SAGESSE

ISSN 2560-7014

Smart wearables and Canadian Privacy: Consumer concerns and participation in the ecosystem of the Internet of Things (IoT)

by Emily Speight

From smart cars to smart clothing, the Internet of Things (IoT) has the potential to revolutionize the way we live. Smart City IoT initiatives are facilitating more efficient traffic flows for commuters, and enabling bike sharing programs to reduce emissions and improve quality of life (Vinke). IoT solutions are redefining the aging experience by allowing individuals to remain independent in their homes longer. Voice activated Smart Home technologies provide solutions that remove barriers for individuals with mobility impairment; tasks such as shopping, manipulating window blinds and adjusting a thermostat can be achieved by issuing a voice command (AgingInPlace.org). Smart Wearables technologies provide means for healthier living; bras and shirts made from smart textiles can monitor blood pressure and heart functioning (electrocardiogram monitoring), providing insight for self-quantification (Awazade). Despite the potential of IoT technology, Canadians have been hesitant to adopt the technology and those that do often abandon the technology. This paper will examine resistance to IoT technology defined by Perera et al. as “smart wearable” and discuss measures to improve consumer engagement.

While abstract concepts of IoT are translated into technologies that impact daily life, defining IoT remains a challenge. The Internet of Things has been defined in numerous ways.

According to Perera et al. the Internet of Things is “a network of networks where, typically, a massive number of objects/things/sensors/devices are connected through communications and information infrastructure to provide value-added services” (585). Tzafestas describes the Internet of Things as “things/objects in our environment being connected so as to provide homogeneous communication and contextual services” (98). A central theme regularly underlying the various descriptions and definitions is the connection of everyday objects to the internet using sensors. IoT technology is pervasive and facilitates discreet, passive collection of mass amounts of data, which may be used to improve the lives of humans (Perera et al. 585). Smart wearables, simply put, are electronic, sensing technological devices worn on – or implanted into - the human body. Some examples of smart wearables available today include rings that track physical activity and provide the wearer with customized alerts for phone notifications; socks that measure pressure distribution on feet; watches that allow the wearer to track physical activity and perform functions normally associated with smartphones, such as sending and receiving SMS text messages; and armbands that track the wearer’s heart rate.

The Ecosystem of IoT

The IoT is expanding rapidly. Gartner predicts that by the year 2020 up to 30 billion devices will be connected as part of a 1.9 trillion-dollar industry (Gartner). Amidst the hype, it is interesting to note that adoption rates of IoT technology are low and attrition rates among users of IoT technologies are high (Garg 1). Garg describes an “ecosystem of IoT” that is composed of connected devices, the data generated by these devices, and stakeholders. The stakeholders involved in this ecosystem of IoT include “people/users, organizations and regulators” (2). Garg argues that only when the needs of stakeholders are met can the ecosystem of IoT function at its highest capacity; failure to meet these needs results in

disengaged stakeholders and erodes the IoT ecosystem (3). The high rate of user abandonment of IoT technologies suggests that in the current environment consumer needs are not being fully realized. Analysis of user requirements is challenging given the broad range of applications that functions within the IoT ecosystem.

Consumer Concerns Regarding IoT

Canadian consumers have a number of concerns regarding smart wearables. User design is important as consumers need to understand the technology and be comfortable operating appropriate hardware and software, such as smartphones and mobile apps (Puri v). The technology must be convenient for the consumer, with low impact on the consumer's day-to-day life. Wearables that are unfashionable or cannot be worn discreetly are less likely to be adopted, as well as wearables that require significant effort to maintain due to short battery life or other design weaknesses (Emrich). Cost and value both play a role in adoption and use, IoT technology must be affordable for entry and must offer long term value for maintaining consumer use (Emrich).

Value provided to the consumer is impacted in a variety of ways. In some instances, IoT technology may cause more harm than benefit. The Owlet Baby Care "smart sock," technology which monitors infant vital signs has been the subject of criticism. Doctors report that frequent false alarms by these devices have resulted in increased stress levels for parents, additional strain on the medical system and even unnecessary testing being performed on infants (Thompson). Similar concerns regarding data quality and the impact of false positives are reported on other smart wearable devices such as the Apple Watch (McGrath). Concerns around the safety and adverse health effects of smart wearables also brings forth questions

regarding the level of value provided versus the risk of smart wearables (Physicians for Safe Technology).

The most commonly cited deterrent to smart wearables is privacy concerns. According to Kerr et al. privacy and security are the foremost concerns of consumers regarding the use of smart wearables (1068). Research by Epstein et al. on consumer abandonment of smart wearable devices revealed privacy considerations as the most prevalent reason for desertion (1111). In fact, Epstein et al. found that 45.2% of the time privacy concerns were cited as driving consumer decisions to abandon smart wearables. The concerns were multi-faceted. Consumers were uncomfortable with location tracking that revealed their movements to others and objected to selling their information to third parties for advertising purposes (1110).

