The Internet of Things:
Implications for Consumer Privacy under Canadian Law

by Samuel E Trosow, Lindsay Taylor and Alexandrina Hanam*

Table of Contents

* Samuel Trosow <strosow@uwo.ca> is an Associate Professor at the University of Western Ontario holding a joint appointment in the Faculty of Law and Faculty of Information & Media Studies (FIMS). He is the principal and corresponding author for this study. Lindsay Taylor and Alexandrina Hanam (2017 FIMS-M.L.I.S graduates) assisted with the research and writing of this study.

Daniel Weiss (2018 UWO JD candidate) and Scott Tremblay (2017 UWO JD) also assisted with the research for this study and are co-authors of the companion *Submission to the Office of the Privacy Commissioner of Canada Consultation on Consent and Privacy*.

This project was supported by a grant from the Foundation for Legal Research with additional support from the Faculty of Law at UWO.

Abstract:

Much recent attention has focused on the development of what is coming to be known as the Internet of Things (IoT). New digital products and services ranging from "smart" kitchen appliances, home heating/lighting/security systems and children's' toys to "wearable" personal health devices are promising to bring the benefits of real time network connectivity to a range of everyday activities. In providing consumers with devices that can communicate directly with each other, end-users are promised the benefits of efficient information data collection which can result in lower energy costs, improved health monitoring, enhanced safety and a variety of other claimed benefits.

At the same time, the ability of advanced information systems to collect, store, evaluate, transmit and reuse vast amounts of data linked to the personal activities of individuals has very serious implications for security and privacy. As the range of connected consumer products expands to include more aspects of daily life, the tension between the practical social and economic benefits of the IoT with the security and privacy related risks and problems continues to widen. And as the amount of personal information that is being collected, stored and re-used continues to grow, new questions are arising about the continued adequacy of our current laws that are intended to protect the privacy, integrity and security of personal information.

In addition to the growing threat of unauthorized intruders breaking into data systems, the ability of the legitimate custodians of that data to reuse and share personal information has serious implications for personal privacy. The types of information gathered by the emerging Internet of Things are potentially very valuable from a marketing perspective, especially with the growing ability to link and analyze vast stores of data.

This paper examines these developments through the lens of Canadian privacy law, and asks how well emerging Internet of Things fits with these laws and their underlying policies. The statutory framework for Canadian privacy laws pre-date the emergence of the Internet of Things and many settled principles are no longer well equipped to deal effectively with the quick pace of technological change. So it is important to ask not only whether current IoT practices comply with the law as it now stands, but also what changes are needed in order to better reflect the purposes and policy goals underlying PIPEDA in light of technological developments.

In order to make this assessment, the general literature on privacy and its Canadian legal framework was reviewed as were specific terms in the privacy policies and terms of service agreements that consumers are given

Our general conclusion is that Canadian privacy law is not keeping pace with the rapid changes accompanying the spread of the network technologies and the Internet of Things. Significant policy changes are therefore needed to adequately protect the privacy and security interests of Canadian consumers.

I. Introduction

Much recent attention has focused on the development of what is coming to be known as the Internet of Things (IoT). New digital products and services ranging from "smart" kitchen appliances, home heating/lighting/security systems and children's toys to "wearable" personal health devices are promising to bring the benefits of real time network connectivity to a range of everyday activities. The Pew Research Center attributes the rise of the IoT to an "urge to create connectivity, [which] extends to such prosaic items as toothbrushes, dental floss, hairbrushes, pillows, egg trays, wine bottle sleeves, baby monitors and changing tables, silverware, umbrellas, all manner of toys and sporting goods and remote-controlled pet food dispensers, to name a few."[1] In providing consumers with devices that can communicate directly with each other, end-users are promised the benefits of efficient data collection which can result in lower energy costs, improved health monitoring, enhanced safety and a variety of other claimed benefits.[2]

At the same time, the ability of advanced information systems to collect, store, evaluate, transmit and reuse vast amounts of data linked to the personal activities of individuals has profound implications for security and privacy. As the range of connected consumer products expands to include more and more aspects of daily life, the tension between the practical benefits of the IoT with the security and privacy related risks and problems it contributes to widen. And as the amount of personal information that is being collected, stored, processed, analyzed and re-used continues to grow, new questions arise about whether our current laws intended to protect the privacy, integrity and security of personal information are robust enough to meet these new challenges.

---

[1] Pew Research Center, *The Internet of Things Connectivity Binge: What are the Implications*? (June 2017), online: <http://www.pewinternet.org/2017/06/06/theinternet-of-things-connectivity-binge-what-are-theimplications/> [***Pew Connectivity Report***].

[2] While there are also significant implications of the emerging IoT for businesses, government agencies and other institutions, this report will focus on consumer applications.

In addition to the growing threat of unauthorized intruders breaking into data systems, the ability of the legitimate custodians of that data to reuse and share personal information has serious implications for personal privacy. The vast quantity of data gathered through the Internet of Things is potentially very valuable from a marketing perspective, especially with the growing ability to combine and analyze these massive stores of data.

This study will examine these developments through the lens of Canadian privacy law, and ask how well the emerging Internet of Things fits with these laws and their underlying policies. Since the statutory framework for Canadian privacy laws pre-dates the emergence of the Internet of Things, it should not be surprising that many settled principles are not well equipped to effectively account for the quick pace of technological change. While Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA)[3] was enacted in 2000, many of its underlying principles are derived from earlier measures.

The Office of the Privacy Commissioner (OPC) stated that "technological developments in the context of the Internet of Things has not been matched by an equivalent evolution of overarching privacy governance models."[4] The OPC further asserts that "[b]efore we too readily endorse smart devices and sensors that can send into the cloud information about many personal aspects of our daily lives, it is essential to have an informed discussion about the implications of

[3] *The Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 [***PIPEDA***]. The substantive requirements of PIPEDA are set forth in its Schedule 1, attached as Appendix A.

[4] 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* (Research paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada, 2016) at 23. Online: <https://www.priv.gc.ca/media/1808/iot_201602_e.pdf >. [***OPC, IoT Introduction***]

the Internet of Things and to plan the integration of privacy principles and safeguards into the conception and implementation of the many smart environment components."[5]

So it is important to ask not only whether current IoT practices comply with the law as it now stands, but also what changes are needed in order to better reflect the purposes and policy goals underlying PIPEDA in light of technological developments. In order to make this assessment, this research project reviews the general literature on privacy, its Canadian legal framework, and will also examine specific terms in the privacy policies and terms of service agreements that consumers are given and to which they must consent to in order to use various Internet of Things devices.

Part II will consider the concept of privacy in general, tracing its development as a legal concept and noting the historical importance of technological changes on its understanding. This part will then consider various definitions of IoT and assess the growth of the industry it has spawned. Part III will look at the growing vulnerability of the IoT to data breaches and external attacks as well as the problems associated with different security protocols.

Part IV will consider key PIPEDA principles in greater detail including the initial characterization of data as "personally identifiable," whether this data is considered "sensitive" and the meaning of consent to the collection of data and the scope of its subsequent use and

[5] *Ibid* at 16. See also Jules Polentsky, "Protecting privacy and promoting inclusion with the 'Internet of Things'" (June 29, 2016), online: <http://thehill.com/blogs/pundits-blog/technology/285962-protecting-privacy-and-promoting-inclusion-with-the-internet-of>. (arguing that regulators "must encourage strategies that benefit everyone, while at the same time apply common sense privacy protections that build trust in IoT technologies to help ensure that consumers enjoy the full benefits of IoT sensors and devices."

processing.[6]

In order to assess how these principles are being applied to the consumer IoT market in practice, Part V will examine provisions from the Privacy Policies and Terms of Service (ToS) agreements from various IoT vendors and services. While there are differences between the approaches taken by different vendors, there is a noticeable disconnect between many of these provisions with the objectives of Canada's regulatory regime. These contractual terms need to be easier to understand and standardized. But they also need to be brought into a closer alignment with Canada's privacy policies. Our general conclusion is that Canadian privacy regulations are not keeping pace with the rapid changes accompanying the spread of network technologies generally and Internet of Things more specifically. As a result, significant policy changes are needed to adequately protect the privacy and security interests of Canadian consumers and these are outlined in Part VI.

---

[6] See Office of the Privacy Commissioner of Canada. *Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act 2016* (Prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada, 2016), online: <https://www.priv.gc.ca/media/1806/consent_201605_e.pdf>>[***OPC, Consent and Privacy***]; Samuel E. Trosow, Scott Tremblay & Daniel Weiss, "Submission to the Office of the Privacy Commissioner of Canada: Consultation on Consent and Privacy" (August 2016) online: https://samtrosow.files.wordpress.com/2016/08/consent-submission-to-the-opc.pdf [**Trosow, OPC Submission**].

II. Privacy and the Internet of Things

A. What is Privacy?

Thomas Cooley's definition of privacy as "the right to be left alone,"[7] as elaborated by Samuel Warren and Louis Brandeis' seminal 1890 article in the *Harvard Law Review*[8] is generally taken as the starting point of modern privacy doctrine. Due to the expansive nature of the concept of privacy, later writers have had difficulty fashioning a more precise definition.

In an extensive comparative analysis of data protection in the United States and Europe, Colin Bennett notes that "privacy" is a vague and ambiguous term which embraces various rights, tensions, problems and duties.[9] While noting the difficulty in constructing an exhaustive list of privacy interests, Bennett includes (1) the right to be free from intrusive police searches and wiretapping; (2) the right to be free from intrusive journalists and photographers; (3) the right to make private decisions in relation to intimate family concerns (including contraception, abortion); and (4) the right to have some control over the collection, storage and disclosure of personal information by other institutions.

Other authors have attempted similar classification schemes and definitions. Alan Westin classifies "privacy" into four states: solitude, intimacy, anonymity and reserve[10]. In the state of solitude, the individual is separated from the group and freed from observations by others. Intimacy involves the individual acting as a part of a small unit which claims to exercise seclusion so a close, relaxed and frank relationship may be achieved between two or more individuals.

---

[7] Thomas M. Cooley, A *Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contracts*. 2d ed (Chicago: Callaghan & Co., 1888).

[8] Samuel D. Warren & Louis D. Brandeis. "The Right to Privacy" (1890) *Harvard Law Review 4*(5): 193-220.

[9] Colin J. Bennett. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca, NY: Cornell University Press, 1992)

[10] Alan F. Westin, *Privacy and Freedom.* (New York: Athenium, 1967) at 31-32.

Anonymity occurs when the individual is in a public place or performing public acts but is still free from surveillance and identification. Knowledge that one is under observation destroys the sense of freedom and relaxation is sought in many public spaces. The most subtle state, reserve, involves the creation of a psychological barrier against unwanted intrusions.

In 1989 David Flaherty identified thirteen privacy interests which include the right to individual autonomy; the right to be left alone; the right to a private life; the right to control information about oneself; the right to limit accessibility; the right to exclusive control of access to private realms; the right to minimize intrusiveness; the right to expect confidentiality; the right to enjoy solitude; the right to enjoy intimacy;: the right to enjoy anonymity; the right to enjoy reserve; and the right to secrecy.[11]

These classification schemes can be distilled into three general types of interests. The first is the right **to be free from** intrusive police searches, wiretapping and intrusive journalists and photographers. The second is the right **to be free to** make private decisions in relation to intimate family concerns including contraception and abortion; and the third is the right **to have control over** the collection, storage and disclosure of personal information about oneself by government, corporations and other institutions. This third interest is captured by Westin's definition of information privacy as: "…the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others." [12] Colin Bennett argues that a more accurate term for the group of policies concerned with the latter is the European nomenclature: Data Protection (*datenschutz*). He notes that while English speaking use the word "privacy" for its popular appeal, "data protection" is a more

[11] David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989) at 8.
[12] Westin, *supra* note 10 at 31-32.

precise terminology and it helps distinguish the more specific contemporary policy problem from the traditional and general social values associated with privacy more broadly.[13] While all three of these interests are implicated in the expansion of the Internet of Things to some degree, the third is the most prominent and will be the focus this report.

Advances in technology have historically been closely related to the development of privacy policies. The policy challenges being raised by the Internet of Things are simply the latest in a long line of technological developments that challenge conceptions of privacy and how it is treated as a legal concept.

In their 1890 article, Warren and Brandeis established technology as a strong and consistent privacy theme. They were concerned about advances in photography that allowed a picture to be taken surreptitiously, without a formal sitting. The interest in privacy was revived in 1960's when computers began to take a prominent place in public awareness.

In 1967 Alan Westin identified the "reproducibility of communication" as a new type of surveillance enabled by advances in technology through which information surreptitiously obtained may be reproduced at will. As recording devices become more prevalent, Westin predicted their use will spread from law enforcement agencies into the general government, business and personal worlds. [14] Similarly in 1971, Arthur Miller recognized a strong relationship between bureaucracy, information technology and the collection of personal data. He predicted that technological improvements in information-handling capabilities would be followed by a tendency to engage in a more extensive manipulation and analysis of data which would motivate the collection of more data disclosing more variables and which will ultimately result in the

[13] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithica, NY: Cornell University Press, 1992) at 13.

[14] Westin, *supra* note 10 at 62.

extraction of more personal information from people. [15] The proposal of a computerized federal data center in the U.S. in the mid 1960's sparked a series of Congressional Hearings looking at different aspects of privacy and ultimately resulted in the enactment of Privacy Act of 1974.[16]

The theme of technology was also emphasized by Oscar Gandy in his critique of what he termed the "*panoptic sort*." "Panoptic" refers to an all-seeing technology which involves the collection, processing and sharing of information about people and groups, and "Sort" refers to the segmentation and categorization of subjects based on their worth to the market, a practice Gandy sees as inherently discriminatory.[17] For Gandy, this panopticon was not limited to prisons, as originally envisioned by Jeremy Bentham, but can be extended to the operation of the modern economy where the panoptic sort is used to both coordinate the creation and direction of consumer demand and control access to the distribution of goods and services. Gandy views the panoptic sort as an anti-democratic system of control and he does not believe that data protection regulation might keep it under control.

David Lyon also presents a sociological analysis of the "surveillance society," characterized as the pervasive gathering of personal information.[18] Earlier, Jacques Ellul warned that the relentless pursuit of *la technique* confines man "to the role of a recording device; he will note the effects of techniques upon one another, and register the results" [19] Westin, Miller, Gandy, Lyon and Ellul were all prescient in their ability to anticipate technological advances and their troubling implications for privacy. These and other similar works are important to recognize as

---

[15] Arthur Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press, 1971) at 21.

[16] Pub.L 93-579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C.sec 522a. (which applies to the collection maintenance use and disclosure of personal information by federal agencies).

[17] Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993).

[18] David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis: University of Minneapolis Press, 1994).

[19] Jacques Ellul, *Technological Society* (trans. by John Wilkinson) (NY: Vintage Books, 1964) at 9.

they help us ground these recent technological and market developments in a solid historical framework.

B. General Development of Canada's Privacy Regime

Canada's current privacy framework is derived from the Guidelines published by the Organization for Economic Cooperation and Development (OECD) in 1980 which set out eight fundamental principles. These eight principles, which have since been incorporated into PIPEDA, concern collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. The OECD Guidelines were voluntary, they were not binding, and there was no enforcement mechanism.

In Canada, a similar model based on self-regulation was adopted by the Canadian Standards Association in 1995.[20] It adopted the eight OECD principles and added two others relating to consent and challenges. The growing tension between the self-regulatory approach and a more robust set of binding legislative mandates gave rise to both the adoption of the EU Data Protection Directive[21] in 1995 as well as the enactment of PIPEDA in 2000 which incorporated the ten CSA standards. The EU Data Protection Directive contained adequacy requirements for non-member countries and the European Commission has ruled that Canada's PIPEDA satisfied these requirements.[22]

The purpose of PIPEDA , stated in section 3 "…is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of

[20] Canadian Standards Association (1995) The model was also approved by the Standards Council in 1996.
[21] EU Data Protection Directive 95/46/EC.
[22] More recently the Directive has been replaced by the EU General Data Protection Regulation (GDPR) which was approved in April 2016 and will become enforceable in May 2018. See <http://www.eugdpr.org>. It is not yet clear how the adequacy of non-member privacy regimes will be assessed, so the previous finding of PIPEDA's adequacy cannot be taken as permanent.

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."[23] The need for balancing different interests is thereby incorporated into the basic framework of the Act, and it is reasonable to recalibrate this balance as needed.

Subject to certain exceptions, PIPEDA applies to "every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of commercial activities."[24] So the crucial threshold question underlying PIPEDA analysis turns on what is considered to be "personal information."[25] Further details about this issue and other specific PIPEDA provisions and requirements will be elaborated in Part V.

C. Overview of the Internet of Things and the IoT Industry

In general, the 'Internet of Things' is the networking of physical objects connecting through the Internet.[26] There is a proliferation of definitions for the Internet of Things.[27] Ernst & Young define it as "a future-facing development of the internet wherein objects and systems are embedded with sensors and computing power, with the intention of being able to communicate

[23] PIPEDA, section 3.

[24] PIPEDA Section 4(1)), but it does not apply to:
(a) any government institution to which the Privacy Act applies;
(b) *any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes* and does not collect, use or disclose for any other purpose; or
(c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose. (PIPEDA, Section 4(2)) These and other exceptions are not applicable to consumer Internet of Thing applications.

[25] Further details about this issue and other specific PIPEDA provisions and requirements will be elaborated in Part V

[26] OPC, *Internet of Things Introduction*, *supra* note 4 at 1.

