ["CBA"].

[171] Antoine Aylwin, "L'obligation de notification en cas de violation de la confidentialité pour une entreprise du secteur privé" (2015) 74 Revue du Barreau 465 at 450.

[172] *Ibid.*

[173] Commission d'accès à l'information du Québec, "Aide-mémoire a l'intention des organismes et des entreprises : quoi faire en cas de perte ou de vol de renseignements personnels?" (2009), online: < www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_org-ent.pdf > .

[174] *CCQ*, *supra* note 40 at art. 1457.

[175] Aylwin, *supra* note 171 at 6.

[176] Kende, *supra* note 15 at 26.

Commissioner on Facebook,[177] it was emphasized that contractual safeguards were not sufficient when dealing with information held by third party developers.[178] Concrete technological solutions should be used to prevent them from gaining "unauthorized access to personal information that they do not need".[179]

A last issue exists with regard to tampering. Several wearable connected devices contain sensitive data that has been used in court cases,[180] or could be one day used for insurance premiums.[181] This implies that the data was securely obtained and recorded, yet many of these devices do not contain any protection against user tampering.[182] A team of researchers had a test subject using a popular wearable connected device send data to the company stating that they had taken 10 billion steps in a single day.[183]

This further demonstrates that the list of chinks in the armour of connected objects is seemingly never-ending. The compliance issues between connected objects and this principle will only grow as they become omnipresent in our lives. This potential clash is fundamental to the debate concerning connected objects, since they can reveal people's most intimate "lifestyles, habits and choices".[184]

Exactitude

This principle has two components. One requires that users have access to their information, and the other requires that this information be accurate. Firstly, it requires that organizations present the information regarding their privacy policies in a format users can access and understand.[185] The same principle exists in the *Code civil du Québec*.[186] The information should include the people responsible for privacy within the organization, which information is captured, how it is used, and how it is shared.[187] A recent assessment of online privacy policies has found a significant percentage of organizations to lack either a privacy policy, privacy contact, or explanations as to the use, collection and disclosure of information and the company's compliance with applicable privacy laws.[188]

[177] Denham, *supra* note 134.

[178] Denham, *supra* note 134 at para. 200.

[179] *Ibid.*

[180] Hilts, *supra* note 156 at 36.

[181] *Ibid.*

[182] *Ibid.*

[183] *Ibid* at 33.

[184] Andy Crabtree et al, "Building Accountability into the Internet of Things: The IoT Databox Model" (2018) 4:1 J Reliable Intelligent Environments 39 at 42.

[185] OPC re Bell Canada, *supra* note 65 at para. 57-60.

[186] *CCQ*, *supra* note 40 at arts. 38-39.

[187] Power, *supra* note 51 at s. 4.1.7.8.

[188] Office of the Privacy Commissioner of Canada, "Results of the 2013 Global Privacy

With regard to connected objects, the same problems are present. For instance, a few organizations with wearable connected objects did not have an available privacy policy.[189] Among those that did, a few had several different privacy policies depending on the app used with the connected device, leaving users in a fog as to the applicable policy.[190] Many of them referenced other legal documents with different guidelines.[191] All of them lacked clear explanations of key areas of privacy, such as the applicable law, how long the data was retained, security, the circumstances in which it could be shared to a third party, as well as access and correction practices.[192]

This principle also requires organizations to inform people, upon request, as to whether they hold any personal information.[193] If there is personal information, they must also give access to this information.[194] Technical difficulties in obtaining this data or the relevance of the information are not acceptable reasons to refuse a request.[195] The individual's demand to obtain their personal information must be made in writing according to *PIPEDA*.[196] If the individual feels that not all the information was revealed or found, they must "establish at least a *prima facie* case that the search was inadequate".[197] The data must be given at little or no cost and must be generally understandable.[198] In Quebec, this same principle of access applies.[199] Although free access to the information must be given, a reasonable cost can be required for its reproduction.[200] An organization may refuse to share information if it falls under certain exceptions,[201] and the dispositions of the *Code civil du Québec*

Enforcement Network Internet Privacy Sweep: Backgrounder" (13 August 2013), online: < www.priv.gc.ca/en/opc-news/news-and-announcements/2013/bg_130813/ > .

[189] Hilts, *supra* note 156 at 41-42.

[190] *Ibid.*

[191] *Ibid* at 42.

[192] *Ibid* at 43-48.

[193] Office of the Privacy Commissioner of Canada, *Bank Accused of Withholding Audit Trail Information*, *PIPEDA* Case Summary #2002-74 (9 October 2002), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/*PIPEDA*-2002-074/ > .