Consumer apprehension regarding the collection of data by smart wearables is not without merit. The data captured by smart wearables can be very personal. Consider the example of smart underwear made from smart fabric that tracks and measures levels of urinary leakage. The smart underwear currently can be used in the treatment of incontinence and is expected to have future applications in monitoring fertility and diabetes (Brusco). The Office of the Privacy Commissioner of Canada (OPC) recognizes the human body as "the vessel of our most intimate personal information" (Office of the Privacy Commission of Canada [OPC], "The Strategic Privacy Priorities"). In recent years, advancements in smart wearables have allowed the integration of biotechnology to collect consumer health data (Wissinger 779). Without adequate assurances and practices in place to protect such highly personal data and information, consumers will remain hesitant to participate in the ecosystem of IoT. Robust privacy legislation is a necessary ingredient for an effective ecosystem of IoT.

Privacy Challenges

Many nations are currently grappling to balance privacy with other competing interests, such as the need for national security, the need to foster innovation, and the need to support research. The European Union (EU) recently updated its privacy legislation from the EU Data Protection Directive (EU Directive 95/45/E) to the General Data Protection Regulation (GDPR) which was enacted in May 2018. Canada has chosen to employ an omnibus approach to privacy. Privacy laws are enacted by the federal government and the provinces are given the choice to comply with the federal legislation or enact substantially similar provincial legislation. This approach ensures that all Canadians enjoy a certain standard of privacy protection. While Canada has legislation to address privacy in both the public and private-sector, this paper will focus solely on the private sector. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal legislation that governs how private-sector organizations are expected to manage personal information. Some provinces have elected to enact provincial privacy legislation governing the private sector; these laws provide protections that meet or exceed the protections mandated by PIPEDA. An examination of PIPEDA is informative about the general private-sector privacy environment as the legislation serves as a minimum standard of privacy protection in Canada. Canada appoints a Privacy Commissioner to the Office of the Privacy Commissioner of Canada (OPC), which is independent of the government and the Privacy Commissioner reports to Parliament. The role of the OPC is to oversee compliance with privacy legislation and advocate for privacy rights.

As an advocate for privacy rights, the Office of the Privacy Commissioner of Canada has consistently called for increased regulatory powers for the OPC and significant reforms to existing privacy legislation. The PIPEDA legislation was passed in 2000 in a digital and political

environment that was distinctly different than the one we face today. PIPEDA was enacted before the widespread emergence of technologies such as Web 2.0, biometric facial recognition software, artificial intelligence, big data, IoT, and cloud computing in everyday life. The legislation is dated and does not effectively address the challenges that technological advances have created for society. A recently enacted amendment to PIPEDA has legislated mandatory data breach reporting for companies that collect the personal information of Canadians in a commercial capacity. While this amendment brings a much-needed reform to the Act, Canada's privacy legislation is still in dire need of an update. Whether PIPEDA, in its current form, meets the requirements of "adequacy" of the recently enacted GDPR remains the subject of much debate.

PIPEDA broadly defines both personal information and personal health information. Personal information is defined as, "information about an identifiable individual" (PIPEDA 4) and personal health information is defined as:

(a) information concerning the physical or mental health of the individual;

(b) information concerning any health services provided to the individual;

(c) information concerning the donation by the individual of any body part or bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; information that is collected incidentally to the provision of health services to the individual (PIPEDA 3-4).

The broad definition employed by PIPEDA extends privacy protections to Canadians who chose to employ IoT technology. Further, the OPC has been very clear in its position that data collected by IoT technology, and specifically smart wearables, fit the definition of personal

information (OPC “Wearable Computing” 1; OPC “The Strategic Privacy Priorities” 2-4) and is protected under PIPEDA.

PIPEDA’s Fair Information Principles

Canada’s PIPEDA legislation is based on ten fair information principles that organizations subject to the legislation must follow namely: (a) accountability; (b) identifying purposes; (c) consent; (d) limiting collection; (e) limiting use, disclosure, and retention; (f) accuracy; (g) safeguards; (h) openness; (i) individual access; (j) challenging compliance (OPC “Fair Information Principles”).

a) Accountability

The principle of accountability places responsibility on businesses to comply with PIPEDA and requires that the organization, as well as any third-party partners with the organization, act in accordance with PIPEDA legislation (OPC, “Fair Information Principles”).

b) Identifying Purpose

The principle for identifying purpose asserts that consumers must be informed regarding the reason for the collection of their personal information either prior to or at the time of collection (OPC, “Fair Information Principles”).

c) Consent

The principle of consent requires that organizations obtain meaningful consent prior to the collection, use or disclosure of personal information (OPC “Fair Information Principles”).