[27] See Guido Noto La Diega, "Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom" (2016) 9 *Journal of Law and Economic Regulation* 69 (identifying over 60 different definitions of the term).

with each other"[28] It has been broadly defined as "a paradigm that considers pervasive presence in the environment of various things that through wireless and wired connections are able to interact and cooperate with other connected things to create seamless communication and contextual services, and reach common goals."[29]

Calum McClelland argues that most IoT definitions are overly-complex and he offers the following simplified account: "The Internet of Things is actually a pretty simple concept, *it means taking all the things in the world and connecting them to the internet*."[30] He adds that "… all the things that are being connected to the internet can be put into three categories: (1) Things that collect information and then send it; (2) things that receive information and then act on it; and (3) things that do both.[31]

More specifically, the Internet of Things refers to networks of physical devices integrated with apps, remote computing centers, and the broader internet, through various forms of wireless communication such as wifi, radio, or bluetooth. They often gather real-world data through sensors and transmit it, without human intervention, through these networks in order to provide a service to the user by acting on the data collected, often automatically. [32]

Andy Rhodes likens the Internet of Things to an octopus because "...every octopus has not one brain, not two, not three or even four, but nine brains total, one in each tentacle, along with a

---

[28] Ernst &Young, "Cybersecurity and the Internet of Things" (March 2015) at 2. Online: <http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf> [**Ernst & Young, Cybersecurity and the IoT**]

[29] Sridipta Misra, Muthucumaru Maheswaran, & Salman Hashmi, *Security Challenges and Approaches in Internet of Things* (Switzerland: Springer International Publishing, 2017) at 6. [**Misra, Security Challenges**]

[30] Calum McClelland, "What is IoT? A Simple Explanation of the Internet of Things" *IoT for all* (May 30, 2017), online: <https://iot-for-all.com/what-is-iot-simple-explanation/>

[31] *Ibid.*

[32] James Manyika, et al,"Disruptive technologies: Advances that will transform life, business, and the global economy" McKinsey Global Institute, (May 2013) at 52, online: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies>

central brain in the head. Suction cups act as sensors that feed "data" into the tentacles' brains, which are coordinated (to the best of researchers' knowledge) by the central brain in the octopus' head. That's a lot like a distributed-analytics architecture stretching from the edge to the fog to the cloud."[33]

Kayleen Manwaring prefers to use the term *eObjects*, which she defines as "an object that is not inherently computerised, but into which has been embedded one or more computer processors with data-collection, data-handling and data communication capabilities."[34]

The IoT industry is growing rapidly. According to global data including Canada, sales of sensors, a key component in IoT data collection, has grown annually by approximately 70% since 2010.[35] Ernst & Young estimates that "machine-to-machine (M2M) communications alone will generate approximately US$900 billion in revenues by 2020,"[36] and a recent report in the Globe and Mail notes the total value of the IoT market in Canada alone is projected to reach $21-billion

[33] Andy Rhodes, "IoT is evolving like an octopus" *Smart Industry* <https://www.smartindustry.com/blog/smart-industry-connect/iot-is-evolving-like-an-octopus/. Rhodes is the VP and general manager of IoT solution with Dell. See also Sean Kinney. "The internet of things is an octopus…" *Enterprise IoT Insights* (May 9, 2017), online: <http://enterpriseiotinsights.com/20170509/internet-of-things/20170509internet-of-thingsinternet-of-things-octopus-tag17> and Liu, Kuan-lin "'IoT is an octopus … and we are everything except the suckers': Dell VP" The *China Post* (June 1, 2017), online: <http://www.chinapost.com.tw/taiwan/business/2017/06/01/498157/iot-is.htm> .

[34] Kayleen Manwarring, "Emerging Information Technologies: Challenges for Consumers" *Oxford University Commonwealth Law Journal* (2017) Vol. 17 (Forthcoming) UNSW Law Research Paper No. 25 (p. 3). See also Kayleen Manwarring & Roger Clarke. 'Surfing the Third Wave of Computing: A Framework for Research into Networked eObjects' (2015) 31 *Computer Law & Security Review* 586.

[35] Office of the Privacy Commissioner, 2016, p.54 ??

[36] Ernst & Young, Cybersecurity and the IoT, *supra* note 28 at 6).

by 2018.[37] Projections of market growth for the IoT global market vary widely depending on the source, expected to be worth between $15 billion and $1.9 trillion by 2020.[38]

While several major companies (such as Apple, Amazon and Google) develop and market consumer products in the IoT market, there is a significant start-up culture within the indusrty as well, and some devices are being crowdfunded. It is therefore common for IoT devices to be "designed by less experienced product developers, many of whom are not focusing upon security considerations."[39] The current market is considered to be ill-equipped to deal with security issues; a recent study from Hewlett Packard "found that100 percent of the studied devices used in home security contain significant vulnerabilities, including password security, encryption and authentication issues.[40]

It is reasonable to expect that given the rapid growth within the industry, more novice business will expand into the IoT market. In a 2017 report, McAfee Labs predicted that the ongoing "learning period" for startup companies or organizations implementing IP-enabled devices for first time would last longer than four years.[41] A Verizon report identified that venture capital funding for startups surpassed that for large corporations in 2014, was later redirected back

[37] M. Masse, and P. Beaudry. The CRTC is not ready for the Internet of Things. *Globe and Mail* (May 22, 2017), online: <https://www.theglobeandmail.com/report-on-business/rob-commentary/the-crtc-is-not-ready-for-the-internet-of-things/article35078149>

[38] Office of the Privacy Commissioner of Canada (2016b). The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments [pdf document]. Retrieved from <https://www.priv.gc.ca/media/1808/iot_201602_e.pdf>

[39] L.Wasser, R. Hill, & M. Koczerginski, *Cybersecurity and the Internet of Things* (2016). <http://www.mcmillan.ca/mobile/Cybersecurity-and-the-Internet-of-Things>.

[40] Hewlett-Packard Development Company, "HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems" *HP News.*(February 10, 2015), online: <http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050

[41] McAfee Labs, *McAfee Labs: 2017 Threats Predictions (2016)* online: <https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf>.

to those large corporations.[42] It is thought that larger firms are better prepared to enforce proper security standards, which often require significant resources. However, issues with data management and security vulnerabilities remain a general concern regardless of the size of the firm.

Despite the striking growth in the industry, a Cisco Systems study reported that 60 percent of IoT initiatives stall at the Proof of Concept stage; only 26 percent of companies have had an IoT initiative that they considered a complete success, and a third of all completed projects were not considered a success.[43] While the Cisco report cites a number of reasons for the poor performance, they do not mention privacy or security.

Although independent bodies may release recommendations for developing IoT technologies, there do not seem to be any unifying bodies within the industry in place to promote standards and best practices across the market. This lack of standardization is a concern from the perspective of security and data management, as there are not consistent expectations in place for IoT developers to protect end-user data. While many privacy policies typically promise customers a secure infrastructure,[44] the massive number of connected devices and the volume of data they generate is becoming increasingly problematic. If implemented properly, these platforms could help mitigate the insufficient security and data management issues in IoT start-ups, and McAfee Labs says that vendor interest in security and privacy is expected to stem from consumer values

---

[42] Verizon, *State of the Market: Internet of Things 2016* Online: <https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>.

[43] Cisco Systems, "Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing." (May 23, 2017), online: <http://www.marketwired.com/press-release/cisco-survey-reveals-close-to-three-fourths-of-iot-projects-are-failing-nasdaq-csco-2217795.htm> (citing an estimate that the worldwide installed base of Internet of Things (IoT) endpoints will grow from 14.9 billion at the end of 2016 to more than 82 billion in 2025.

[44] See Table 6 *infra*.

and buying power more so than regulation.[45] As others think security issues warrant more attention from government regulators, it is becoming increasingly clear that there is no consensus as to whether privacy and security concerns will be adequately addressed through a market-based self-regulatory approach, or whether greater governmental regulation is needed.

Given the growing importance of security concerns, Part III will look at the problem of IoT threats and vulnerabilities in greater detail.

---

[45] McAfee Labs, Threats Predictions, *supra* note 41.

III. Security Vulnerabilities in the Internet of Things

A. Breaches of Personal Information

Privacy threats exist from both the authorized data collecting organization itself as well as from unauthorized external parties intercepting and tampering with personal information that is being collected and stored about end-users. A "privacy threat" has been more technically defined as "a possible event of exposure of sensitive data to entities (person, enterprise or artificial intelligence) which are not authorized to or required to possess those data. It can either be in the form of wrong data in the wrong entity's hands, or too much data in the hands of the right entity."[46]

In its 2016 report on the IoT applications in the home, the Office of the Privacy Commissioner observed that: "[a]s consumers and organizations begin to use Internet-enabled devices and sensors, more and more points are open to attack. An attack on one of these interconnected devices could provide an opportunity for a hacker to not only gain control of a device, but leverage it as a gateway to gain access to all kinds of personal information."[47]

In a 2015 report on IoT security issues Ernst &Young make the claim that "[i]n today's world of 'always on' technology and not enough security awareness on the part of users, cyber-attacks are no longer a matter of 'if' but 'when.'"[48] The report states that it will be easier for attackers to enter a network because "[t]raditionally closed operating technology systems have increasingly been given IP addresses that can be accessed externally, so that cyber threats are making their way out of the back office systems and into critical infrastructures, such as power generation and transportation systems and other automation systems."[49] The IoT network has also

[46] Misra, *Security Challenges*, *supra* note 29 at 33.
[47] OPC, *Internet of Things Introduction*, *supra* note 4 at 21.
[48] Ernst & Young, *Cybersecurity and the IoT*, *supra* note 28 at 10.
[49] *Ibid* at p.13.

been likened to a "giant, internet-connected global robot which is so disparate and insecure that cyberattacks against it are going to cause major societal problems if it isn't regulated." [50]

Besides the obvious breach of privacy when an unauthorized party views personal information, such parties may also use that information for nefarious purposes. The persistent footprint of the original user, the ID of their devices which are tied to them, may then fraudulently indicate criminal activity.[51] Unauthorized parties may also publish personal information; commit identity theft, or other such activities that could cause the subject of the information great distress. The IoT presents some significant, and in some cases, unique security concerns, and there has been an inadequate lack of mitigation on the part of IoT developers.

Breaches of consumer's personal data in general have been increasing,[52] and the security problem is being increasingly recognized as a main challenge for the development of the Internet of Things. The *Data Breach Database* by Gemalto identified 77 breaches occurring within Canada in 2016, compared to 31 in 2013, and approximately 84,382,464 records being compromised from 2013 onward.[53] However, much of Canadians data, especially consumer data, is stored on U.S. servers, where over 4 billion records were compromised over the same time period, though these could very likely be under-representations due to lack of reporting.[54]

Large-scale data breaches seem to occur most commonly as a result of hacking by third parties.[55] While higher profile examples like Ashley Madison, Target, and Yahoo generate

---

[50] Danny Palmer, "The Internet of Things? It's really a giant robot and we don't know how to fix it" *ZD Net* (June 8, 2017), online: <http://www.zdnet.com/article/the-internet-of-things-its-really-a-giant-robot-and-we-dont-know-how-to-fix-it/>.
[51] Misra, Security Challenges, *supra* note 29 at 35.
[52] See BusinessWire, "Survey: Nearly Half of U.S. Firms Using Internet of Things Hit by Security Breaches" (June 1, 2017), online: <http://www.businesswire.com/news/home/20170601006165/en>.
[53] Gemalto Inc., *Breach Level Index* (2017) online: <http://www.breachlevelindex.com/
[54] *Ibid.*
[55] D. McCandless, "World's Biggest Data Breaches & Hacks" *Information is Beautiful* (2017), online: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

significant publicity, lower profile internal breaches by employees, either negligent or malicious, should still be considered. It is clear that data breaches are prevalent in many aspects of society, and the risks become more prevalent when IoT technology becomes involved. The increased sensitivity of data collected from close and ubiquitous interaction with end-users personal lives makes data collected through IoT a greater privacy concern.[56] Additionally, the IoT poses new security vulnerabilities, many of which have not been actively addressed by IoT developers.

B. Fundamental Security Issues across the IoT

In their recent internet security report, Ernst & Young note that"[e]ffective cybersecurity is increasingly complex to deliver. The traditional organizational perimeter is eroding and existing security defenses are coming under increasing pressure. Point solutions, in particular antivirus software, IDS, IPS, patching and encryption, remain a key control for combatting today's known attacks; however, they become less effective over time as hackers find new ways to circumvent controls."[57]

In examining the security of IoT technology, it is important to recognize that the technology itself exists on many levels, as networks of many interacting components. Security vulnerabilities are determined to occur on four levels: the application layer (overall design of the device and program itself); the computing layer (where computations occur, either in the device or on a server elsewhere); the communication layer (information transport between device and servers/other devices); and the gadget layer (the hardware of the device itself).[58] Recognition of

[56] For a thorough analysis of the data collected by "fitness wearables", see Andrew Hilts, Christopher Parsons and Jeffrey Knockel, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security* (2016) online: <https://openeffect.ca/reports/Every_Step_You_Fake.pdf> [**Every Step you Fake**].

[57] Ernst & Young, *Cybersecurity and the IoT*, *supra* note 28 at 10.

[58] Misra, *Security Challenges*, *supra* note 29 at 15-16.

these different levels is important when considering the unique vulnerabilities that exist within each, and that each will have different standards or best practices which should be implemented.

Each IoT device and network may have security issues unique to its components, software, protocols, etc. However, there are some common fundamental security issues which are inherent across IoT devices. In some cases, it is impossible to directly address the issue without compromising the features that define a technology as IoT. For example, a commonly noted concern is the increase in the number of attack entry points, given that IoT devices are increasingly popular and pervasive as everyday objects. Security issues are multiplied by the network effect of IoT, meaning that one entry point can provide forced access to other components of the IoT system,[59] including multiple devices and data storage points which hold and transmit sensitive user data. Reducing the number of entry points would be counterproductive to the goal of IoT to provide interconnectivity of services; therefore, security must instead be strengthened and enforced throughout each component of the system.

However, there are several barriers to achieving this goal. Most IoT devices are light-weight, and there are significant limitations on battery power and digital storage space, meaning that there are less resources for implementing security features.[60]

In arguing that IoT is "notoriously insecure", privacy expert John Gregory argues that "(t)he people who build and sell the devices are more interested in connectivity than in security….[t]here is little space on some devices for a lot of code – so elements for access control such as passwords, plus capacity for updates, patches and the like are simply not included."[61]

There are also other issues arising in applying security patches. Security expert Bruce

[59] *Ibid* at 20.
[60] W. Trappe, R. Howard, & R.S.Moore, "Low-Energy Security: Limits and Opportunities in the Internet of Things" (2016) *IEEE Security and Privacy Magazine*.
[61] John Gregory, "Further Legal Snapshots From the Internet of Things" *Slaw* (May 17, 2017), online: <http://www.slaw.ca/2017/05/17/further-legal-snapshots-from-the-internet-of-things/>.

Schneier identifies multiple reasons why patching is not properly applied to routers, many of which could apply to other components of IoT networks, such as the implementation of outdated software which is no longer supported, a disconnect between the manufacturer of device components and the distribution, and a lack of interfaces for users to identify security issues and implement updates manually.[62] Besides being a practical issue, a lack of user interface for applying security patches is also a legal issue. As explained by Wasser, Hill, & Koczerginski Canada's Anti-Spam Law ("CASL") contains provisions governing software installation in the course of commercial activities which prohibit the installation of computer programs on another person's computer system without express consent. [63] They note that "since IoT devices often do not have interfaces that allows communication between a device and the owner, developers must consider alternative ways to obtain express consent for the installation of software updates."[64]

Ernst & Young also identified bandwidth problems as another barrier to security because "[t]housands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can bring down the server. Additionally, most of the sensors use an unencrypted link to communicate, and hence, there is a possibility of lag in the security. The bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless communications, which also operate on the megahertz frequencies like radio, television, emergency services, etc." [65]

---

[62] Bruce Schneier, "The Internet of Things Is Wildly Insecure - And Often Unpatchable" *Wired* January 6, 2014), online: <https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem>.

[63] L. Wasser, R. Hill, & M. Koczerginski, Cybersecurity and the Internet of Things (2016), online: <http://www.mcmillan.ca/mobile/Cybersecurity-and-the-Internet-of-Things>.

[64] *Ibid.*

[65] Ernst & Young, Cybersecurity and the IoT, *supra* note 28 at 15.

C. Problematic IoT Devices and Protocols

Security flaws appear to be widespread across IoT technologies. For example, in a study by Hewlett-Packard[66] which examined "smart home" devices, all devices tested had significant vulnerabilities, specifically a lack of requirement for a strong password, lack of two-factor authentication, and the lack of a lock-out feature. All cloud-based interfaces examined allowed account harvesting, and half of mobile interfaces allowed it as well. All cloud connections were deemed to be vulnerable to attack because transport encryption was not configured to secure the connection**.** 70% of devices also had software update issues, for example, a lack of encryption in authenticating and downloading update files, in some cases leading to ability to intercept or replace updates with malicious ones.

Unfortunately, the Hewlett-Packard study did not identify the specific devices examined, so an examination of other problematic IoT devices is necessary to appreciate the scope of security issues in the industry. There have been several recent reports of problematic devices including vehicle security,[67] defective smart lightbulbs,[68] childrens' toys, [69] a Bluetooth enabled vibrator,[70] and a menstrual cycle tracker.[71]

---

[66] Hewlett Packard Development Co., "HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems" *HP News.* (2015, February 10), online: <http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050>.

[67] See Shaun Nichols. "Sons of IoT: Bikers hack Jeeps in auto theft spree *The Register* (May 31, 2017) <https://www.theregister.co.uk/2017/05/31/bikers_hack_jeeps_in_auto_theft_spree/>. (reporting on a biker gang using lifted codes and stolen logins to bypass security and working in small teams to identify specific models of Jeep Wranglers in the San Diego area).

[68] See Ry Crist, "Hackers find security weaknesses with the Lifx smart LED" *C/Net* (July 7, 2014), online: <https://www.cnet.com/news/hackers-discover-security-weaknesses-within-the-lifx-smart-led/>. (reporting that researchers were able to hack wifi connection, who decrypted wifi credentials and accessed the wifi network associated with the device).

[69] See Rebecca Joseph, "My Friend Cayla: the doll for children accused of 'illegal espionage'" *Global News* (Feb 18, 2017), online: <http://globalnews.ca/news/3258509/my-friend-cayla-doll-illegal-espionage/> (reporting on security vulnerabilities in My Friend Cayla where a Bluetooth connection was found to be insecure and could allow third-parties to record children's conversations).

[70] See Kimoko de Freytas-Tamura, "Maker of 'Smart' Vibrators Settles Data Collection Lawsuit for $3.75 Million" *The New York Time* (2017, March 14, 2017), online:

Beyond these flaws in individual devices and apps, significant flaws have been found in protocols used across many IoT networks. For example, a security flaw in Zigbee[72] allowed attackers to identify and use network keys, leaving devices open for man-in-the-middle attacks (MITM) and device hijacking. MITM attacks are particularly relevant to the discussion of privacy, as they involve interception and manipulation of communications.[73] Another reported flaw involved numerous vulnerabilities in Belkin's WeMo home automation devices that put over a half-million in danger of being hacked.[74]

A recurring form of security breach perpetrated by hackers on IoT technologies are destructive in nature rather than research-based. According to a U.S. Homeland Security report, a common theme is the perpetration of Distributed Denial of Service attacks, which cripple servers by flooding them with superfluous traffic, and are typically carried out on networks such university servers, government websites, etc. to prevent users from accessing services.[75]

While there has been a lack of recognizable monetization opportunities for IoT hacking, it

---

<https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html>. (reporting on security flaws in vibrator device allowing couples in long distance relationships to control vibrator remotely via their smart phones resulting in ability of third parties to gain control of the device).