[194] *Ibid.*

[195] *Ibid.*

[196] *PIPEDA*, *supra* note 33 at s. 8.1*PIPEDA*.

[197] *Johnson v. Bell Canada*, 2008 FC 1086, 2008 CarswellNat 3546, 2008 CarswellNat 4659, [2008] F.C.J. No. 1368 (F.C. T.D.) at para. 43.

[198] *PIPEDA*, *supra* note 33 at sched. 1, s. 4.9.4.

[199] *CCQ*, *supra* note 40 at arts. 38-39.

[200] *Ibid.*

[201] QC *Private Sector Privacy Act*, *supra* note 34 at s. 37-41; *Monette c. Westbury Canadienne, cie d'assurance-vie*, 1999 CarswellQue 1250, [1999] C.A.I. 550 (C.S. Que.) at para 11.

cannot be used to circumvent these restrictions.[202] These restrictions are specified in the Act,[203] but they stem from the larger definition of Article 39 *CCQ*,[204] which allows for a refusal based on serious and legitimate reasons, or when the information may cause serious harm to another person.[205]

Recent studies by the Citizen Lab have highlighted the laborious and often inadequate efforts by organizations with connected objects to comply with this principle.[206] In all cases, the connected objects were health wearables that had the capacity to collect massive amounts of data, as they were with the user at almost all times. Only a few companies had explicit policies regarding access to data for the individual.[207] Requests were made to each company for the data collected to be shared in a readable format.[208] Almost half did not respond to the request at all.[209] Even among those that did respond, most did not provide for all of the individual's collected information in a readable format.[210] This further demonstrates the difficulties a user will face when trying to obtain this data, and the lack of compliance with this principle by organizations with connected devices.

The second component of this principle, accuracy, prohibits personal information from being routinely updated. These are only allowed if the purposes of the data gathering require it.[211] The degree of accuracy required by this principle will differ depending on the importance of accuracy when using the information.[212] A credit reporting agency, whose sole purpose is to provide a base of information for decisions by credit guarantors, will thus have a high threshold of accuracy.[213] The commercial and practical necessities of a certain system for an organization do not provide a defense from this principle.[214] Managing a large amount of data cannot exempt an organization from being accurate.[215] The vast amounts of information obtained from connected objects, and the profiles of individuals created from this data, could breach this principle

[202] *Monette*, *supra* at para. 11.

[203] QC *Private Sector Privacy Act*, *supra* note 34 at s. 37-41.

[204] *CCQ*, *supra* note 40 at art. 39; Power, *supra* note 51 at s. 4.5.10.

[205] *Ibid.*

[206] Christopher Parsons et al, "Approaching Access" (2018) Citizen Lab Research Brief No. 106, online: <citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf>.

[207] *Ibid* at 48.

[208] *Ibid.*

[209] *Ibid* at 29.

[210] Hilts, *supra* note 156 at 48; Parsons, *supra* note 206 at 29.

[211] *PIPEDA*, *supra* note 33 at sched. 1 s. 4.6.2.

[212] *Nammo v. TransUnion of Canada Inc.*, 2010 FC 1284, [2010] F.C.J. No. 1510 (F.C. T.D.) at para. 40.

[213] *Ibid.*

[214] *Ibid* at paras. 37-39.

[215] *Ibid.*

if an inaccurate profile was created, even if the quantity in question made accuracy far more difficult.

Provincially, Article 37 of the *Code Civil du Québec* ensures that when enterprises make a decision based on information they have collected, it must be accurate and up to date.[216] A negative mention on a credit dossier based on inaccurate information can violate Article 37.[217] This could apply in the case of decisions based on insurance files built from wearable connected objects which had recorded inaccurate information.

Accountability

Accountability is a blanket concept which applies to all the others. It is the "acceptance of responsibility for personal information protection".[218] This acceptance is expressed in *PIPEDA* in the form of a designated individual who is responsible for the company's compliance with these principles, even if others are affected to data collection or management.[219] This person is often referred to as a privacy officer.[220] Although this specific individual, or group of individuals, is responsible for data protection within the company, this does not discharge the company's obligation onto these people; rather, it makes the "organization responsible and accountable as a whole".[221] When a complaint is addressed to an organization by a third party, it must provide the client with the relevant contact information of the privacy officer,[222] even if another employee can answer the question or solve the issue.[223]

Another aspect of accountability is responsibility after transfer to a third party.[224] This forces the organization, when transferring the data to a third party, to ensure that comparable measures of protection are in place.[225] A certain

[216] QC *Private Sector Privacy Act*, *supra* note 34 at s. 11; *Nadler c. Rogers Communications inc.*, 2014 QCCQ 5609 at paras. 53-56, [2014] J.Q. no 6384 (C.Q.) ["*Nadler*"].