d) Limiting Collection

The principle of limiting collection requires that businesses limit the collection of personal data to only what is required to fulfil the purposes identified to consumers (OPC "Fair Information Principles").

e) Limiting Use, Disclosure, and Retention

The principle of limiting use, disclosure, and retention obligates businesses to restrict the use and disclosure of personal data to only those purposes for which consent has been given. Personal data should not be retained after it is no longer required for legal reasons or identified purposes and should be destroyed in a secure manner (OPC "Fair Information Principles"). Personal information that is kept longer than required must be anonymized (OPC "The Internet of Things" 16).

f) Accuracy

The principle of accuracy necessitates businesses to take measures to ensure personal information is accurate and that procedures are established to allow consumers to have inaccurate information corrected (OPC "Fair Information Principles").

g) Safeguards

The principle of safeguards obligates businesses to take measures to protect personal information against loss and theft (OPC "Fair Information Principles").

h) Openness

The principle of openness allows consumers to challenge businesses regarding compliance with PIPEDA's fair information principles (OPC "Fair Information Principles").

i) Individual Access

The principle of individual access provides consumers with the right of access to their personal information. Consumers have a right to verify their personal information and have incorrect or incomplete information about them corrected. (OPC “Fair Information Principles”).

j) Challenging Compliance

The principle of challenging compliance allows consumers to challenge businesses regarding compliance with PIPEDA and the fair information principles. (OPC “Fair Information Principles”).

Identifying Purpose and Consent

A close relationship exists between the principles of identifying purpose and consent because meaningful consent necessitates that users be properly informed. Written notices are often employed to inform consumers regarding why their personal information is being collected and how their data will be used. Typically, written collection notices are vague, written in complex language and are overly lengthy which renders them of little value to consumers. Often consumers do not read the collection notices as the time investment required is significant. Cranor and McDonald estimated that to read all the privacy policies an American Internet user encounters each year would require an annual time investment of 201 hours (565). Reading collection notices is clearly excessively burdensome for consumers and, given the opacity of most collection notices, arguably provides little benefit. Consumers are left with a sense of confusion concerning what data are being collected, how data are being used and shared, and the impact on personal privacy. It is unsettling to consider that a decision to participate in the ecosystem of IoT requires consumers consent to risks and practices they do not understand.

Challenges regarding consent are further compounded by the egregious misappropriations of the principle of consent that sometimes occur. Research by Wissinger revealed attitudes of blatant disregard for consumer privacy protections that cited user consent as justification for negligence toward security and privacy obligations (781). Attitudes of apathy are incongruent with both the letter of the law and the spirit of PIPEDA; the OPC is clear in its position that consent does not remove PIPEDA imposed obligations to protect personal privacy and provide adequate safeguards. Clearly, the current approach to informing consumers and obtaining meaningful, informed consent is inadequate. Adding requirements to ensure clear, succinct, plain use language can provide some benefit in the pursuit to improve existing models for identifying purpose and consent; however, these changes would only be one facet of a comprehensive solution to current shortcomings.

While businesses may have been able to use opacity as a tool to conceal how consumer data were used in the past, potential secondary uses of personal data are gaining attention. Recent reports of Fitbit data being used in Canadian courts (Waggot and McCutchan) and American courts issuing subpoenas for Amazon Echo recordings (CBS Interactive Inc.) are shedding light on the issue that there are privacy issues associated with smart devices of all types, including wearables. The OPC acknowledges that notice (identifying purpose) and consent are areas of challenge in today's digital environment and has taken action to address these shortcomings (OPC "PIPEDA Fair Information Principle 3"). The OPC ("Wearable Computing") also notes that the current binary model which limits user choice to either opt-in completely or opt-out completely and consent is only collected once, is insufficient regarding smart wearable technology. The OPC has made several recommendations intended to address challenges associated with notice and consent such as personalized privacy options that can be controlled by the consumer (10).

The most significant challenges about notice and consent in the IoT ecosystem are the introduction of smart wearables, such as Lifelogging technologies, and voice activated technologies that are constantly "listening," that do not limit data collection to the individual wearing the device. Instead, these devices collect data from the environment surrounding the individual wearing the device. Current methods which were designed to provide notice, obtain consent, and address the other privacy principles with an individual at a single-point in time, are insufficient to protect the personal privacy of individuals who are in the environment of a consumer wearing these types of smart devices. Certainly, many individuals may wish to opt-out of their image being captured by a stranger's lifelogging technology, or intimate data from a conversation with friends being captured by one party's voice activated device. Questions clearly emerge regarding how to notify individuals that their personal information may be collected by another consumer's smart wearable. If a method is in place to notify the individual that their information may be collected by another consumer's smart wearable, how does an individual provide consent or opt-out? Who is responsible to ensure compliance with the Fair Information Principles and protect the privacy rights of individuals whose personal information is being collected by a consumer's wearable device?