[71] Jerry Beilinson, "Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds. *Consumer Reports* (July 28, 2016), online: <http://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/> (reporting on security flaws in pregnancy app containing sensitive user info such as medication and history of abortion that could have allowed hackers to access passwords, emails, and personal information).

[72] See <http://www.zigbee.org/what-is-zigbee/>

[73] Charlie Osborne, "Critical IoT security flaw leaves connected home devices vulnerable" *ZDNET* (2015, August 6), online: Retrieved from <http://www.zdnet.com/article/critical-security-flaws-leave-connected-home-devices-vulnerable/. See also Ms. Smith "Researchers exploit ZigBee security flaws that compromise security of smart homes" CSO Online (August 15, 2015) <http://www.csoonline.com/article/2969402/microsoft-subnet/researchers-exploit-zigbee-security-flaws-that-compromise-security-of-smart-homes.html>.

[74] See Ms. Smith. "500,000 Belkin WeMo users could be hacked; CERT issues advisory" *CSO Online* (Feb. 28, 2014), online: <http://www.csoonline.com/article/2226371/microsoft-subnet/500-000-belkin-wemo-users-could-be-hacked--cert-issues-advisory.html>.

[75] United States. Computer Emergency Readiness Team, "Security Tip (ST04-015): Understanding Denial-of-Service Attacks" (Feb. 6, 2013), online: <https://www.us-cert.gov/ncas/tips/ST04-015>.

is expected that they will emerge and that ransomware will migrate to the IoT, taking devices and data hostage in return for payment. The use of ransomware has increased in recent years, and recently, a global attack using the ransomware WannaCrypt, targeted outdated Windows operating systems.[76] It seems reasonable to expect that an expanding base of connected Internet devices will attract an expanding base of individuals looking to exploit those systems for nefarious purposes. Key targets for hacking the IoT are expected to be "control planes" of IoT networks, which provide access to multiple devices, as well as data aggregation points.[77] "Strengthening the IoT's security is a major challenge. Being still an immature technology, a major issue affecting the acceptance and applicability of the IoT is the lack of a mature and comprehensive security model and standards."[78]

---

[76] Alexander Urbelis, "WannaCrypt ransomware attack should make us wanna cry" *CNN* (2017, May 14), online: <http://www.cnn.com/2017/05/14/opinions/wannacrypt-attack-should-make-us-wanna-cry-about-vulnerability-urbelis/index.html>.

[77] McAfee Labs, Threats Predictions, *supra* note 41.

[78] Misra, *Security Challenges*, *supra* note 29 at 15. See also Wasser, L., Palmay, F., Hill, R., & Koczerginski, M. (2016) Cybersecurity – The Legal Landscape in Canada (2016) http://mcmillan.ca/Cybersecurity--The-Legal-Landscape-in-Canada (pointing to gaps in the regulatory frameworks for cybersecurity)

IV. Personally Identifiable Information, Sensitive Information and Consent

This part will elaborate on three specific PIPEDA issues which are increasingly pertinent to discussions about the Internet of Things. The first two are definitional and have historically been framed as dichotomies: what information is "personally identifiable," and what information is deemed to be "sensitive." But given the dynamic nature of the IoT, these dichotomies no longer make sense. In the context of data gathered through IoT consumer applications, this information should be deemed to be both personally identifiable and sensitive.

The third area which has become increasingly problematic is the requirement of "consent" to the collection and use of personal information and whether the current "consent model" remains adequate in light of technological changes.

A. What is Personally Identifiable Information?

A threshold question which determines whether the requirements of PIPEDA apply is whether the information is considered to "personally identifiable," defined in section 2 simply as "**…**information about an identifiable individual." Since the inception of PIPEDA, the Office of the Privacy Commissioner has adjudicated several cases that turn on the question of whether or not particular information is deemed to be personally identifiable within the meaning of the Act. In an Interpretative Bulletin summarizing rulings on what constitutes personally identifiable information, the Privacy Commissioner has set out several general principles.[79]

First, the definition should be given a broad and liberal interpretation. Second, "personal information is information 'about' an identifiable individual. 'About' means that the information

[79] Office of the Privacy Commissioner of Canada, *Interpretation Bulletin: Personal Information*. (October 2013) Available at: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/>.

relates to or concerns the subject."[80] Third, the information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.[81]

The Bulletin provides examples of cases that have arisen in various contexts, including cases arising in the technological context. Personal information includes fingerprints[82] and voiceprints,[83] and a photograph of a person's home could constitute personal information depending on the context. [84] It can also include tracking information collected from a Global Positioning System (GPS)[85] as could info gathered through RFID tags.[86]

Vendors typically offer reassurance to consumers that any personally identifiable information about them will go through a process of de-identification through which identifying information will be separated from other 'non-identifying' data.[87] However, these processes are rarely elaborated or explained to the consumer in any detail. Nor is this process subject to any standards or regulation by an administrative body.

Current methods of anonymizing data may not be sufficient to truly protect end-user identities. Hashing, for example, is common cryptographic method used to protect instances of

[80] The Bulletin cites *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157.
[81] The Bulletin cites *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII).
[82] Privacy Commissioner's Report of Findings: Law School Admission Council Investigation (May 29, 2008)
[83] *Wansink v. TELUS Communications Inc.* (F.C.A.), 2007 FCA 21.
[84] PIPEDA Case Summary #349 - Photographing of tenants' apartments without consent for insurance purposes.
[85] PIPEDA Case Summary #351 - Use of personal information collected by Global Positioning System considered.
[86] Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices: A Consultation Paper, March 2008.
[87] See Table 2, *infra*

user data, however, it is still unique to each user, thus not anonymizing, and original data is able to be guessed and then confirmed using the hash function [88]

With respect to the creation of aggregated customer profiles, the OPC has stated that while the profiling, "may be done with aggregate or de-identified information, the amount of detailed information that can be obtained from ubiquitous, always-on devices expands the scope, scale and potential sensitivity of information."[89] They further note that "[c]ombining location data with offline and online information related to purchase histories and online browsing can potentially reveal a detailed portrait of an individual including sensitive information related to finances, purchases, or interests."[90]

In 2015, a new analytical algorithm developed to analyse consumers shopping habits was able to identify consumers using only four points of time and location metadata, with up to ninety percent accuracy.[91] Anonymization provides no protection for algorithms such as these, since the names, account numbers and other data which are removed in the anonymization process are not needed for the identification process.

Databases of consumer metadata are now the norm for many types of businesses, who often justify its collection and analysis in order to improve services. For the IoT however, the collection metadata is often the service itself, or a necessary component of it, therefore, it is a technology for which data de-identification is a particularly important issue.

In applying the test to determine whether or not particular information is deemed to be

[88] Ed Felten, " Does Hashing Make Data 'Anonymous'?" *Tech@FTC* (April 22, 2012) online: <https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous>.
[89] OPC, IoT Introduction, *supra* note 4 at 18.
[90] *Ibid*.
[91] Robert Lee Hotz, "Metadata Can Expose Person's Identity Even Without Name" *Wall Street Journal* (Jan. 29, 2015), online: <https://www.wsj.com/articles/metadata-can-expose-persons-identity-even-when-name-isnt-1422558349>.

personally identifiable, it is increasingly important to take into account the changing nature of how data is collected, stored, re-used and combined with other data.

Once it is determined the threshold test for "personally identifiable" information has been met, then Section 5 of PIPEDA requires compliance with obligations set out in Schedule 1, which correspond to the ten CSA Standards.

Much of the concern about how well anonymization can actually protect the private nature of personal information has resulted from technological advances in the field of "big data", which the OPC describes "as data sets so large, lacking in structure, and changeable from one moment to another that traditional methods of data analysis no longer apply."[92] Complex algorithms are used to find correlations in these data sets, but they are opaque to individuals and regulators as organizations consider them proprietary. [93]

As indicated, the distinction between personally identifiable and non-personally identifiable information is a crucial threshold issue because PIPEDA requirements apply only to personally identifiable information. This dichotomy is becoming increasingly problematic because "[t]he purpose of big data algorithms is to draw correlations between individual pieces of data. While each disparate piece of data on its own may be non-personal, by amassing, combining and analyzing the pieces, the processing of non-personal information may result in information about an identifiable individual."[94] These analytical procedures have the capability of reconstituting identities that have been stripped away, so it is difficult to know in advance when an algorithm will re-identify an individual.[95]

There is merit in abandoning the strict binary operation of the personal/non-personal

[92] OPC, *Consent and Privacy*, *supra* note 6 at 6**.**
[93] *Ibid*.
[94] OPC, *Consent and Privacy*, *supra* note 6 at 7**.**
[95] *Ibid.*

dichotomy in favour of a more nuanced approach based on potential risk to data subjects. However, this may prove difficult to put into practice as specific details about the data anonymization process are not readily transparent, which is exacerbated by the general lack of transparency surrounding the collection of the data in the first place.

The OPC has observed that "[d]ata collection in the IoT environment is often invisible to individuals. There is no interface between consumers and organizations where data would be exchanged in a visible and transparent way. Instead, data collection and sharing occurs device to device, without human involvement, as a result of routine activities."[96]

The underlying premise that data is capable of being de-identified is itself subject to debate. Some have argued that "information can never be truly de-identified, for the simple reason that too much secondary data is available which, when combined with the de-identified data, can enable the identification of individuals."[97] It has also been argued that the "risk of re-identification of de-identified data sets grows over time as re-identification techniques become more effective and more data sets become available for matching." [98] Others take a more optimistic approach to de-identification efforts, pointing to the Future of Privacy Forum (FPF), which "is working to establish a framework for applying privacy protections to de-identified data factoring in nature of data, and risk of re-identification, as well as the presence of any additional administrative safeguards and legal protections, such as data protection policies or contractual terms that restrict how third parties can use the data."[99] Given the fast-changing and dynamic nature of how data is collected and analyzed through the Internet of Things, it is evident that the assumptions about how

[96] *Ibid* at 8
[97] OPC, *Consent and Privacy*, *supra* note 6 at 15. (citing Paul Ohm, "Broken Promises of Privacy: Responding to the surprising failure of anonymization." *UCLA Law Review*, 57, 1701 (2009) online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>.
[98] OPC, *Consent and Privacy*, *supra* note 6 at 15.
[99] OPC, *Consent and Privacy*, *supra* note 6 at 16. See Future of Privacy Forum, *A Visual Guide to Practical De-Identification* (April 25, 2016), online: <https://fpf.org/issues/deid/>.

information can be characterized needs to be re-assessed. The dichotomy between "personally-identifiable and "non-personally identifiable" information needs to be replaced with a more nuanced approach that recognizes the inherent personal and identifiable nature of data gathered through consumer IoT applications. [100]

Once information is determined to be personally identifiable, then a further assessment is made as to its degree of sensitivity which also has significant bearing on the legal requirements for its use.

B. What is "Sensitive" Personal Information?

The sensitivity of data is important to consider in discussions of privacy, where the level of sensitivity is often used to determine what level of type of consent needs to be obtained, and what levels of protection needs to be taken to safeguard the data.

Traditionally, legal frameworks have supported the interpretation of a dichotomy of sensitive versus non-sensitive information. There are many kinds of data collected through IoT applications that are clearly sensitive such as biometric collected by face recognition software, or fitness data collected through wearable products like FitBit. Data collected from children is generally considered more sensitive than that of adults,[101] and concerns are arising from emerging IoT connected toys which record children's speech in order to provide services similar to personal

[100] See Omar Tene & Gabriela Zanfir-Fortuna, "Chasing the Golden Goose: What is the Path to Effective Anonymization" Future of Privacy Forum (2017), online: <https://fpf.org/wp-content/uploads/2017/03/Chasing-the-Golden-Goose-Mar-27-2017.pdf>. ("Concluding, the anonymisation/identifiabilitydebate seems to significantly shift towards a risk-based approach understanding, which includes paying more attention to the spectrum of identifiability and to identifying concrete compliance mechanisms with privacy and data protection law for processing pseydonymised data." at 12-13).

[101] For an example of a device which is designed for use by children, see Ciara O'Brien, "Keep tabs on your kids with this wearable tracker" *The Irish Times* (June 1, 2017), online: <http://www.irishtimes.com/business/technology/keep-tabs-on-your-kids-with-this-wearable-tracker-1.3097803>.

digital assistants.[102] There are also instances where sensitive financial data is stored and transferred, such as with Apple Pay to make instant purchases.

However, it is clear in examining the nature of modern data collection, and especially collection through the IoT, that the dichotomy of sensitive versus non-sensitive personal information is breaking down. Big data has become an increasing concern; although initially anonymized and seemingly impersonal, statistical analysis of large quantities of data are able to reveal emerging patterns which can re-identify end-users, predicting their behaviour and personal details.[103] This re-identification can be accidental, but can also be intentional, such as the incident of a teenage Target customer who was outed as pregnant as part of a marketing scheme which analyzed her purchase records.[104] The IoT facilitates the aggregation of data through the ongoing collection of information from device sensors. The OPC notes that "[c]onsumer devices and "things" that can continuously "talk" to a business can convey information that is of a personal and potentially sensitive nature about an individual."[105] Cross-device tracking is also becoming possible in many services and this increases the risk of re- personalization.

Given the dynamic nature of IoT devices, the "sensitive / non-sensitive" dichotomy should also be abandoned in favour of a purposeful approach, and all of the data collected from consumers should be presumed to be sensitive as well as personally-identifiable.

---

[102] Mike Orcutt, "Connected Toys are Raising Complicated New Privacy Questions".*MIT Technology Review* (July 22, 2016), online: <https://www.technologyreview.com/s/601942/connected-toys-are-raising-complicated-new-privacy-questions/>.

[103] See Matt Scully,"Big Data Tells Mortgage Traders an Amazing Amount About You" *Bloomberg Markets* (June 29, 2017), online: <https://www.bloomberg.com/news/articles/2017-06-29/big-data-can-tell-mortgage-traders-an-amazing-amount-about-you>

[104] Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, Forbes*. (February 16, 2012) online: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did>.

[105] OPC, Internet of Things Introduction, *supra* note 4 at 6.

C. The Consent Model and the Scope of Use of Data

Meaningful consent for the collection and processing of personal information is a fundamental underpinning of PIPEDA.

The OPC considers consent to be the "cornerstone" of PIPEDA,[106] and they view knowledge and consent as a requisite to the collection of personal information in order to give individuals control over their information.[107] Organizations must also inform individuals about what they will collect, how they plan to use or disclose what they have collected, and for what purposes. These requirements are intended "to enable individuals to decide whether or not to provide consent."[108] Furthermore,"[i]n order for consent to be considered meaningful under PIPEDA, individuals should have a clear understanding of what will be collected, how their personal information will be used, and with whom it will be shared."[109]

For consent to be both meaningful and informed, the consumer should be able to locate and understand the terms in the Privacy Policy and Terms of Service agreement. They should understand what rights they are being given, what they are being asked to give up and what choices they have in accepting or rejecting these terms. Taken together, the consumer should understand how these terms will impact their use of the product and what are the potential implications of the terms. Informed consent means that the consumer is able to make a conscious

---

[106] OPC, Consent and Privacy, *supra* note 6 at 1 (stating that "Organizations are required to obtain individuals' consent to lawfully collect, use and disclose personal information in the course of commercial activity. Without consent, the circumstances under which organizations are allowed to process personal information are limited. PIPEDA is based on a technologically neutral framework of ten principles, including consent, that were conceived to be flexible enough to work in a variety of environments.")

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

[108] OPC, Consent and Privacy, *supra* note 6 at 2.

[109] *Ibid* at 3.

choice about how their information will be collected and used, that they are given adequate information to make this choice, and that they actually have choices to make..

In theory at least, consent plays an important role in giving individuals control over their personal information. The OPC says that consent "functions as a way for individuals to protect their privacy by exercising control over their personal information – what personal information organizations can collect, how they can use it, and to whom they can disclose it."[110] The requirement of disclosure about what information they will collect and how they plan to use it is supposed to be clearly provided in advance and in a clear manner. Consent needs to be obtained from the consumer before or at the time of collection, or when a new use of personal information has been identified. [111] Furthermore, organizations may not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information *beyond* that required to fulfill an explicitly specified and legitimate purpose. At the same time, individuals should be informed of the consequences of withdrawing consent, particularly if they are withdrawing consent to a collection, use or disclosure of their personal information that is essential to the service they are signing up for.[112] Informed consent means that a consumer is provided with adequate information to make a decision that is best for themselves given their personal beliefs and preferences on privacy and sensitive information. Yet as a practical matter, given the nature of IoT devices, they are less likely to have an interface from which to facilitate express informed consent as had been the case with discrete transactions.

The OPC raises the concern "that technology and business models have changed so significantly since PIPEDA was drafted as to affect personal information protections and to call

[110] OPC, Consent and Privacy, *supra* note 6 at 2**.**
[111] OPC, *Consent and Privacy, supra* note 6 at 3**.**
[112] *Ibid*.

into question the feasibility of obtaining meaningful consent"[113] They note 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."[114] Advances in technology present new challenges in obtaining informed consent. For example in the case of Google biometric data collection via face recognition, it is the owners of photos who give "consent," but it is the data of individuals present in the photos that is stored on Google'a servers.[115] As a practical matter IoT devices are less likely to have an interface from which to facilitate express informed consent.

According to the OPC, "[b]inary one-time consent is being increasingly challenged because it reflects a decision at a moment in time, under specific circumstances, and is tied to the original context for the decision, whereas that is not how many business models and technologies work anymore."[116] It does not reflect the fluid nature of the IoT environment in which data flows through several devices and is not restricted to a set path. Unlike the case of a traditional discrete transactions, the data which is collected from consumers can now run through any number of devices and systems, beyond what the consumer may assume and even beyond the consumer's use of a specific product.

"The principle of data minimization, collecting as little personal data as possible, is usually

---

[113] OPC, *Consent and Privacy*, *supra* note 6 at 1.

[114] *Ibid*. See also Office of the Privacy Commissioner of Canada. Letter to the Standing Committee on Access to Information, Privacy and Ethics about the study of PIPEDA (Dec 2, 2016), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_161202/> (stating that "the constant and accelerating pace of technological change since the turn of the 21st century when PIPEDA came into force has resulted in some significant pressure points that are having a profound impact on privacy protection.")

[115] Christopher Zara, Google Gets Sued Over Face Recognition, Joining Facebook And Shutterfly In Battle Over Biometric Privacy In Illinois. *International Business Times*. (March 14, 2016), online: <http://www.ibtimes.com/google-gets-sued-over-face-recognition-joining-facebook-shutterfly-battle-over-2330278>.