[217] *CCQ*, *supra* note 40 at art. 37; *Nadler*, *supra* at paras. 53-56.

[218] Office of the Privacy Commissioner of Canada et al, "Getting Accountability Right with a Privacy Management Program" (2012) at 1, online: < www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf > ["OPC on Privacy Management"].

[219] Power, *supra* note 51 at s. 4.1.7.

[220] OPC on Privacy Management, *supra* note 218 at 7.

[221] Office of the Privacy Commissioner of Canada, *Man Objects on Pprinciple to Bank's Identification Program*, *PIPEDA* Case Summary #2001-27 (4 December 2001), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/*PIPEDA*-2001-027/ >.

[222] *PIPEDA*, *supra* note 33 at sched. 1 s. 4.1.2. *PIPEDA*

[223] *Web-centred Company's Safeguards and Handling of Access Request and Privacy Complaint Questioned*, *PIPEDA* Case Summary #2005-315 (9 August 2005), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/*PIPEDA*-2005-315/ >.

[224] *PIPEDA*, *supra* note 33 at sched. 1 s. 4.1.3. *PIPEDA*

[225] *Ibid.*

amount of control by the organization is required when using a subcontractor or a service provider.[226] A 2012 report by the Privacy Commissioners of Alberta and Canada stated that, at the very least, service providers should be contractually bound to comply with the organization's privacy provisions.[227]

The issue of accountability faces multiple shortcomings. Even if we were to assume that companies had effective privacy policies with privacy officers in place, people would be hard pressed to know where to turn. Connected objects are constantly communicating, and several complimentary actors are involved in the data retention and collection.[228] The data is often processed through "an unobtrusive and seamless infrastructure in which connected devices typically lack user interfaces and the communication of data is invisible".[229] Thus, it is more complicated to hold any single actor responsible. Mapping data flows will be primordial in assessing responsibilities[230] and, in turn, complying to this principle.

CONCLUSION

The Canadian privacy framework is woefully ill-equipped to face the rise in connected objects. Resources must be dedicated to rethinking what we view as adequate consent, how our data is collected and why, how this data is protected, how it portrays us and what to do if the shoe does not fit, and how we will make organizations accountable for these issues in a globalized world.

While Canada is lagging behind in terms of legislation addressing concerns regarding IoT and connected objects, the United States of America has recently awoken to the explosion of the IoT devices. The Federal Trade Commission (FTC) has a wide mandate to protect consumers in the US.[231] For the past decade, it has used its broad s. 5 powers regarding "unfair or deceptive acts or practices"[232] to police organizations with insufficient data security.[233] Recognizing the potential dangers of connected objects, it organized a workshop in early 2013 to discuss the issues that arose from this new IoT wave. In January 2015, the FTC published a report in collaboration with leading

[226] Power, *supra* note 51 at s. 4.1.7.1.

[227] OPC on Privacy Management, *supra* note 218 at 15.

[228] OPCC on IoT, *supra* note 76.

[229] Crabtree, *supra* note 184 at 42.

[230] OPCC on IoT, *supra* note 76.

[231] Federal Trade Commission, *Federal Trade Commission Strategic Plan for Fiscal Years 2018 to 2022* (February 2018), online: < www.ftc.gov/system/files/documents/reports/2018-2022-strategic-plan/ftc_fy18-22_strategic_plan.pdf > .

[232] *Federal Trade Commission Act*, 15 U.S.C.A. § 45 (2006), s. 5(a).

[233] Ryan Bergsieker et al, "The Federal Trade Commission's Enforcement of Data Security Standards" (2015) 44:6 The Colorado Lawyer 39 at 40, online: < www.gibsondunn.com/wp-content/uploads/documents/publications/Bergsieker-Cunningham-Young-FTC-Data-Security-Enforcement-06.2015.pdf > .

technologists and academics, industry representatives, and consumer advocates.[234] The report described the axis upon which the FTC would develop its policy on connected devices, with an emphasis on the need for greater layered security, employee awareness, as well as a series of industry specific self-regulatory programs.[235] The participants also highlighted "the need for substantive data security and breach notification legislation at the federal level".[236]

Following the workshop in 2013, the FTC adopted a more aggressive strategy towards smart object makers. Using its s. 5 powers,[237] It charged TRENDnet,[238] ASUSTek Computing[239] and D-Link[240] with failing to provide adequate protection for their products. The FTC's approach with regard to security issues has thus experienced some success. This particular component could serve as a model for Canada, at a time when its current privacy legislation is toothless in comparison.

The FTC has more generally encouraged organizations to adopt a voluntary data minimization, notice and consent policy.[241] Companies would self-regulate to minimize the amount of consumer data collected.[242] This would occur through a diminishment of the data collected, or through the collection of less sensitive information, as well as de-identification procedures.[243] This approach seems severely flawed, especially with regard to connected objects. There are doubts as to whether de-identification is even possible,[244] and there are no compliance mechanisms to keep in check companies who collect data. While the FTC has successfully used its power to regulate the *security* aspect of privacy and data collection, it has been powerless to impose a clear form of consent and limitations as to the size and quality of the data collected. A caveat to the American approach is the disparity of regulations between the state and federal levels, leaving a patchwork of regulations which can be hard for citizens to navigate.[245]

[234] Federal Trade Commission, "Internet of Things: Privacy & Security in a Connected World" (2015), online: < www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf > .

[235] *Ibid.*

[236] Ibid.

[237] Branden Ly, "Never Home Alone: Data Privacy Regulations for the Internet of Things" (2017) 2017:2 U Illinois J L Tech & Pol'y 539 at 553.

[238] *TRENDnet*, *supra* note 18.

[239] *ASUSTeK*, *supra* note 21.

[240] *D-Link*, *supra* note 14.

[241] Ly, *supra* note 237 at 553.

[242] *Ibid* at 554.

[243] *Ibid.*

[244] Yves-Alexandre de Montjoye et al, "Unique in the Crowd: The Privacy Bounds of Human Mobility" (2013) 3 Scientific Reports 1376 at 1379.

Through this thistle of inconsistent privacy legislation,[246] California has been a pioneer in data protection and reporting obligations.[247] The California Civil Code requires organizations that collect data to use “reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction use, modification, or disclosure”.[248] Since 2003, there have been notification obligations when data breaches of specific personal information occur.[249] Diverging from the Canadian rules, these obligations are triggered by the reasonable belief that this information has been obtained by an unauthorized person.[250] Other states have used the “harm” standard present in *PIPEDA*.[251]

Recently, in an effort to modernize its privacy framework, California has enacted the *California Consumer Privacy Act of 2018*.[252] The definition of personal information was broadened to “identifiable information,” mirroring the Canadian approach.[253] One component of this change should be closely examined by Canadian authorities wishing to update current privacy legislature to face the rising tide of connected objects. A liability rule for data breaches was created.[254] Businesses can now be held privately liable if they inadequately secure their data, without consumers having to prove that any harm could or did occur.[255] The Attorney General has the ability to pursue these businesses.[256] Canada should also implement a form of liability, in the wake of recent data breaches due to outdated protocols, to motivate organizations to invest in their security and, by correlation, that of their customers.

[245] CBA, *supra* note 170 at 14.

[246] For a list of all privacy breach related laws in the US see National Conference of State Legislatures, *Security Breach Notification Laws* (29 September 2018), online: < www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx > .

[247] Aylwin, *supra* note 171 note at 6.

[248] *California Civil Code* § 1798.81.5; Kamala Harris, “California Data Breach Report 2012-2015” (2016) at 28, online: < oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf > .

[249] Harris, *supra* at 2.

[250] *Ibid.*

[251] *Ibid* at 4.

[252] Sullivan & Cromwell LLP, “California Consumer Privacy Act of 2018: New Statute Introduces Privacy Protections for California Consumers and Subjects Businesses to Potential Liability” *Sullivan & Cromwell LLP* (blog) (2 July 2018), online: < www.sullcrom.com/files/upload/SC-Publication-New-Statute-Introduces-Privacy-Protections-for-California-Consumers-and-Subjects-Businesses-to-Potential-Liability.pdf > .

[253] *Ibid* at 2.

[254] *Ibid* at 6; *California Privacy Act* § 1798.150(a)(1).

[255] Sullivan & Cromwell, *supra* note 252 at 6.

[256] *Ibid*; *California Civil Code* § 1798.155(a)—(b).

Dawn is breaking over a new era of social connectivity. The omnipresence of connected objects will bring about a true IoT. This change will redefine how we interact with others and the things we own. Such a paradigm shift will come at a price — beleaguering intimacy into linguistic cemeteries. Definitions of privacy and security, as well as the law, will have to evolve in order to stay economically reasonable and relevant. Technology is always faster than the government at adapting to the demands of today's world. Modern organizations have very little incentive to protect the everyday person from the multitude of security threats. At the current breakneck speed of innovation, how will our leaders address the issues that will redefine the next generation's relationship with its data?