[116] OPC, *Consent and Privacy*, *supra* note 6 at 6.

regarded as paradoxical with IoT, where sensors generally monitor as much data as possible."[117] This can be an issue of organizations having an overly broad purpose for which to collect the data or simply a matter of how the sensors are designed. Data minimization can also be made difficult by technical issues in IoT devices themselves. Sensors which collect end-user data are often very simple, and control is restricted due to low computing power, thus they are simply designed to collect data as efficiently as possible.[118]

The reason for the implementation of the data minimization principle is increasingly inconsistent with emerging IoT practices, and this growing disparity needs to be affirmatively addressed. Since by their nature many IoT devices are "always-on," they collect 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. Many security and monitoring devices are also collecting information about third parties who may not even be aware of the presence of the device or what information it is collecting about them. Of course, it is in this continuous and pervasive data collection that these products find their value, and the effect is there is much more data in the marketplace about individuals than there previously was or than there should be.

---

[117] V.A. Almeida, D. Doneda, & M. Monteiro, " Governance Challenges for the Internet of Things" *IEEE Internet Computing, 19*(4), 56-59 (2015) [**Almeida, Governance Challenges**].
[118] *Ibid*.

V. Privacy Policies and End-User Agreements for IoT Devices

To conduct our analysis of the Privacy Policies and Terms of Service agreements (ToS), we selected 19 products that are marketed to Canadian consumers. Table 1 shows the device or vendor with the link to the corresponding Privacy Policy and ToS.[119] Tables 2 through 8 show various provisions in these documents.

In several cases, (i.e., Android and Apple) there is not a separate set of privacy and ToS pages for a particular product, but rather a generic policy that covers a range of products offered by the company.

A. Stated Purpose of Data Collection

The second PIPEDA Principle requires that "the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."[120] This identification of purposes "at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes."[121] This requirement establishes the baseline for which the subsequent Limiting Collection principle (Clause 4.4, which limits collection to only that necessary for the stated purposes) can be measured. Yet the policies suggest that the stated purposes cannot really be linked to the data that will be collected in any discernible way. The typical policy reads like a large list of purposes accompanied by a listing of the types of data that will be collected. These policies are listed in Table 2.

Based on these terms, it appears that the purpose limitation is not a particularly useful in the IoT context where indiscriminate data collection is itself built into the system. The purpose of

[119] All of the links for this Table were accessed on June 29, 2017. Typically, the privacy policies and the terms of use are set out in separate documents.
[120] PIPEDA, Schedule 1, Clause 4.2
[121] *Ibid*, Clause 4.2.2

this principle is to determine the point at which the organization has collected 'enough' data to carry out its purpose. But where data collection is itself a substantial purpose, it becomes impossible to say how much data is 'enough.' The economic reality that data is increasingly seen as a source of value only exacerbates the problem.

Several of the vendors utilize lists of examples of purposes for the collection of data (Belkin, GE, Nymi, Pebble, Phillips and Tesla) and the wording (such as, includes) suggests the list is non-exclusive. In some cases, the terms describe the data collection policies as a whole, rather than make a distinction based on the source of the data. This conflation of sources makes it even more difficult to distinguish what data is being collected from the device itself, from the website, or at the time of purchase. For example, Pebble lists administering contests, device usage patterns and effectiveness, providing support, and sending marketing updates among its purposes It would be reasonable to believe that data collected from the smartwatch itself was not used for sending marketing updates or administering contests. The likely source of the data used for those purposes is data that is provided to register for an account to be used for Pebble's online services. Being specific about the source is an important distinction. In many cases, organizations collect the IP addresses of visitors to their websites. In that context, the IP address would be associated with a computer or smartphone that belongs to someone who took an affirmative act to visit the website. Taking a discrete and affirmative act is accompanied by a set of reasonable expectations that are different from an "always-on" device that allows the user's IP address to be continuously collected.

Belkin's policy also covers more than data than that generated from the device. Their purposes include: online account creation, notification of policy changes, measuring the effectiveness of advertising, improving Belkin products, and helping the consumer monitor and

safeguard his or her home network. These broad purposes are too much for a WeMo user to reasonably digest.

The breadth of these purposes also result in the problem of circular reasoning. In several instances, organizations have stated the purpose of data collection to be something along the lines of 'improving the product.' While this purpose may be accurate, it is vague and consequently has no practical meaning to the consumer. Such a lack of precise meaning should be viewed as a barrier to meaningful and informed consent, and consequently, as a failure of the privacy regime more generally.

While the language provided is non-specific and of little use to the consumer, it is difficult to conceive of language that would provide more practical information. For example, data is collected by the biometric fitness shirt Hexoskin to "Provide your services, improve our services and algorithms, perform research and data analysis." The reality is that IoT companies often perform complex data analysis for purposes that are not clearly stated, and through processes that are not disclosed. The PIPEDA requirement that 'purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed,"[122] is being frustrated. And even if the terms take the further step of describing the analysis techniques, the result could be a longer, more cumbersome, and less understandable privacy policy.

B. Methods of De-identification of Data

Privacy policies typically differentiate between identifying and 'non-identifying' data. PIPEDA's requirements only apply to data that is considered to be "personally identifying" Organizations are typically clear that identifying data would not be sold or otherwise commercially exploited.[123]

However, these provisions are often followed by other statements that authorize relatively

[122] PIPEDA Principle 4.3.2

[123] The Fitbit privacy policy begins with '[f]irst and foremost: We don't sell any data that could identify you." Belkin provides a similar assurance.

unfettered use of data that has been 'de-identified.' PIPEDA theoretically cannot restrict these practices as it only applies to personally identifiable information.[124] In essence, what is happening is that IoT companies are making the de-identification and exploitation of personal information a purpose to justify the initial collection.[125]

The glaring problem with this model is that there is no standard to assess the validity of 'de-identification' of data. The data should not be considered non-personal just because of the assurance in a privacy policy. There is not even an apparent best-practices among companies. Certain companies mention that data can be aggregated to achieve 'de-identification'[126] whereas others claim that the personality can be stripped from any data set.[127]

The means by which organizations claim to de-identify personal data is shown in Table 3.

C. Nature of Consent and How it is Obtained

In the context of the Internet of Things, consent is generally obtained under terms of service and privacy policy through the purchase and use of the device. The underlying assumption is that the consumer becomes familiar with these provisions before using the device. The terms of use we have reviewed are very consistent in applying this assumption to the use of the product. The general message is along the lines of, "If you do not consent to these terms, do not use the product."

But this assumption that agreeing to the terms of service constites any form of meaningful

[124] PIPEDA, s 4(1)(a).
[125] Pebble states that "de-identified data is not subject to any restrictions." August smart locks uses de-identified data for "business purposes." Nest uses non-identified data "to help us make sales, marketing, and business decisions." "Fitbit may share or sell aggregated, de-identified data that does not identify you, with partners and the public in a variety of ways."
[126] See, for example, the privacy policies published by Fitbit and Nest.
[127] For example, the privacy policy published by Google defines "non-personally identifiable information" as "information that is recorded about users so that it no longer reflects or references an individually identifiable user."

consent is a fiction in reality. While PIPEDA requires both knowledge and consent,[128] it does not require organizations to ensure that the consumer *actually* knows the purposes for which the data is being collected, it simply requires companies to make a reasonable effort to ensure knowledge.[129]

However, even if we assume that consumers are familiar with the contents of legal documents, the consent may still not be informed and freely given. This would require that the consumer actually has a choice to make.

Of the devices studied, only Tesla and Recon Fitness Glasses allow consumers to refuse to consent to the surrender of their data while maintaining product functionality. GE and Belkin also allow limited forms of opt-out. For most devices, the consumer is not left with any meaningful choice. The policies either do not address the issue, or they state that you can refuse to supply your data but then the product would not work.[130]

Another issue is that some devices have the capability to collect data from parties who have not purchased the device. For example, the August Smart Lock allows homeowners to send a virtual 'key' to guests for a period of time. Using this guest key requires guests to download the app to their mobile device. As mentioned in August's Privacy Policy, 'guests' are subject to the same data collection and usage practices as the owner of the device including having 'anonymized' data used for 'business purposes.' It seems improbable that guests would have been at least as informed as the primary user. Further complicating the issue is that the device can be linked to social media accounts at the discretion of the owner. This linking allows personal information to be shared between August and the social media provider. This means that it is

[128] PIPEDA, Schedule I, Principle 4.3.2
[129] PIPEDA, Schedule I, Principle 4.3.2
[130] Apple's Privacy Policy states "You are not required to provide the personal information that we have requested, but, if you chose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have."

possible that a guest's information is shared with a social media service without the guest even having the *possibility* of knowing how their data is being used. This is surely an untenable solution.

Where a device (such as the Amazon Echo)[131] records data in a room it functions as an "always-on" personal assistant that will respond to all voice commands given in a room. There is a high potential for this device to run afoul of several facets of PIPEDA. Similar to the August Smart Lock, there is the potential for guests to have their information collected without the possibility of knowing how the data is being used. Table 4 shows the various policies on how consent is obtained.

D. Limiting the Scope of Data Collected

This limiting principle is a qualifier on Principle 2 regarding the identification of the purposes for the collection. The rationale behind identifying the purpose of data collection is to ensure that organizations collect the minimum amount of information possible to achieve that purpose.

PIPEDA Principle 4 requires that organizations collect the minimum amount of data necessary to fulfil the identified purposes.[132] However, the stated purposes are generally not linked to the data that will be collected in any discernible way. The typical policy reads like a large list of purposes followed by a large listing of the types of data that will be collected.[133] These principles are critical to the functioning of the scheme as a whole. The underlying notion of PIPEDA is that the purpose of any given instance of data collection must be justified. In accordance with Principles 4.2.1 and 4.2.3., organizations are required to inform consumers of

[131] The Amazon Echo was not yet available in Canada at the time of our selection of products. See Torstar News Service "Why Canadians are being left out of voice-activated tech trend" *Toronto Metro* (January 23, 2017), online: <http://www.metronews.ca/life/technology/2017/01/23/why-canadians-being-left-behind-in-voice-activated-tech.html>.

[132] PIPEDA, Schedule 1, Clause 4.4.

[133] See Table 2, *infra.*

these purposes. However, PIPEDA does not specifically require organizations to specify what data will be used to fulfil a specific purpose. However, without a better coupling between the purpose and the data collected, the goals of PIPEDA are not being met.

An issue encountered with regard to the specification of the information to be collected, is that certain companies do not provide an exhaustive list. For example, the August Smart Lock lists the data it collects as "Includes but is not limited to…" Similarly, the Fitbit Privacy Policy states that "it *can* collect…" It seems that these simplifications are meant to minimize the amount of text and prevent the kind of list that is found in the Nest privacy policy. This tradeoff is clearly a balancing act. It may be impossible to specify all the data that is collected while at the same time presenting the information in a digestible format. PIPEDA unfortunately provides no guidance as to the appropriate balance.

The Myo fitness tracker by Thalmic Labs comes with a privacy policy that is clearly designed to mirror the issues that PIPEDA addresses. One section of that privacy policy is titled "Limiting Use, Disclosure, and Retention" which is identical to the language used in PIPEDA Principle 5. However, the section goes on to stipulate that "your information will be used for the purpose for which it was collected, or when it is required or permitted by law" which is also identical to the language used in PIPEDA Principle 5. This statement doesn't help determine whether Thalmic Labs has complied with its PIPEDA obligations. Without more clarity in the disclosure requirements, there is really not a meaningful way to limit, or to determine an appropriate limit to the data that is to be collected.

While they are separate, Principle 5 is closely related to Principle 2. While studying the privacy policies, we found that the stated purposes for the collection of data are generally stated at the same time as any restrictions on the use, disclosure, and retention of that data.

E. Safeguarding / Security Measures Specified

Table 5 shows the methods taken organizations to provide security for the data they hold. Given the growing importance of this issue, the general lack of any specificity or detail provided to the consumer about the types of measures taken is a glaring deficiency.

Once personal information has been collected, organizations have an obligation under PIPEDA to protect it "against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification"[134] its provisions do not specify details about what measures should be taken, only requiring that the "safeguards used to achieve this must be appropriate to the sensitivity of the data."[135] As a result, the terms of service and privacy policies we studied generally do not provide consumers with an adequate level of information in order to assess how well their data is being protected. And, as previously argued, data collected through consumer IoT applications should be deemed to be both personally identifiable and sensitive, it should follow that safeguards must be above the minimum. In any event, the standards need to be better defined.

Without a baseline standard with a more precise definition than simply "appropriate to the sensitivity of the data", it is difficult if not impossible for consumers to gage how well their information is being protected. As a practical matter the data has gone into a black hole, and little thought is given to how it is being handled unless there is a reported breach. This lack of transparency about how data is being protected should be a larger concern, given the current state of security in the IoT industry. is lacking in security standards.

While recent amendments to PIPEDA will require organizations to report breaches to the OPC, this in itself does not adequately address the problem of the vague safeguarding principle. While this new requirement will be a step in the right direction, it is not an effective method to

[134] Schedule 1, section 4.7.1.
[135] Schedule 1, section 4.7.2.

ensure that proper security precautions are built into the system in the normal course of routine data collection. While businesses may be influenced to implement certain security measures by fear of loss of reputation and market sanction by consumers should there be a reported breach, it is becoming clear that they need further motivation to implement security standards above the minimum requirements. The problem of inadequate security is compounded by the entry of new participants in the IoT industry who are under pressure to deliver a product to market at minimal cost and weight.

F. Governing Law and Dispute Settlement

The terms of service agreements typically contain a clause specifying the choice of applicable law that will govern the relationship between the vendor and the consumer as well as other matters relating to dispute settlements. Table 6 shows how the agreements treat these provisions.

Six of the vendors, all smaller firms, are based in Canada (Ecobee, Hexoskin, Nymi, Recon Fitness, Thalmic Myo and We-Vibe) so there is no issue about the status of PIPEDA. But the others vary in their treatment of applicable law. Android, August, Belkin, FitBit, Apple and Nest all point to California law. Phillips points to New York law, Mimo to Massachusetts and Owlet to Utah. Others are less clear. Several of the agreements provide for binding arbitration coupled with waivers of class arbitration, and some of these allow the consumer to opt-out of the arbitration provision. Among the Canadian firms, Ecobee provides for binding arbitration in Ontario.

The inevitable question arising from non-Canadian agreements purporting to resolve disputes in the vendor's home jurisdiction is whether Canadian consumers can waive their protections under PIPEDA.

The OPC has asserted jurisdiction over foreign entities doing business in Canada and the

Supreme Court of Canada has recently ruled in *Douez v Facebook, Inc*,[136] that contractual waivers of statutory rights might not be enforceable. The plaintiff had brought a class action in the British Columbia Supreme Court under B.C.'s privacy statute and Google sought to dismiss the action based on the forum selection provision in the Terms of Service that specified California as the forum. The court declined to enforce the term in the agreement and the action is now proceeding. In addition to its direct impact on enforceability of forum selection clauses, the case may have further implications for other terms in what are considered to be contracts of adhesion where the parties have disparate bargaining positions.[137]

..

---

[136] While a full treatment of the implications of this case is beyond the scope of this report, the Supreme Court's ruling in *Douez v Facebook, Inc*, 2017 SCC 33 suggests that contractual waivers of statutory PIPEDA rights might not be enforceable. For a detailed discussion of forum selection clauses in consumer contracts, see Public Interest Advocacy Center, *Shopping for Consumer Protection: Current Jurisdictional Issues* (April 2017), online: <https://www.piac.ca/wp-content/uploads/2014/11/shopping_for_consumer_protection.pdf>.

[137] See Samuel Trosow, *Douez v Facebook: Implications for Canadian Information Policy* (presentation, July 2017), online:<http://ir.lib.uwo.ca/fimspres/48>

VI. Conclusions and Policy Recommendations

Several recurring issues emerge from this study. A persistent theme is that many of the assumptions underlying the PIPEDA regulatory environment when it was in the development stage are no longer viable. The consent model, along with the underlying personal/non-personal and sensitive/non-sensitive distinctions has lost their relevance. The growth of "big-data" with its powerful algorithms that are capable of performing complex analysis and the ability to combine massive amounts of data from different sources requires new thinking about whether personally-identifiable information can be de-identified with any reasonable certainty. And while any given item of data may in itself be non-sensitive, this status is questionable after it is combined with other data to create a detailed profile about a consumer. The dynamic and continuous collection of data through devices that are "always-on" has outpaced the ability of organizations to properly safeguard and protect the security and integrity of the vast stores of information they hold. As an emerging and competitive industry, consumer device manufacturers are under pressure to bring new products to market where price, size, style and power consumption are key factors, and these can work at cross-purposes with security concerns.

As a practical matter, the assumptions underlying the consent model are undermined by the very nature of the unregulated Internet of Things. The purposes for the collection of the data are stated in the broadest of terms, the uses to which the data can be put are essentially unlimited, and consumers are forced to consent to these practices by virtue of harsh adhesion clauses which essentially say agree to these terms or don't use the service. This strips the end user of any real choice in terms of how their data will be used. As a result, a thorough review of the PIPEDA principles are needed to address all of these inter-related issues. This need is pressing as the Internet of Things continues to grow and as more Canadian households become exposed to the

privacy and security risks associated with the collection, storage and processing of their personal information. Such a review is especially timely given that the European Union General Data Protection Regulations will become enforceable in May 2018 and Canada will have to carefully review its policies to ensure they retain their adequacy status. As this undertaking will require significant effort from the Office of the Privacy Commissioner, it is important that they receive adequate funding and support in order to accomplish these tasks.

As an initial matter, the following recommendations are proposed:

Recommendation 1:

Data gathered from consumers through the Internet of Things should be presumed to be "personally-identifiable" and "sensitive" in nature.

The dichotomies between personally-identifiable information and non-personally-identifiable information, as well as between "sensitive" and non-sensitive information is becoming effectively irrelevant because of the power of complex algorithms to analyze large sets of data. As these capabilities become stronger and able to analyze larger amounts of data, it is necessary to update PIPEDA to recognize this technological reality. These emerging methods of data analytics, or the whole field of "big-data", as it is called, were not widely anticipated when PIPEDA was drafted. The potentially privacy-destructive nature of these advances in technology needs to be met with changes in our regulatory structure.

As a precautionary measure, all information collected from consumers using IoT applications should be presumed to be personally-identifiable as well as sensitive, even after it has been nominally depersonalized. These precautions are now necessary because of the enhanced possibility of re-identification as well as the ability of algorithms to make sensitive inferences from otherwise facially insensitive information which has been accumulated, combined, analyzed

and packaged for further use.

Recommendation 2:

In order to make privacy policies easier to understand, a standard format should be developed in order to promote public awareness of common terms.

A recurring problem we observed is that privacy policies are often difficult to read, much less fully understand. In in the case of larger vendors, they are difficult to even locate and it is not always clear what policies are applicable to any particular product or service. Given the general assumption that consumers consent to the collection and use of personal information by agreeing to the terms of a privacy policy, having greater clarity and standardization in these documents is a good first step towards ensuring that the consent is meaningful. A standardized template representing PIPEDA-compliant "best-practices" can certainly be developed. It would be reasonable then to require that any deviation from these terms be identified and separately spelled out and that these terms act as default rules in interpreting these policies. Reducing the amount of information contained in privacy policies and presenting it in a clear manner would be a useful step in the direction of improving the quality of informed consent. It would also make it easier for consumers to compare and contrast the privacy policies of different vendors. Crafting a model policy that is PIPEDA (and GDPR) compliant, consumer friendly and easy to understand will help improve the consent model and it should be relatively easy to draft.

Recommendation 3:

The limitations on the scope of data that can be collected and the requirement to disclose the purposes for its collection should be specified with greater clarity.

Our review of privacy policies and terms of service agreements confirms that most companies are not complying with the spirit and intent of these requirements. The purposes for

which data is being collected is typically stated in very broad and open ended terms. As a practical matter, the principle of limiting the scope data collection is frustrated by the practices of the IoT industry where data is indiscriminately collected. This problem is only exacerbated by the perceived value in the data itself. There is little incentive for the developers of IoT devices to build in limitations on the data it collects. By stating the purposes for collection in the broadest of terms, and then demanding consent as a condition of using the service, several important PIPEDA principles are vitiated. These clauses need to be drafted with much more specificity and they should not be stated in inclusive open-ended terms. There needs to be a more direct linkage between the nature of the service being provided and the particular data that is being collected. Simply stating that the data is being collected, somehow anonymized, and then analyzed for purpose of providing "improved services" is too vague, and its breadth vitiates the general principle that the purposes for the collection need to be disclosed.

Recommendation 4:

The limitations on the use, disclosure and retention of data should be specified with greater clarity.

The issue of how the data is being used is closely related to the problem of specifying the reason for its collection. If there were reasonable limits on the purposes for which data that can be collected, there would be less of a problem in terms of how it is being used as there would be less data in the system. As with the scope of data collected, the privacy policies do not provide adequate disclosure about how the vast stores of data are being used. While consumers are typically assured that data that personally identifies them will not be shared, they are given no information about how this will occur.

Presuming that the data remains personally identifiable information as outlined above will

help solve this problem. But there needs to be more explicit limits on how data can be used, how long it can be retained, how it is processed, and how the consumer can request its deletion.

Recommendation 5.

The consumer should have the opportunity to decline sharing data without losing the benefit of using a purchased device.

Presenting consumers with the standard "take-it or leave-it" choice should not be considered as an acceptable practice. Consent to some level of information collection is needed to complete the transaction, register the product and make it operational. But beyond this reasonable minimum, consumers should be given the choice of withholding their consent without being deprived of the use of a product. For example, in the case of wearable devices that generate health data, consumers should have the option of turning off the data collection that is reported back to the vendor. PIPEDA Principle 4.3.3 already prohibits requiring consent as a condition of the supply of a product, but this is limited to "information beyond that required to fulfil the explicitly specified, and legitimate purpose." This exception clause is overbroad because it goes beyond supplying information that is necessary to use the product.

A Canadian consumer who purchases an IoT device or who subscribes to a service should be given the standardized privacy policy discussed above. It should include a listing of clauses which deviate from the standard policy but which are necessary for the device or service to properly function. It should also include a listing of collection and use practices that are not necessary for the individual device to function along with the option to opt in or out of these collections or uses without penalty. Vendors would not necessarily be precluded from providing incentives to consumers for consenting to the collection of such additional data on reasonable terms, but that decision would be for the individual purchaser to make.

Recommendation 6:

The obligations to safeguard the information by organizations should be stated with greater specificity.

While PIPEDA states that the nature of safeguards "should" be organizational, physical, and technological (Principle 4.1.3), the quality of these safeguards are not sufficiently defined, much less enforced. Consumers should have more detailed information about the types of security measures being employed beyond the vague statements in most of the policies we studied. The OPC should be able to specify a set of best practices. The setting of standards is now typically accepted in many industries and there is no reason why the IoT industry should be exempt from reasonable regulations in this regard. While Principle 4.1.2 indicates that safeguards must be appropriate to the level of sensitivity, this language is vague and needs to be clarified, especially given the previous discussion about data sensitivity. A related issue is that consumers need to be given timely and accurate notice of any security breach as part of an overall approach to safeguarding.

By tightening up the safeguarding principle by making it more specific and giving it some substance through the development of standards, the overall state of internet security can be improved.

Recommendation 7:

Consumers should not be required to waive the protections of Canadian privacy laws, and they should not be required to submit to jurisdiction and venue outside of Canada.

Non-Canadian firms wishing to do business in Canada must understand that consumers cannot be asked to waive their rights under PIPEDA. Nor can they be asked to waive their rights to resolve any disputes in a local forum. Yet the choice of law and forum clauses in most of the agreements

from U.S. based vendors we reviewed do exactly that. While these provisions are already of questionable validity in light of the decision in *Douez v Facebook, Inc*, (2017 SCC 33), this point needs to be emphasized by way of clear and direct clause written into the model policy.

To summarize and conclude, the Office of the Privacy Commissioner should undertake a series of broad consultations to review and update the PIPEDA Principles in order to recalibrate the balance that is an underlying purpose of the Act. The technological, economic and social environment in which personal information is now collected, processed and re-used is quickly changing. It is a very different landscape than what was present in 2000 when PIPEDA was enacted. In order to address the challenges of these changes, the OPC will need to take a more active role in making sure regulations are kept up to date and that the interests of consumers do not lag behind. Like other technological developments in the past, the Internet of Things presents compelling evidence that laws need to adopt to changing circumstances. Without deliberate action, this balance that underpins PIPEDA will increasingly tilt away from the privacy interests of individual consumers. This is asking a lot from an agency, so it is important that policy makers ensure the OPC is adequately funded and staffed and they be given enforcement authority commensurate with the tasks they need to undertake.

Each of these recomendations will benefit from additional research and elaboration. It is hoped that others will take up the task of pursuing these (and other) proposals in order to recalibrate the balance that is an underlying purpose of PIPEDA.

Table 1:
Links for Selected Privacy Policies and Terms of Service

Device/Vendor	Link
Android	https://www.google.com/policies/privacy/ https://www.google.com/policies/terms/
August Smart Lock	http://august.com/legal/privacy-policy/ http://august.com/legal/eula/
Belkin WeMo	http://www.belkin.com/us/privacypolicy/ http://www.belkin.com/us/terms-of-use/
Ecobee	https://www.ecobee.com/legal/use/
Fitbit	https://www.fitbit.com/en-ca/legal/terms-of-service https://www.fitbit.com/en-ca/legal/privac
GE Connected Appliances (Café)	http://www.geappliances.com/privacy/privacy_policy.htm
Hexoskin	https://www.hexoskin.com/pages/privacy-policy https://www.hexoskin.com/pages/terms-of-use
iDevices	https://www.apple.com/privacy/privacy-policy/
Mimo	http://mimobaby.com/legal/
MomSense	https://mymomsense.com/terms-and-privacy/
Nest	https://nest.com/ca/legal/privacy-statement-for-nest-products-and-services/
Nymi	https://nymi.com/privacy https://nymi.com/legal
Owlet	http://www.owletcare.com/privacy/ http://www.owletcare.com/terms/
Pebble	https://www.pebble.com/legal/privacy
Philips Hue	http://www2.meethue.com/en-us/privacy-policy/ http://www2.meethue.com/en-us/terms-conditions/
Recon Fitness Glasses	https://reconinstruments.com/privacy-policy/ https://www.reconinstruments.com/terms-and-conditions/
Tesla	https://www.teslamotors.com/about/legal
Thalmic Myo	https://www.thalmic.com/privacy https://www.thalmic.com/terms/
We-Vibe	http://we-vibe.com/we-connect-privacy http://we-vibe.com/legal

Table 2:
Stated Purposes of Data Collection

Device/Vendor		Purposes of Data Collection
Android		We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads. We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics.
August Smart Lock		PII 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 (vii) 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.
Belkin		We may use the information we collect for a number of purposes. These purposes will be consistent with the reason you provided the information to us or for a directly related purpose. The uses we make of such information include the following: -To set up an account for you on Belkin websites or Belkin Products. -To facilitate your purchase and/or download of Belkin Products. -To authenticate use of your account or purchases and/or use of a Belkin Product. -To register your Belkin Product in our product database. -To carry out our obligations arising from any contracts entered into between you and us and to provide you with the information, products and services that you request from us. -To assist you with customer support.

		-To communicate about and administer participation in customer promotions and surveys. -To provide the Belkin Products you request. -To provide you with information about the Belkin Products you use, such as new features, bug fixes, service downtimes or upgrades. -To help us develop new Belkin Products and improve current Belkin Products. -To provide you, or permit selected third parties to provide you, with information about goods or services we feel may interest you. We (or selected third parties) will contact you by electronic means only if you have opted-in to receive marketing information. "Opt-in" means that you have taken an affirmative action to receive information, such as by checking a box or clicking a button. -To notify you about changes to Belkin websites and Belkin Products and changes to our terms, conditions and policies. -To administer Belkin websites and Belkin Products for internal operational purposes, including troubleshooting, data and statistical analysis, testing, research and survey purposes. -To improve Belkin websites and Belkin Products and to ensure that content is presented in the most effective manner for you and for your computer or device. -To ensure the security of Belkin websites and Belkin Products. -To monitor and regulate interactive features of Belkin websites and Belkin Products that you may choose to participate in, including online forums and chat rooms relating to Belkin Products. -To help you navigate Belkin websites. -To help you access and use certain features of Belkin Products remotely and to help you monitor and safeguard your home and home network. -To provide you with information and recommendations about Internet and utility usage in -your home. -To measure or understand the effectiveness of advertising we serve to you and others who visit Belkin websites and to deliver relevant personalized advertising to you and others. -To determine which aspects of Belkin websites and Belkin Products are most useful to you and other users of Belkin websites and Belkin Products.
Ecobee		Not clear
Fitbit		When activating a Fitbit Device, you will be asked to download the Fitbit App or install Software and enter information about yourself, such as height, weight and gender. We use this information to personalize your fitness stats–for example, calories burned and distance traveled. When you sync your Device through an App or the Software, data recorded on your Device about your activity is transferred from your Device to our servers. This data is stored and used to provide the Fitbit Service and is associated with your account. Each time a sync occurs, we log data about the transmission. Some examples of the log data are the sync time and date, device battery level, and the IP address used when syncing. 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. (several examples given)

GE Connected Appliances (Café)		We may use the personal information collected about you for the following purposes: To provide, administer and communicate with you about products, services, events, surveys and promotions (including by sending you marketing communications); To contact you in the event of a service notification for your registered appliance or to provide other notices concerning the safety of your appliance regardless of your stated privacy preferences. To process, evaluate and respond to your requests, inquiries and applications; To provide you access to the GE Appliances Store and GE Appliance Parts Store websites, we may ask for information such as your name, email address, postal address and phone number; To confirm and process your order, provide you with updates regarding your order, process returns and contact you concerning your order; To create, administer and communicate with you about your account (including any purchases and payments); To verify your identity to ensure security for the other purposes listed here; To evaluate your interest in employment and contact you regarding possible employment; To operate, evaluate and improve our business (including developing new products and services; managing our communications; performing market research; determining and managing the effectiveness of our advertising and marketing; analyzing our products, services and websites; administering our websites; and performing accounting, auditing, billing, reconciliation and collection activities); To protect against and prevent fraud, unauthorized transactions, claims and other liabilities, and manage risk exposure and quality; To conduct investigations and comply with and enforce applicable legal requirements, industry standards and our policies and terms, such as this and other Haier sites' terms of use; To ensure the safety of GE Appliances network services, information resources and employees. We also may use personal information for other additional purposes, which we identify at the time of collection. You may choose not to provide us with certain types of information, but doing so may affect your ability to use some services.

Hexoskin		Carré Technologies may use your personal information to: Provide you services, Improve our services and algorithms, Send you updates and information concerning your usage of the Services, Research and data analysis.
iDevices		Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising. You are not required to provide the personal information that we have requested, but, if you chose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have. We also use personal information to help us create, develop, operate, deliver, and improve our products, services, content and advertising, and for loss prevention and anti-fraud purposes.
Mimo		Our primary purpose in collecting Personal Information (as defined below) is to provide you with a safe, smooth, efficient, and customized experience. This allows us to provide Services and features that most likely meet your needs, and to customize our Services to make your experience safer and easier. We only collect Personal Information about you that we consider necessary for achieving this purpose, although we may collect additional Personal Information if you decide to provide it to us. In general, you can use our Services without telling us who you are or revealing any Personal Information about yourself. You can choose not to provide us with certain information, but by doing so, you may not be able to take advantage of many of our Services' features and functionality. We use Personal Information to deliver the Services to you, to improve our Services and to develop analytics and aggregated data that allows us and our affiliates to improve our Services. In order to make full use of our Services, you must first complete the registration form, create Login Credentials and configure your Lilypad(s) and Turtle(s). Once you give us your Personal Information, you are no longer anonymous to us. In addition, we collect information related to your usage of our Services. When you have a configured Turtle attached to your child's layette, the Turtle will collect certain biometric information, such as skin temperature, body position and breathing rate. A Lilypad can collect audio and ambient temperature information. We will not share that information with third parties, except for internet or telecommunications companies who we use to provide the Services. As one example, you can use our Services to receive a Mimo App alert regarding such information.
MomSense		We use the Personally-Identifying Information in the data we maintain about you, and other information we obtain from your current and past activities in connection with

		the Application to: deliver the products and services that you have requested, manage your account, if applicable, and provide you with customer support, communicate with you by email, postal mail, telephone and/or mobile devices about products or services that may be of interest to you either from us, our affiliate companies or other third parties, develop and display content and advertising tailored to your interests on the Application and other sites, resolve disputes, troubleshoot problems, measure consumer interest in our services, inform you of updates, customize your experience, detect and protect us against error, fraud and other criminal activity, enforce our End User License Agreement, and as otherwise described to you at the time of collection. At times, we may look across multiple users to identify problems. In particular, we may examine your Personally-Identifying Information to identify users using multiple listener IDs or aliases. We may compare and review your Personally-Identifying Information for accuracy and to detect errors and omissions. We may use financial information or payment method to process payment for any purchases made through the Application, enroll you in the discount, rebate, and other programs in which you elect to participate, to protect against or identify possible fraudulent transactions, and otherwise as needed to manage our business.
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. We may also use this information in an aggregated, non-identified form for research purposes and to help us make sales, marketing, and business decisions. For example, we use aggregated user information about the number of active thermostat users in a particular state to help us decide what energy companies might be good partners, and aggregated smoke and CO alarm data to study emergency alarm rates across our customers. We may use service providers to perform some of these functions. Those service providers are restricted from sharing your information for any other purpose.
Nymi		You acknowledge and agree that Nymi may use personal information that you voluntarily disclose to us to: 1. Provide you with information about new products, services, newsletters, informative emails, and research on future product ideas or improvements, where you have agreed to receive such materials; 2. Provide you with special offers that may be of interest to you and to improve your experience on our Web sites or with our products and services; 3. Assist us in creating better products and services to meet your needs; 4. Allow you to purchase and download products, obtain access to services or

		otherwise engage in activities you select including but not limited to the Nymi Band product; 5. Provide you with technical support; 6. Help you quickly find software, services, or product information important to you; 7. Send transaction-related communications such as welcome letters and product/service order confirmations. Nymi may also send you surveys or marketing communications to inform you of new products or services or other information that may be of interest; 8. Restrict the availability of some of the products, services, and content to certain parts of the world, where required for legal reasons, by using your address, IP address, and other information in order to enforce those restrictions; 9. To carry out other purposes that are disclosed to you and to which you consent; and 10. To carry out any other purpose permitted or required by law.
Owlet		We may collect certain health information about your infant when you use the Services, such as your infant's heart rate and blood oxygen level. We may aggregate and anonymize this information, and we may disclose such aggregated, anonymized data without restriction. We will not disclose health information unless it has been de-identified. Even if you do not provide us with any of your Personal Information, we may automatically track, collect, and store other information when you use our Application or Services, including without limitation the information that is made available to us through the Application, applicable operating system, and monitoring device. We aggregate and store such information to help us compile reports as to trends and other behavior about users visiting and using the Application. We reserve the right to share aggregated information with others in our sole and absolute discretion. We collect information automatically using the a variety of technologies, including the following: (several specified)
Pebble		We use the information that we collect in order to: -Provide you with the services and products you have purchased or requested and send you information about your relationship or transactions with us; -Notify you about new features of the Services, special events, and send you newsletters; -Administer sweepstakes and contests; -Generate and review reports and data about our user base and Service usage patterns; -Analyze the accuracy, effectiveness, usability, or popularity of the Services; -Provide you with support and improve the content and features of the Services or develop new Services; -Personalize the content and marketing that you see on the Services; -Permit you to obtain materials that enable you to develop applications if you use our developer services;

		-Send you marketing emails about Pebble products, software updates, and third-party products, software, and services that we believe may be of interest to you; -Send you push notifications about Pebble products and third party products and applications that we believe may be of interest to you on your mobile device if you have given us permission to do so; -Update third party applications that you have downloaded to your Smartwatch; -Help prevent fraud and enforce the legal terms that govern your use of the Services; and Administer and troubleshoot the Services.
Philips Hue		Sharing your personal data with us is necessary in order for us to provide you with the services that you have purchased, including: Using the Services Using other applications, products and functionalities made available by Philips Lighting or third parties that can be connected to the Services Buying goods on store.meethue.com Assisting you with after sales services Storing your preferences Providing software updates Improving website/app functionalities Helping us to develop products that are designed around you, optimize customer services and continuously improve our Services
Recon Fitness Glasses		Recon uses your personal information for various purposes, including: (a) to provide you with services (including to create and manage your accounts for Recon services) and to improve your experience; (b) to administer Recon's relationship with you, including to contact and correspond with you regarding products and software you have purchased, downloaded or registered with Recon and Recon services for which you have registered; (c) to facilitate your transactions with Recon, including processing orders and payments; (d) to process and respond to your inquiries, requests and other communications with Recon; (e) to provide you with general information regarding Recon and its products and services, to the extent permitted by applicable law; (f) to administer and facilitate your participation in contests and promotions related to Recon products, software and services; (g) to maintain, protect and improve Recon products, software and services to develop new products, software and services; and (h) to protect and enforce Recon's legal rights, interests and remedies and to protect the business, operations and customers of Recon or other persons.

		Recon may combine your personal information collected by Recon through various sources (including information collected through Recon's website and services and from Recon products and software). Recon may use personal information to create non-personal information, and Recon may then use, disclose, transfer and retain the non-personal information as explained below in this Privacy Policy.
Tesla		We may use information we collect to communicate with you, to provide and improve our products and services, and for other purposes. Examples of how we use information for these purposes are provided below. *To communicate with you* We may use information we collect to communicate with you, such as: ▪ To respond to your inquiries and fulfill your requests, such as to send you newsletters or product information, information alerts, or brochures. ▪ To set up, evaluate, and provide feedback regarding your Tesla test drive. ▪ To advise you of important safety-related information or to notify first responders in the event of an accident involving your vehicle. ▪ To send administrative information to you, for example, information regarding the Services and changes to our terms, conditions, and policies. ▪ To present products and offers tailored to you and to enhance our lists with information from other sources. ▪ To allow you to participate in contests and similar promotions and to administer these activities. ▪ To facilitate social sharing and communications functionality. Your communication choices: ▪ Receiving electronic communications from us or our affiliates: If you no longer want to receive marketing-related e-mails from us or our affiliates, you may opt out of receiving them by following the opt-out instructions in any e-mail received from us or by contacting us at the address below. Please note that we may still send you important administrative and safety messages even if you opt out of receiving marketing e-mails. ▪ Receiving marketing-related calls from us: If you receive a marketing-related call from us and do not want to receive similar calls in the future, simply ask to be placed on our "do not call" list. Please note that we may still call you regarding administrative, safety, or product service issues even if you opt out of receiving marketing calls. *To provide and improve our products and services* We may use information we collect to provide and improve our products and services, such as: ▪ To complete and fulfill your purchase, e.g., to process your payments, have

		your order delivered to you, communicate with you regarding your purchase, and provide you with related customer service. ▪ To provide service to your Tesla product, such as to contact you with service recommendations and to deliver over-the-air updates to your product. ▪ To monitor your Tesla product's performance and provide services related to your product. ▪ To develop and promote new products and services, and to improve or modify our existing products and services. ▪ To analyze and improve the safety and security of our products and services. ▪ To deliver any other services you have requested. *For other purposes*We also may use information we collect for other purposes, such as: ▪ For our business purposes, such as: data analysis; audits; fraud monitoring and prevention; identifying usage trends; determining the effectiveness of our promotional campaigns; and operating and expanding our business activities. ▪ Except as described above and below, Tesla may use or share information that does not personally identify you for any purpose, such as for operational or research purposes, for industry analysis, to improve or modify our products and services, to better tailor our products and services to your needs, and where legally required.
Thalmic Myo		Our collection of Personally Identifiable Information is limited to what is reasonable under the circumstances, and your information will be used for the purpose for which it was collected, or when it is required or permitted by law. Thalmic may ask to collect Personally Identifiable Information from you when you use the Thalmic Site. Thalmic also automatically receives and records information on our server logs from your browser, including your IP address, cookie information and the page you request. It is always your choice whether or not you provide us with your Personally Identifiable Information; however, a decision to withhold Personally Identifiable Information may restrict or prevent us from providing you with a particular product or service.
We-Vibe		You can use We-Vibe products without the We-Connect app. No information related to your use of We-Vibe products is collected from you if you don't install and use the app. We collect and use information for the purposes identified below. As with many applications, certain limited data is required for the We-Connect app to function on your device. This data is collected in a way that does not personally identify individual We-Connect app users. This data includes the type of device hardware and operating system, unique device identifier, IP address, language settings, and the date and time the We-Connect app accesses our servers. We also collect certain information to facilitate the exchange of messages between you and your partner, and to enable you to adjust vibration controls. This data is also collected in a way that does not personally identify individual We-Connect app users.

Table 2: Stated Purpose for Collection of Data

Table 3:
Method of De-identification of Personal Data

Device/Vendor	Stated method of de-identification of Personal Data
August Smart Lock	August may collect and analyze non-PII information about the performance of its Services. From time to time, August may disclose and use aggregate and non-personally-identifying information for industry analysis, demographic profiling, marketing and advertising, and other business purposes, e.g., by reporting on trends in the usage of its devices, Sites or Services.
Belkin WeMo	Information may be aggregated and/or anonymized. When information is aggregated, it is combined with information about other customers and users. When information is anonymized, Personal Information is removed from collected data and the remaining portion of the data, containing only Non-Personal Information, is repurposed for internal or external use, such as, for example, to determine how many users of a particular router include an Internet-enabled television in a home network environment, or how many users viewed a particular website video or advertisement. Aggregated information that includes Personal Information is considered Personal Information until it has been anonymized. Anonymized information is considered Non-Personal Information. In general, usage data collected when you visit Belkin websites or use Belkin Products is both aggregated and anonymized so it does not identify you personally and is therefore Non-Personal Information. we may share aggregated and anonymized Non-Personal Information, including usage data about Belkin Products, with third parties for a variety of purposes, including to analyze trends about home networking and utility use, to show third parties how their products could work with Belkin Products and to generally improve home networking. We've taken steps to ensure that this information cannot be linked back to you and we require third parties to keep all shared information in its anonymized form
Fitbit	We don't sell any data that could identify you. We only share data about you when it is necessary to provide the Fitbit Service, when the data is de-identified and aggregated, or when you direct us to share it. **DATA THAT COULD IDENTIFY YOU** Personally Identifiable Information (PII) is data that includes a personal identifier like your name, email or address, or data that could reasonably be linked back to you. We will only share this data under the following circumstances:[listing] **DATA THAT DOES NOT IDENTIFY YOU (DE-IDENTIFIED DATA)** Fitbit may share or sell aggregated, de-identified data that does not identify you, with partners and the public in a variety of ways, such as by providing research or reports about health and fitness or as part of

	our Premium membership. When we provide this information, we perform appropriate procedures so that the data does not identify you and we contractually prohibit recipients of the data from re-identifying it back to you.
GE Connected Appliances (Café)	We collect certain aggregate and non-personal information through a variety of technologies when you visit this website. Aggregate and non-personal information does not relate to a single identifiable visitor. It tells us such things as how many users visited our site and the pages accessed. By collecting this information, we learn how to best tailor our website to our visitors.
Hexoskin	Carré Technologies may share anonymously: Profile Information, Social Information, and Activity Information with researchers and partners to conduct further research on health, wellness and fitness. Before we share raw or aggregate data, it is de-identified to make sure you cannot be identified personally.
iDevices	We also collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it: [listing] If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.
Mimo	We may share aggregated demographic information about our user base with our affiliates and business associates. This information does not identify individual users. While we do not currently use advertising to support our Services, we reserve the right to share aggregate information with advertisers or data brokers who may be interested in such data. If we do decide to use advertising to support our Services, we may share usage information of our Services with our advertising affiliates to help them target advertisements to appropriate users. We do not link aggregate user data with Personal Information. Your contributions or notes to a module, forum or other service on the Website ("Contribution") may also be aggregated and made publicly available. Your Contributions may be aggregated according to their registration and login status.
MomSense	We may combine Non-Personally Identifying Information we collect with additional Non-Personally Identifying Information collected from other

	sources. We also may share aggregated information with third parties, including advisors, advertisers and investors, for the purpose of conducting general business analysis. For example, we may tell our advertisers the number of visitors to the Application and the most popular features or services accessed. This information does not contain any Personally-Identifying Information and may be used to develop content and services that we hope you and others will find of interest and to target content and advertising. We may combine Non-Personally Identifying Information we collect with additional Non-Personally Identifying Information collected from other sources. We also may share aggregated information with third parties, including advisors, advertisers and investors, for the purpose of conducting general business analysis. For example, we may tell our advertisers the number of visitors to the Application and the most popular features or services accessed. This information does not contain any Personally-Identifying Information and may be used to develop content and services that we hope you and others will find of interest and to target content and advertising.
Nest	We may share non-personal information (for example, aggregated or anonymized customer data) publicly and with our partners. For example, we may publish trends about energy use or elevated carbon monoxide levels in the home. This information may also be shared with other users to help them better understand their energy usage compared to others in the Nest community, raise awareness about safety issues, or help us generally improve our system. We may also share non-personal information with our partners, for example, if they are interested in providing demand-response services or other incentive programs. We take steps to keep this non-personal information from being associated with you and we require our partners to do the same.
Nymi	Personal information does not include "aggregate" anonymous information that does not identify an individual person, which is data we collect about the use of our Web sites and our products and services. Our privacy policy does not restrict or limit our collection and use of aggregate, anonymous information.
Pebble	We may anonymize and/or de-identify information collected by the Services or via other means so that the information does not identify you. Our use and disclosure of aggregated and/or de-identified information is not subject to any restrictions under this Privacy Policy, and we may disclose it to others without limitation for any purpose.
Philips Hue	We may also aggregate details which you have submitted to the website. Aggregate data does not contain any information that could be used to identify you and it is only used to assist us in providing an effective service on this website. We may from time to time supply third parties with this non-personal or aggregated data for uses in connection with this website.
Recon Fitness Glasses	Recon may automatically collect certain non-personal information regarding your use of Recon services (including the Engage™ service), such as the

	dates and times that you access a service, the browsers, operating systems, software and devices that you use to access a service and details of your use of a service. Recon may use that information for various purposes, including to administer and improve Recon products and services. Much of the information that is automatically collected by technological means is non-personal information (because the information does not identify you), and Recon will deal with that non-personal information as explained below in this Privacy Policy unless applicable law requires otherwise. Recon may combine your personal information collected by Recon through various sources (including information collected through Recon's website and services and from Recon products and software). Recon may use personal information to create non-personal information, and Recon may then use, disclose, transfer and retain the non-personal information as explained below in this Privacy Policy. Recon creates and collects non-personal information (information that is not about an identifiable individual), including personal information that has been aggregated or otherwise depersonalized so that it no longer relates to an identifiable individual. Recon may use, disclose, transfer and retain non-personal information for any purpose and in any manner whatsoever. If non-personal information is combined with personal information, then Recon will treat the combined non-personal information as personal information for the purposes of this Privacy Policy for as long as the non-personal information is combined.
Tesla	We do not share information that personally identifies you with unaffiliated third parties for their marketing purposes unless you opt in to that sharing.
Thalmic Myo	Thalmic may combine your information with other information into an aggregate form, so your information no longer personally identifies you. We may then disclose the aggregate information to third parties, so they can obtain an overall picture of Thalmic's products, services, customer usage patterns and/or other statistical information
We-Vibe	We use third party service providers to collect certain analytical information to help us improve our products and the quality of the We-Connect app. We receive this data in an aggregate, anonymous form that does not personally identify any individual We-Connect app user. This anonymous analytical data includes the app features used and time spent on the app. As part of our commitment to privacy, we enable users of the We-Connect app to opt-out of sharing this aggregate, anonymous data through the We-Connect app Settings under Privacy.

Table 3:
Method of De-identification of Personal Data

Table 4:
Nature of Consent and how it is Obtained

Device/Vendor	Link
Android	By using our Services, you are agreeing to these terms. Please read them carefully.
August Smart Lock	If you do not agree to the terms of this Agreement you may return the Device (in its original, unused condition) within thirty (30) days of the date of purchase (or the return period provided by your place of purchase, whichever is longer) for a refund in accordance with our returns policy as set forth in Section 3 of the Limited Warranty Statement below. In such case, you will also cease using, and destroy any Application (defined below) in your possession related to such Device. By using the Device, clicking "I Agree" on our Application or website, creating a user account, downloading or using the Application, you agree to be bound by the terms of this Agreement.
Belkin WeMo	Welcome to Belkin! These Terms of Use cover all Belkin, Linksys and WeMo branded websites and any other websites associated with www.belkin.com, including but not limited to any Belkin, Linksys or WeMo branded social media sites, and create an agreement between you and Belkin regarding your use of these websites (collectively, "Site"), and any apps that facilitate use of the Site or any services available by Belkin on or through the Site (collectively, "Services"). Your use of the Site and Services is governed by these Terms of Use and Belkin's Privacy Policy. Please review these carefully before using the Site or Services. By visiting Belkin websites, using Belkin Products or providing us with your Personal Information (as defined below), you are accepting and consenting to the practices, terms and conditions described in this Privacy Policy.
Ecobee	By checking the "I Agree" box and clicking on the "Submit Order" button to complete the purchase of ecobee Product(s), you hereby represent and agree that (i) you have read and agree to these ecobee terms and conditions of sale ("Standard Terms") and you have full power and authority to execute this Agreement and bind Customer (as hereinafter defined); (ii) you acknowledge and agree that the ecobee web portal service (the "Service") which will enable you to operate and manage the Product thermostat remotely and create and view energy

	performance reports, will require you to (a) register with ecobee at www.ecobee.com (the "Site") and (b) agree to be bound by ecobee's then current Terms of Service (provided by ecobee during the registration process); (iii) ecobee may, in accordance with the Standard Terms, on electronic receipt of the completed order form ("Order") pre-authorize the specified charges on the credit card specified in the Order and process the charges to such credit card prior to shipment of the Products specified in the Order; and (iv) the credit card information provided is yours or you have direct and full permission from the cardholder to carry out this transaction. The Order and the Standard Terms, together with all other agreements referred to herein and hereby incorporated by reference, are together referred to as the "Agreement"
Fitbit	These Terms of Service ("Terms") govern your use of our personal fitness and electronic body monitoring products, our websites, including www.fitbit.com, the software embedded in Fitbit devices, the Fitbit Connect software, the Fitbit mobile applications, memberships and other Fitbit services (collectively, the "Fitbit Service"). You must accept these Terms to create a Fitbit account and to use the Fitbit Service. If you do not have an account, you accept these Terms by visiting www.fitbit.com or using any part of the Fitbit Service. IF YOU DO NOT ACCEPT THESE TERMS, DO NOT CREATE AN ACCOUNT, VISIT WWW.FITBIT.COM OR USE THE FITBIT SERVICE
Hexoskin	By your affirmative actions of registering for and/or using the Hexoskin Services, you signify your agreement to these Terms of Use and our Privacy Policy and consent to allow Hexoskin to communicate with you electronically regarding the Hexoskin Services and Products.
Mimo	By using any of our Services, you consent to the current version of our Privacy Policy
MomSense	BY ACCESSING THE APPLICATION, YOU ARE ACCEPTING THE PRACTICES DESCRIBED IN THIS PRIVACY POLICY.
Nest	By using Nest Products, you agree to allow us to collect and process information as described in this Privacy Statement.
Nymi	The Service is offered subject to your (the "User") acceptance without modification of all of the terms and conditions contained herein and all other rules, policies and procedures

	that may be published from time to time by Nymi or posted on www.nymi.com (the "Site") ("Policies") – including, without limitation, Nymi's Privacy Policy www.nymi.com/privacy. To the extent any of the Policies conflict with this Agreement, such Policies shall control. **IF YOU DO NOT ACCEPT AND AGREE TO BE LEGALLY BOUND BY AND COMPLY WITH THESE TERMS OF USE, YOU ARE NOT PERMITTED TO ACCESS OR USE THE SERVICE.**
Owlet	By clicking "I Agree" or by .ssing or installing any part of the Application (as defined below), you expressly agree to, and consent to be bound by, all of the terms of this agreement (the "Terms and Conditions") and affirm your acceptance of the most recent version of the Terms and Conditions found in various application stores, including, but not limited to, the iTunes Store as provided by Apple Inc. ("Apple") which in no way are superseded or replaced by these Terms and Conditions. If you do not wish to be bound by these Terms and Conditions, please exit now and do not install the Application or, in the event that you have installed the Application, uninstall the Application. Please review these Terms and Conditions carefully before installation and/or acceptance.
Pebble	By accessing or using Pebble's websites (getpebble.com, pebble.com and cloudpebble.net), Pebble Smartwatch ("Smartwatch"), mobile applications, and/or any of Pebble's other online or mobile products ("Services"), you agree to Pebble's Privacy Policy and that we may transfer and store your information in the United States. IF YOU DO NOT AGREE TO THIS PRIVACY POLICY, PLEASE DO NOT USE THE SERVICES.
Philips Hue	By accessing or using this Web Site you agree to be legally bound by the Terms of Use and all terms and conditions contained or referenced herein or any additional terms and conditions set forth on this Web Site. If you do NOT agree to all of these terms, you should NOY access or use this Web Site.
Recon Fitness Glasses	Please read this Agreement carefully, **BEFORE** you indicate your acceptance of this Agreement as part of a transaction on the site. If you check the "I AGREE TO THE TERMS AND CONDITIONS OF THIS SALE" option as part of the transaction in which this agreement is presented, you agree to be bound by this entire Agreement including the warranty disclaimers, limitations of liability and methods of resolving disputes.

Tesla	If you no longer wish us to collect Telematics Log Data or any other data from your Tesla vehicle, please contact us as indicated in the "How to Contact Us" section below. Please note that, if you opt out from the collection of Telematics Log Data or any other data from your Tesla vehicle (with the exception of the Data Sharing setting detailed above), we will not be able to notify you of issues applicable to your vehicle in real time, and this may result in your vehicle suffering from reduced functionality, serious damage, or inoperability, and it may also disable many features of your vehicle including periodic software and firmware updates, remote services, and interactivity with mobile applications and in-car features such as location search, Internet radio, voice commands, and web browser functionality. If you no longer wish us to collect performance data or any other data from your Tesla energy product, please contact us as indicated in the "How to Contact Us" section below. Please note that if you opt out from the collection of performance data from your Tesla energy product, we will not be able to notify you of issues applicable to your energy product in real time, and this may result in your energy product suffering from reduced functionality, serious damage, or inoperability, and it may also disable many features of your energy product including periodic software and firmware updates.
Thalmic Myo	By accessing, browsing and/or using the Thalmic Site, you acknowledge that you have read, understood and agree to abide by and comply with these Terms of Use. Thalmic reserves the right, in its discretion, to update or revise these Terms of Use and to post such updates on this site. **Please check these Terms of Use periodically for changes. Your continued use of this site following the posting of any changes to the Terms of Use constitutes acceptance of those changes.**
We-Vibe	PLEASE READ THE TERMS AND CONDITIONS CAREFULLY. BY ACCESSING THIS WEBSITE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS AND BY ANY AND ALL OTHER POLICIES AND GUIDELINES INCORPORATED BY REFERENCE. IF YOU DO NOT AGREE TO ANY OF THE TERMS AND CONDITIONS, OR YOU DO NOT BELIEVE THAT THEY ARE REASONABLE, YOU ARE NOT AUTHORIZED TO ACCESS THIS WEBSITE.

Table 4: Nature of Consent and How it is Obtained

Table 5:
Safeguarding / Security Measures Specified

Device/Vendor		Safeguarding / Security Measures Specified
Android		We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular: • We encrypt many of our services using SSL. • We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome. • We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems. • We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.
August Smart Lock		The security of your personal information is important to us. We follow generally-accepted industry standards to protect the PII submitted to us, both during transmission and once we receive it. However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, we cannot guarantee its absolute security.
Belkin WeMo		We strive to maintain reasonable administrative, technical and physical safeguards designed to protect the information collected by Belkin websites and Belkin Products. Unfortunately, the transmission of information via the Internet is not 100% secure. Although we will do our best to protect your Personal Information, we cannot guarantee its security; any transmission is at your own risk.
Ecobee		ecobee uses reasonable precautions to keep the information disclosed to us secure. ecobee reserves the right to transfer information in connection with the sale of all or part of ecobee capital stock or assets to any third party. Furthermore, we are not responsible for any breach of security or for any actions of any third parties that receive the information.
Fitbit		Fitbit uses a combination of technical and administrative security controls to maintain the security of your data. If you have a security-related concern, please contact Customer Support.

GE Connected Appliances (Café)		We maintain administrative, technical and physical safeguards to protect against unauthorized disclosure, use, alteration or destruction of the personal information you provide on this web site. We use secure socket layer (SSL) technology and other technologies to help keep the personal information you provide on this site secure.
Hexoskin		We use a combination of firewall barriers, encryption techniques and authentication procedures, among others, to maintain the security of your data and to protect your accounts and our systems from unauthorized access. However, no Internet transmission, telephone call, or regular mail, can be guaranteed to be fully secure or error free. In particular, e-mail sent to or from us may not be secure. Therefore, you should take special care in deciding what information you send to us using these means of communication.
iDevices		Apple takes the security of your personal information very seriously. Apple online services such as the Apple Online Store and iTunes Store protect your personal information during transit using encryption such as Transport Layer Security (TLS). When your personal data is stored by Apple, we use computer systems with limited access housed in facilities using physical security measures. iCloud data is stored in encrypted form including when we utilize third-party storage.
Mimo		The security of your Personal Information is important to us. When you enter sensitive information on our registration forms, we encrypt that information using secure socket layer technology (SSL). We do not encrypt data transmitted from Turtles to Lilypads, from Lilypads to our servers, or between our servers and the Mimo App. We follow generally accepted industry standards to protect the Personal Information submitted to us, both during transmission and once we receive it. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, while we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.
MomSense		We take security of your Personally-Identifying Information seriously and use reasonable electronic, personnel, and physical measures to protect it from loss, theft, alteration, or misuse. However, please be advised that even the best security measures cannot fully eliminate all risks. We cannot guarantee that only authorized persons will view your information. We are not responsible for third party circumvention of any privacy settings or security measures.

Nest		We use industry-standard methods to keep this information safe and secure while it is transmitted over your home network and through the Internet to our servers. Depending on your location and type of data, Nest may process your personal information on servers that are not in your home country.
Nymi		Nymi stores and processes your personal information on computers located in Canada and in the cloud internationally. Nymi employs reasonable physical, organizational, managerial and technical measures to help ensure that your personal information is secure. In addition, our dedicated team of information technology professionals works to maintain data accuracy and help prevent unauthorized access to sensitive information. Personal information may only be accessed by persons within our organization, or our third party service providers, who require such access to carry out the purposes indicated above. Unfortunately, no security system can be guaranteed to be 100% secure. Accordingly, we cannot guarantee the security of your personal information and cannot assume liability for improper access to it.
Owlet		The security of your information is important to us. When you provide Personal Information to us through our registration or order forms, we encrypt the transmission of that information using secure socket layer technology (SSL). We follow generally accepted security standards to protect your information during transmission and once we receive it. No method of transmission over the Internet, or method of electronic storage, is 100% secure, therefore, we cannot guarantee its absolute security. If you have any questions about security of our Application and the Services, please contact us
Pebble		We have put in place appropriate physical, electronic, and managerial procedures to safeguard and help prevent unauthorized access, to maintain data security, and to use correctly the information we collect online. These safeguards vary based on the sensitivity of the information that we collect and store. Although we take appropriate measures to safeguard against unauthorized disclosures of information, we cannot assure you that personal information that we collect will never be disclosed in a manner that is inconsistent with this Privacy Policy.
Philips Hue		At Phillips Lighting we use the highest quality data security tools to keep your data safe and protect Hue from unauthorized access We recognize our responsibility to protect the information you entrust to us. Phillips Lighting uses a variety of techniques to protect your information, including protected servers, firewalls and encryption.
Recon Fitness Glasses		Recon employs reasonable safeguards – including administrative, physical and technical security and safeguarding measures and solutions – appropriate to the sensitivity of the personal information in Recon's possession or under Recon's control in order to protect the information from unauthorized access,

		collection, use, disclosure, disposal or similar risks. Nevertheless, security risks cannot be eliminated and Recon cannot guarantee that your personal information will not be used or disclosed in ways not otherwise described in this Privacy Policy.
Tesla		We seek to use reasonable organizational, technical, and administrative measures to protect information within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account with us has been compromised), please immediately notify us of the problem by contacting us in accordance with the "How to Contact Us" section below. If you sell or transfer your Tesla product to another person, please notify us so that we can determine whether additional steps are required to help safeguard information from or about you from disclosure to the purchaser or transferee of the Tesla product.
Thalmic Myo		Thalmic will take reasonable precautions to maintain the confidentiality and security of your Personally Identifiable Information so that it is not disclosed to anyone outside our group of companies and our selected third party service providers/business partners without your consent, unless required by law or as otherwise set forth herein. Where possible, Thalmic Labs protects the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts the information you input.
We-Vibe		We have implemented administrative, technical and physical measures designed to safeguard the information in our custody and control against theft, loss and unauthorized access, use, modification and disclosure. We restrict access to information on a need-to-know basis to employees and authorized service providers who require access to fulfill their job requirements. We have information retention processes designed to retain information for no longer than necessary for the purposes stated above or to otherwise meet legal requirements.

Table 5: Safeguarding / Security Measures Specified

Table 6:
Governing Law and Dispute Settlement

Device/Vendor	Governing Law/ Dispute Settlement
Android (see table 1 for URLs)	The laws of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services. All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.
August Smart Lock	**This Agreement shall be governed by and construed in accordance with the laws of the State of California and the United States without regard to the conflict of laws provisions therein that would require application of the laws of another jurisdiction.**
Belkin WeMo	If you are located outside of the United States, or if the above arbitration clause does not apply to you or is otherwise unenforceable as adjudicated by a court of competent jurisdiction, the following clause applies to you: These Terms of Use will be governed by California law, without reference to conflict of laws principles. The state and federal courts of California shall have non-exclusive jurisdiction over any claim arising under, or in connection with, these Terms of Use. However, if you are a consumer and you live in a country where Belkin markets or promotes the Site or a Service, local law may require that certain consumer protection laws of your country of residence apply to some sections of these Terms of Use. Each of the United Nations Convention on Contracts for the International Sale of Goods and the United Nations Convention on the Limitation Period in the International Sale of Goods is hereby expressly excluded and will not apply to these Terms of Use.
Ecobee	Any dispute relating in any way to your visit or access of the ecobee inc. website or to the products or services you purchase through the ecobee inc. website shall be submitted to binding arbitration in Ontario, except that, to the extent you have in any manner violated or threatened to violate ecobee inc. intellectual property rights, ecobee inc. may seek injunctive or other appropriate relief in any state or federal court in the province of Ontario, and you consent to exclusive jurisdiction and venue in such courts. The arbitrator's award shall be binding and may be entered as a judgment in any court of competent jurisdiction. To the fullest extent permitted by applicable law, no arbitration under these Conditions of Use shall be joined to an arbitration involving any other party subject to these Conditions of Use, whether through class arbitration proceedings or otherwise.

Fitbit	The Terms of Service and the resolution of any Disputes shall be governed by and construed in accordance with the laws of the State of California without regard to its conflict of laws principles. [Informal dispute resolution followed by Arbitration w/ 30 day opt-out any judicial proceeding (other than small claims actions) will be brought in the federal or state courts of San Francisco County, California. venue and personal jurisdiction in SF Cal. (jury trial waiver)]
GE Connected Appliances (Café)	Not specified
Hexoskin	The Terms of Use and the resolution of any dispute related to the Terms of Use or the Hexoskin Services shall be governed by and construed in accordance with the laws of the Province of Quebec without respect to its conflict of laws principles. You shall bring any legal action or proceeding against Hexoskin related to the Hexoskin Services exclusively in a federal or state court of competent jurisdiction sitting in Montreal, in the province of Quebec, and you agree to submit to the personal and exclusive jurisdiction of such courts.
iDevices	[Terms of use are not clearly specified for individual products.] For internet services; You agree that all matters relating to your access to or use of the Site, including all disputes, will be governed by the laws of the United States and by the laws of the State of California without regard to its conflicts of laws provisions. You agree to the personal jurisdiction by and venue in the state and federal courts in Santa Clara County, California, and waive any objection to such jurisdiction or venue. The preceding provision regarding venue does not apply if you are a consumer based in the European Union. If you are a consumer based in the European Union, you may make a claim in the courts of the country where you reside. For Repair services: To the extent permitted by law, all service orders received from residents of Canada will be governed by the laws of the province of Ontario without giving effect to its conflict of law provisions. Customers in Quebec will be governed by that province's consumer protection legislation.
Mimo	19. These Terms of Service shall be governed by the laws of . . . Massachusetts, USA, excluding: its conflicts of laws principles that would result in the application of the law of any other jurisdiction; the United Nations Convention on Contracts for the International Sale of Goods; the 1974 Convention on the Limitation Period in the International Sale of Goods; and the Protocol amending the 1974 Convention, done at Vienna April 11, 1980. 20. Except if you opt-out or for disputes relating to your or Rest Devices's intellectual property (such as trademarks, trade dress, domain names, trade secrets, copyrights and patents), you agree that all disputes between you and Rest Devices (whether or not such dispute involves a third party) arising out of

	or relating to these Terms of Service, the Services, and/or Privacy Policy shall be finally resolved by arbitration before a single arbitrator conducted in the English language in Boston, Massachusetts, U.S.A. under the Commercial Arbitration Rules of the American Arbitration Association (AAA) and you and Rest Devices hereby expressly waive trial by jury. You and Rest Devices shall appoint as sole arbitrator a person mutually agreed by you and Rest Devices or, if you and Rest Devices cannot agree within thirty (30) days of either party's request for arbitration, such single arbitrator shall be selected by the AAA upon the request of either party. The parties shall bear equally the cost of the arbitration (except that the prevailing party shall be entitled to an award of reasonable attorneys' fees incurred in connection with the arbitration in such an amount as may be determined by the arbitrator). All decisions of the arbitrator shall be final and binding on both parties and enforceable in any court of competent jurisdiction. Notwithstanding the foregoing, either party may apply to any court having jurisdiction over the parties for a judicial acceptance of the award or order of enforcement or to seek injunctive relief, security or other equitable remedies. Under no circumstances shall the arbitrator be authorized to award damages, remedies or awards that conflict with these Terms of Service. Any claim brought by you or Rest Devices must be brought in that parties' individual capacity, and not as a plaintiff or class member in any purported class or representative proceeding. Neither you nor Rest Devices will participate in a class action or class-wide arbitration for any claim covered by these Terms of Service. You hereby waive any and all rights to bring any claim related to these Terms of Service and Privacy Policy as a plaintiff or class member in any purported class or representative proceeding. You may bring claims only on your own behalf. You may opt out of this Agreement To Arbitrate. If you do so, neither you nor Rest Devices can require the other to participate in an arbitration proceeding. To opt out, you must notify Rest Devices in writing within thirty (30) days after the date that you first became subject to this arbitration provision. The opt-out notice must state that you do not agree to the Agreement To Arbitrate and must include your name, address, phone number, and a clear statement that you want to opt out of this Agreement To Arbitrate.
MomSense	The Application is hosted in the United States of America (“United States” or “U.S.”) and is subject to U.S. state and federal law. If you are accessing the Application from other jurisdictions, please be advised that you are transferring your personal information to us in the United States, and by accessing the Application, you consent to that transfer and use of your personal information in accordance with this Privacy Policy. You also agree to abide by the applicable laws of applicable states and U.S. federal law concerning your access to the Application and your agreements with us. Any persons accessing the Application from any jurisdiction with laws or regulations governing personal data collection, use and disclosure different from those of the jurisdictions mentioned above may only use the Application in a manner lawful in their jurisdiction. If

	your access to the Application would be unlawful in your jurisdiction, please do not access the Application.
Nest	11. [Arbitration (w 30 day opt-out. No Class arbitration] 13 (b) Governing Law. The courts in some countries will not apply California law to some types of disputes. If you reside in one of those countries, then where California law is excluded from applying, your country's laws will apply to such disputes related to these terms. Otherwise, you agree that these Terms, and any claim, dispute, action, cause of action, issue, or request for relief arising out of or relating to these Terms or your use of the Products and Services shall be governed by the laws of the State of California without giving effect to any conflict of laws principles that may provide the application of the law of another jurisdiction. You agree to submit to the personal jurisdiction of the state and federal courts in or for Santa Clara County, California for the purpose of litigating all such claims or disputes, unless such claim or dispute is required to be arbitrated as set forth in an above section.
Nymi	23d For users who are not individuals resident in the province of Quebec, this Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and the laws of Canada applicable therein. The Parties agree that the courts located in the City of Toronto, in the Province of Ontario shall have the exclusive jurisdiction and venue to determine all disputes and claims arising between the parties. For users who are individuals resident in the province of Quebec, this Agreement shall be governed by and construed in accordance with the laws of the Province of Quebec and the laws of Canada applicable therein. The Parties agree that the courts located in the City of Montreal, in the Province of Quebec shall have the exclusive jurisdiction and venue to determine all disputes and claims arising between the parties.
Owlet	17b. Governing Law. These Terms and Conditions will be governed and construed under the laws of the State of Utah without regard to conflict of laws. In the event of any disputes concerning this agreement, the parties agree to submit to the jurisdiction of the Salt Lake City District Court, Utah.
Pebble (Pebble has been acquired by FitBit and is no longer taking orders)	Pebble complies with the US-EU Safe Harbor Framework and US-Swiss Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland.

Philips Hue	16. Dispute Resolution These Terms of Use shall be governed by and construed in accordance with the laws of the state of U.S.A. You agree to the non-exclusive jurisdiction of the courts in New York, U.S.A. for any disputes, claim or cause of action arising out of, or relating to or in connection with these Terms of Use or your use of this Web Site, including any disputes relating to the existence or validity of these Terms of Use, provided that you agree to submit any such disputes, claims or causes of action exclusively to the courts of New York, U.S.A.
Recon Fitness Glasses	This Agreement will be governed by and interpreted in accordance with the laws (procedural and substantive) of the Province of British Columbia and the federal laws of Canada as if made and performed by and between parties situate in such province and without regard to the conflict of law rules that would apply a different body of law. Subject to the enforcement by Recon of its rights under this Agreement in any other jurisdiction requiring injunctive relief, and to the dispute resolution procedure set out herein, any dispute arising out of or in connection with or in relation to this Agreement will be submitted to and be subject to the exclusive jurisdiction of the courts of the Province of British Columbia, Canada, situate in Vancouver. [Jury waiver and mediation/arbitration dispute clause]
Tesla	Subject to applicable law, in certain jurisdictions you may also have the rights to request access to and receive information about certain information we maintain about you, update and correct inaccuracies in that information, and have the information blocked or deleted, as appropriate.
Thalmic Myo	This policy was written in accordance with the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). The Thalmic Site is controlled, operated and administered by Thalmic (or its licensees) from its offices within Canada and is not intended to subject Thalmic to the laws or jurisdiction of any state, country or territory other than those of Canada.
We-Vibe	Any matter that arises out of your use of this Website shall be governed by the laws of the Province of Ontario, in the country of Canada. All contracts shall be concluded in English.

Table 6: Governing Law and Dispute Settlement

APPENDIX A
PIPEDA Schedule 1

Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96

4.1 Principle 1 — Accountability An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4 Organizations shall implement policies and practices to give effect to the principles, including

(a) implementing procedures to protect personal information;
(b) establishing procedures to receive and respond to complaints and inquiries;
(c) training staff and communicating to staff information about the organization's policies and practices; and
(d) developing information to explain the organization's policies and procedures.

4.2 Principle 2 — Identifying Purposes The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1 The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6 This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 – Consent The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where 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, 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 and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. 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 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. 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 that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
> **(c)** consent may be given orally when information is collected over the telephone; 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 contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 Principle 4 — Limiting Collection The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3 This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 Principle 5 —Limiting Use, Disclosure, and Retention Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1 Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4 This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 Principle 6 — Accuracy Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2 An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 — Safeguards Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3 The methods of protection should include

> **(a)** physical measures, for example, locked filing cabinets and restricted access to offices;
> **(b)** organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
> **(c)** technological measures, for example, the use of passwords and encryption.

4.7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 — Openness An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2 The information made available shall include

> **(a)** the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
> **(b)** the means of gaining access to personal information held by the organization;
> **(c)** a description of the type of personal information held by the organization, including a general account of its use;
> **(d)** a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
> **(e)** what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 — Individual Access Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4 An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 — Challenging Compliance An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1 The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2 Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3 Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4 An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

References

ACM (2017) *Statement on Internet of Things Privacy and Security*. (ACM U.S. Public Policy Council and ACM Europe Council Policy Committee) <http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_iotprivacysecurity.pdf> (Accessed 8 June 2017)

Almeida, V.A., Doneda, D., Monteiro, M. (July-August 2015). Governance Challenges for the Internet of Things. *IEEE Internet Computing*, *19*(4), 56-59.

Beilinson, Jerry. (2016) 'Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds', *Consumer Reports*, (July 28, 2016). Available at: <http://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/> (accessed 30 June 2017).

Bennett, Colin J.(1992) *Regulating Privacy: Data Protection And Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Blaine, S. (2016) *Are wearable devices at work magic or a menace? Business Day Live* (2016), online: http://www.bdlive.co.za/business/innovation/2016/06/28/are-wearable-devices-at-work-magic-or-a-menace and <http://www.pressreader.com/south-africa/business-day/20160628/281719793889732> (Accessed 30 June 2017).

Bonderud, Douglas "The Ashley Madison Security Breach: An Affair to Remember?" *Security Intelligence*. (Aug 25. 2015). online:<https://securityintelligence.com/news/the-ashley-madison-security-breach-an-affair-to-remember> (Accessed 30 June 2017).

Brandon, John (2016). Security concerns rising for Internet of Things devices [WWW Document]. CSO Online. URL http://www.csoonline.com/article/3077537/internet-of-things/security-concerns-rising-for-internet-of-things-devices.html (Accessed 30 June 2017).

Brandon, Russell. *Apple's new facial recognition feature could spur legal issues | The Verge* (June 16, 2016),. online: http://www.theverge.com/2016/6/16/11934456/apple-google-facial-recognition-photos-privacy-faceprint (Accessed 30 June 2017).

BusinessWire. "Survey: Nearly Half of U.S. Firms Using Internet of Things Hit by Security Breaches" (June 1, 2017), online: <http://www.businesswire.com/news/home/20170601006165/en> (Accessed 30 June 2017).

Cameron, Alex and Mimi Palmer (Oct 2009) Invasion of Privacy as a Common Law Tort in Canada. *Canadian Privacy Law Review* 6(11) pp 105-117.

Chandler, J. (2008). Negligence Liability for Breaches of Data Security. *Banking and Finance Law Review*, 23(2), 223-273.

Cisco Systems. "Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing" (May 23, 2017), online: <http://www.marketwired.com/press-release/cisco-survey-reveals-close-to-three-fourths-of-iot-projects-are-failing-nasdaq-csco-2217795.htm> (Accessed: 30 June 2017).

Constantin, L., 2017. IoT malware starts showing destructive behavior [WWW Document]. CIO. URL http://www.cio.com/article/3188321/security/iot-malware-starts-showing-destructive-behavior.html (Accessed: 30 June 2017).

Crist, Ry. "Hackers find security weaknesses with the Lifx smart LED" *C/Net* (July 7, 2014), online: <https://www.cnet.com/news/hackers-discover-security-weaknesses-within-the-lifx-smart-led/> (Accessed 30 June 2017).

CyberLex. 2015. *The Internet of Things: Guidance, Regulation and the Canadian Approach* [WWW Document], 2015 online: <http://www.canadiancybersecuritylaw.com/2015/11/the-internet-of-things-guidance-regulation-and-the-canadian-approach/ (accessed 30 June 2017).

Duhigg, C. (2012) 'How Companies Learn Your Secrets', *The New York Times*, (February 16, 2012), online: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (Accessed 30 June 2017).

Ellul, Jacques.(1964). *Technological Society* (trans. by John Wilkinson). (New York: Vintage Books).

Ernst and Young (March 2015) "Cybersecurity and the Internet of Things" online: <http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf (Accessed 1 June 2017)

Felten, Ed. "Does Hashing Make Data 'Anonymous'"? *Tech@FTC* (April 22, 2012) online: <https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous> (Accessed 30 June 2017).

de Freytas-Tamura, Kimoko. Maker of 'Smart' Vibrators Settles Data Collection Lawsuit for $3.75 Million. *The New York Times.*(March 14, 2017), online: <https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html> (accessed 30 June 2017).

de Freytas-Tamura, Kimoko 2017b. The Bright-Eyed Talking Doll That Just Might Be a Spy. The New York Times. (Feb 17, 2017), online: <https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.htm>l (Accessed 30 June 2017)

Future of Privacy Forum. *A Visual Guide to Practical De-Identification* (April 25, 2016), online: <https://fpf.org/issues/deid/>. (accessed 30 June 2017).

Gandy, Oscar H. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO. Westview Press, 1993)

Gemalto Inc. (2017). Breach Level Index. online: <http://www.breachlevelindex.com/> (accessed 30 June 2017).

Goodin, Dan, 2017. Rash of in-the-wild attacks permanently destroys poorly secured IoT devices [WWW Document]. *Ars Technica.* online: <https://arstechnica.com/security/2017/04/rash-of-in-the-wild-attacks-permanently-destroys-poorly-secured-iot-devices/> (accessed 30 June 2017).

Gregory, John. 2017 Further Legal Snapshots From the Internet of Things. *Slaw* (May 17, 2017), online:<http://www.slaw.ca/2017/05/17/further-legal-snapshots-from-the-internet-of-things/> (Accessed: 30 June 2017).

Hesseldahl, A. (2015) *A Hacker's-Eye View of the Internet of Things, Recode*. Online:: http://www.recode.net/2015/4/7/11561182/a-hackers-eye-view-of-the-internet-of-things (Accessed: 30 June 2017).

Hewlett-Packard Development Co. (2015). HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems. *HP News* (February 10, 2015), online: http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050 (Accessed 30 June 2017)

Hill, Kashmir. *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, *Forbes* (February 16, 2012), online: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did (accessed 30 June 2017).

Hilts, Andrew, Christoph Parsons. and Jeffrey Knockel. *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security* (2016),online: <https://openeffect.ca/reports/Every_Step_You_Fake.pdf> (Accessed 30 June 2017).

Hotz, R. L. Metadata Can Expose Person's Identity Even Without Name. *Wall Street Journal.* (2015,Jan 29), online: < https://www.wsj.com/articles/metadata-can-expose-persons-identity-even-when-name-isnt-1422558349

Joseph, R. 2017. My Friend Cayla: the doll for children accused of "illegal espionage" - National | Globalnews.ca online: <http://globalnews.ca/news/3258509/my-friend-cayla-doll-illegal-espionage/> (Accessed: 30 June 2017).

Kinney, Sean. (2017) "The internet of things is an octopus…" *Enterprise IoT Insights* (May 9, 2017), online: < http://enterpriseiotinsights.com/20170509/internet-of-things/20170509internet-of-thingsinternet-of-things-octopus-tag17> (Accessed 30 June 2017).

La Diega, Guido Noto. 'Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom' (2016) 9 *Journal of Law and Economic Regulation* 69.

Liu, Kuan-lin (2017) "'IoT is an octopus … and we are everything except the suckers': Dell VP" The *China Post* (June 1, 2017), online: <http://www.chinapost.com.tw/taiwan/business/2017/06/01/498157/iot-is.htm> (accessed 30 June 2017).

Lyon, David. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis, MN: University of Minneapolis Press. 1994).

Manwaring, Kayleen. (2017) Emerging Information Technologies: Challenges for Consumers *Oxford University Commonwealth Law Journal* (2017) Vol. 17 (Forthcoming) UNSW Law Research Paper No. 25

Manwaring. Kayleen and Roger Clarke. (2015) 'Surfing the Third Wave of Computing: A Framework for Research into Networked eObjects' 31 *Computer Law & Security Review* 586.

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy.* Retrieved from http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies> (Accessed: 30 June 2017).

Masse, M & P. Beaudry. "The CRTC is not ready for the Internet of Things" *Globe and Mail* (May 22, 2017), online: <https://www.theglobeandmail.com/report-on-business/rob-commentary/the-crtc-is-not-ready-for-the-internet-of-things/article35078149 (Accessed: 30 June 2017).

McAfee Labs. (2016). McAfee Labs: 2017 Threats Predictions [pdf document]. Retrieved from https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf (accessed 30 June 2017).

McCandless, D. "World's Biggest Data Breaches & Hacks" *Information is Beautiful*. (updated April 25, 2017) , online:<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/> (Accessed: 30 June 2017).

McClelland, Calum (2017) "What is IoT? A Simple Explanation of the Internet of Things" *IoT for all* (May 30, 2017) https://iot-for-all.com/what-is-iot-simple-explanation/ (accessed 30 June 2017)

McLellan, Calum."How hackers attacked Ukraine's power grid: Implications for Industrial IoT security". *ZDNet*.(March 4, 2016), online: <http://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security> (Accessed: 30 June 2017).

Miller, Arthur R. (1971). *The Assault on Privacy: Computers, Data Banks, and Dossiers.* Ann Arbor: University of Michigan Press.

Misra, S., Maheswaran, M., Hashmi, S. (2017). *Security Challenges and Approaches in Internet of Things*. Switzerland: Springer International Publishing.

Nayak, D. (2016) *Amazon's Alexa Can Now Lock Doors With Voice Commands Androidheadlines.com, AndroidHeadlines.com*. (July 30, 2016), online: <http://www.androidheadlines.com/2016/07/amazons-alexa-can-now-lock-doors-voice-commands.html> (Accessed: 30 June 2017).

Nichols, Shaun. "Sons of IoT: Bikers hack Jeeps in auto theft spree *The Register* (May 31, 2017) https://www.theregister.co.uk/2017/05/31/bikers_hack_jeeps_in_auto_theft_spree/ (accessed 30 June 2017).

O'Brien, Ciara (2017) "Keep tabs on your kids with this wearable tracker" *The Irish Times* http://www.irishtimes.com/business/technology/keep-tabs-on-your-kids-with-this-wearable-tracker-1.3097803 (Accessed 30 June 2017).

Orcutt, M. (2016, July 22). Connected Toys are Raising Complicated New Privacy Questions. MIT Technology Review. https://www.technologyreview.com/s/601942/connected-toys-are-raising-complicated-new-privacy-questions/ (Accessed: 30 June 2017).

Osborne, Charlie. (2015, August 6). Critical IoT security flaw leaves connected home devices vulnerable. ZDNET. Retrieved from http://www.zdnet.com/article/critical-security-flaws-leave-connected-home-devices-vulnerable/ (Accessed: 30 June 2017).

OWASP Internet of Things Project - OWASP [WWW Document], n.d. URL https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project (Accessed 30 June 2017).

Palmer, Danny (2017) "The Internet of Things? It's really a giant robot and we don't know how to fix it" ZD Net (June 8, 2017), online: < http://www.zdnet.com/article/the-internet-of-things-its-really-a-giant-robot-and-we-dont-know-how-to-fix-it/> (Accessed 30 June 2017).

Pew Research Center (June 2017) "The Internet of Things Connectivity Binge: What are the Implications?" Available at: <http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/> (Accessed 30 June 2017).

Polenetsky, Jules. "Protecting privacy and promoting inclusion with the 'Internet of Things'" Available at:< http://thehill.com/blogs/pundits-blog/technology/285962-protecting-privacy-and-promoting-inclusion-with-the-internet-of > June 29, 2016 (Accessed 30 June 2017).

Polenetsky, Jules. "Kids, Connected Toys and Devices, and Privacy" (2016) *Future of Privacy Forum*. Available at: <https://fpf.org/2016/07/20/kids-connected-toys-devices-privacy/> (Accessed 30 June 2017).

Privacy Rights Clearinghouse | Data Breaches online: <https://www.privacyrights.org/data-breaches> (Accessed 30 June 2017).

Public Interest Advocacy Center. (2017) Shopping for Consumer Protection: Current Jurisdictional Issues (April 2017), online: <https://www.piac.ca/wp-content/uploads/2014/11/shopping_for_consumer_protection.pdf>.

Prosser, William L. (1960) Privacy, 48 *California Law Review*. 383.

Rhodes, Andy.(2017) "IoT is evolving like an octopus" Smart Industry (June 5, 2017) , online: <https://www.smartindustry.com/blog/smart-industry-connect/iot-is-evolving-like-an-octopus/> (Accessed 30 June 2017).

Richarz, Allan. (2014). "Near-field Communication Technology: Regulatory and Legal Recommendations for Embracing the NFC Revolution" *Canadian Journal of Law and Technology, 12(1),* 27-50.

Schneier, Bruce. The Internet of Things Is Wildly Insecure — And Often Unpatchable. *Wired*. (2014, Jan. 6), online: <https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/> (Accessed: 30 June 2017). "These embedded computers are riddled with vulnerabilities, and there's no good way to patch them."

Scully, Matt. "Big Data Tells Mortgage Traders an Amazing Amount About You" *Bloomberg Markets* (June 29, 2017), online: <https://www.bloomberg.com/news/articles/2017-06-29/big-data-can-tell-mortgage-traders-an-amazing-amount-about-you>. (Accessed 30 June 2017).

Seals, Tara. "Data Wiping Malware Takes Aim at IoT Devices" *Info Security Magazine* (May 23, 2017) https://www.infosecurity-magazine.com/news/datawiping-malware-takes-aim-at/ (Accessed 30 June 2017). "IoT devices are handy additions for botnets—easily enslaved and, because they lead an existence that tends to be free of human interaction, can be compromised without notice for long periods of time."

Smith, Ms. "Researchers exploit ZigBee security flaws that compromise security of smart homes" *CSO Online* (August 15, 2015), online: <http://www.csoonline.com/article/2969402/microsoft-subnet/researchers-exploit-zigbee-security-flaws-that-compromise-security-of-smart-homes.html> (Accessed 30 June 2017).

Smith, Ms. "500,000 Belkin WeMo users could be hacked; CERT issues advisory" *CSO Online* (Feb 28, 2014), online: <http://www.csoonline.com/article/2226371/microsoft-subnet/500-000-belkin-wemo-users-could-be-hacked--cert-issues-advisory.html> (Accessed 30 June 2017).

Tene, Omar & Zanfir-Fortuna, Gabriela. "Chasing the Golden Goose: What is the Path to Effective Anonymization" Future of Privacy Forum (2017), online: <https://fpf.org/wp-content/uploads/2017/03/Chasing-the-Golden-Goose-Mar-27-2017.pdf>.

Thompson, K., and Mattalo, B. The Internet of Things: Guidance, Regulation and the Canadian Approach. (Nov 24, 2015) online: <http://www.canadiancybersecuritylaw.com/2015/11/the-internet-of-things-guidance-regulation-and-the-canadian-approach/> (Accessed: 30 June 2017).

Tode, Chantal. *Location tracking opt-out could land big blow to retail technology - Mobile Marketer - Legal/privacy* (no date). Available at: <http://www.mobilemarketer.com/cms/news/legal-privacy/17211.html> (Accessed: 30 June 2017).

Torstar News Service "Why Canadians are being left out of voice-activated tech trend" *Toronto Metro* (January 23, 2017) http://www.metronews.ca/life/technology/2017/01/23/why-canadians-being-left-behind-in-voice-activated-tech.html (Accessed 30 June 2017).

Trappe, W., Howard, R., Moore, R.S. (2016). Low-Energy Security: Limits and Opportunities in the Internet of Things. *IEEE Security and Privacy Magazine*.

Trosow, Samuel E., Tremblay, Scott and Weiss, Daniel. "Submission to the Office of the Privacy Commissioner of Canada: Consultation on Consent and Privacy" (August 2016), online: <https://samtrosow.files.wordpress.com/2016/08/consent-submission-to-the-opc.pdf> (Accessed: 30 June 2017)

Trosow, Samuel E., *Douez v Facebook: Implications for Canadian Information Policy* (presentation, July 2017), online:<http://ir.lib.uwo.ca/fimspres/48>.

Urbelis, A. (2017, May 14). WannaCrypt ransomware attack should make us wanna cry. *CNN*. Online: <http://www.cnn.com/2017/05/14/opinions/wannacrypt-attack-should-make-us-wanna-cry-about-vulnerability-urbelis/index.html> (Accessed: 30 June 2017)

Verizon (2016). State of the Market: Internet of Things 2016. Online: https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf (Accessed: 30 June 2017).

Wasser, L and Koczerginski, M. (2016). Cybersecurity and the Internet of Things. Online: http://www.mcmillan.ca/mobile/Cybersecurity-and-the-Internet-of-Things (Accessed: 30 June 2017).

Wasser, L., Palmay, F., Hill, R., & Koczerginski, M. (2016). Cybersecurity – The Legal Landscape in Canada. Online: <http://mcmillan.ca/Cybersecurity--The-Legal-Landscape-in-Canada> (Accessed: 30 June 2017).

Wilkinson, Kate. The Internet of Things could be worth $500 billion in Canada alone, 2014. . *Canadian Business* (March 6, 2014), online: <http://www.canadianbusiness.com/technology-news/cisco-toronto-internet-of-things/> (Accessed: 30 June 2017).

Zara, Christopher "Google Gets Sued Over Face Recognition, Joining Facebook And Shutterfly In Battle Over Biometric Privacy In Illinois" *International Business Times*. (March 14, 2016), online: <http://www.ibtimes.com/google-gets-sued-over-face-recognition-joining-facebook-shutterfly-battle-over-2330278 (Accessed: 30 June 2017).

Government Publications:

Office of the Privacy Commissioner of Canada. *Interpretation Bulletin: Form of Consent*. (2014) Available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_07_consent/ (Accessed 8 June 2017)

Office of the Privacy Commissioner of Canada. *Fact Sheet: Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts* (2004), online: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_26_e.asp> (Accessed 30 June 2017).

Office of the Privacy Commissioner of Canada. *Interpretation Bulletin: Personal Information* (October 2013), online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/ (Accessed: 4 June 2017).

Office of the Privacy Commissioner of Canada. *Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act 2016* (Prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada, 2016), online: <https://www.priv.gc.ca/media/1806/consent_201605_e.pdf> (Accessed 30 June 2017).

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* (Research paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada, 2016), online: <https://www.priv.gc.ca/media/1808/iot_201602_e.pdf> (Accessed 30 June 2017).

Office of the Privacy Commissioner of Canada. *The Digital Privacy Act and PIPEDA - of Canada* n.d. online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/legislation-related-to-pipeda/02_05_d_63_s4/ (Accessed 30 June 2017).

Office of the Privacy Commissioner of Canada. PIPEDA Report of Findings #2016-005: Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner n.d., Online: https://priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/ (accessed 30 June 2017).

Office of the Privacy Commissioner of Canada. Letter to the Standing Committee on Access to Information, Privacy and Ethics about the study of PIPEDA (Dec 2, 2016), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_161202/>.

United States. Certified Emergency Response Team. *Security Tip (ST04-015): Understanding Denial-of-Service Attacks.* (2013, Feb. 6), online: <https://www.us-cert.gov/ncas/tips/ST04-015> (Accessed: 30 June 2017)

United States. Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning *In the Matter of The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*. (June 2, 2016), online: <https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf> (Accessed: 30 June 2017).

United States. Federal Trade Commission Bureau of Consumer Protection and Office of Policy Planning. *In the Matter of The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*. (June 2, 2016), online: <https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf> (Accessed: 30 June 2017)

Statutes:

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) <http://laws-lois.justice.gc.ca/eng/acts/P-8.6>./

Cases:

Douez v. Facebook, Inc., 2017 SCC 33 (CanLII), online: <http://canlii.ca/t/h4g1b>.

Englander v. Telus Communications Inc. (2004). online: <http://canlii.ca/t/1j6r7>.

Jones v Tsige, 2012 ONCA 32. <http://canlii.ca/t/fpnld>

Saumur c. Avid Life Media Inc., 2016.

Wansink v. TELUS Communications Inc. 2007 FCA 21.

Zuckerman c. Target Corporation, 2017.

Office of the Privacy Commissioner. PIPEDA Report of Findings # 2013-017 (2013). *Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising* Available at: http://canlii.ca/t/g90wl (Accessed June 30 2017)