Limiting Use

The value of data in the ecosystem of IoT and today's environment of "big data" cannot be overstated. Data have been referred to as "the new oil" (Pringle) and "the new gold" (Farkas 5). The potential for personal data to be used as a resource for revenue generation, and their significance in "improving" customer service through personalization, positions data as a highly valuable asset. Given the value of data, businesses have significant motivation to expend

efforts to justify increased data collection, rather than critically evaluating what data are truly needed. Voice activated technologies that are always "listening" demonstrate how expansive data collection can become. The OPC has already voiced concerns regarding the handling of data from voice activated devices and has stated that limitations must be put in place to ensure that private conversations are not being recorded and sent to company servers (OPC "The Internet of Things" 20). Decisions regarding acceptable collection should not be left to the sole discretion of private enterprise; frameworks and rules need to be in place to provide guidance regarding acceptable collection.

While PIPEDA also creates limitations about the retention of information, this too is another area where businesses and consumers often have conflicting interests. Although anonymization of data has been provided as an acceptable option which allows organizations to retain data longer than necessary, there are challenges surrounding the effectiveness of anonymization processes. In many instances, given the amount of data collected, it is possible to track the data back to the individual it pertains to (OPC "The Internet of Things" 16). For anonymization to be an acceptable alternative, processes must be in place that ensures that data cannot be re-identified to individuals.

Accuracy

Given the value of IoT collected data to both consumers and businesses, it could be easy to mistakenly assume that a discussion of data accuracy in the ecosystem of IoT would be superfluous. Accuracy is indeed a challenge with IoT devices where sensors collect vast amounts of data. Efforts to control costs of smart devices may necessitate the use of cheaper, less accurate sensors. Users have reported inaccurate data as a common reason for abandoning IoT wearables (Epstein et al. 1110). The lack of mechanisms to correct

inaccurately recorded sensor data creates a significant challenge to ensuring accurate data. Accuracy of data and the lack thereof, is especially concerning in the ecosystem of IoT where the personal data generated are analysed and used for various purposes which directly impact the individuals. Smart wearables are often used for diagnosis and decision-making in a medical context (OPC "Wearable Computing" 11), where accuracy is extremely important. The OPC also cites concerns regarding the impact of inaccurate notification on accuracy; if consumers are unaware of what data are being collected, they are not equipped to request the appropriate data collected in an effort to verify accuracy (OPC "The Internet of Things" 20).

Security, Safeguards, Accountability, and Openness

Security is a leading concern of consumers in the ecosystem of IoT. The importance of the safeguard principle cannot be overstated as failure to comply can result in devastating consequences. Many smart wearables play a role in maintaining health (pacemakers, implantable cardio-defibrillators, insulin pumps) that, if hacked, could be seriously detrimental and result in death. Unfortunately, the rush to get smart wearable devices to market quickly has come at the expense of security. A study conducted by HP (as cited in OPC "The Internet of Things") revealed that approximately 70% of IoT devices had security vulnerabilities, 70% of devices failed to use encryption for communications, and 60% did not use encryption for software updates (21). Security and safeguards must be implemented to ensure consumer confidence and continued participation.

On November 1, 2018, PIPEDA's mandatory breech reporting rules were enacted, which provide consumers with increased protections and may serve to motivate businesses to apply a more respectful attitude toward security. The principle of accountability complements the principle of safeguards and affords protections to consumers when data storage or

processing is outsourced, which is especially relevant in today's global economy. Furthermore, openness is essential for building consumer confidence as it provides an avenue for consumers to voice complaints. The OPC has called for an end to self-regulation in the private-sector regarding privacy and continues to request powers be given to the OPC to proactively ensure compliance ("Annual Report 2018" 2). "Trust but verify," was a central theme in the OPC's most recent annual report, which argues that the OPC should be granted the ability to inspect the privacy practices of private companies in a regulatory capacity, without the need of a formal complaint ("Annual Report 2018" 2). Equipping the OPC with greater powers would be beneficial in building consumer confidence, ensuring compliance, and demonstrate in a meaningful way that Canada is committed to privacy protection.

Daniel Therrien, the current Privacy Commissioner of Canada, has indicated that PIPEDA is too permissive in an era of IoT, and that the legislation allows companies excessive leeway to exploit personal information for company gain (OPC "Annual Report 2018" 2). Ann Cavoukian (as cited in Jones), former Information and Privacy Commissioner of Ontario, has argued that the business model that disregards privacy is becoming obsolete, and that privacy considerations are integral when designing processes, products, and technologies. While businesses may balk at the additional time and expense to build privacy and security protection into IoT solutions and business models, Cavoukian (as cited in Jones) has argued that privacy protection is good for business and can help businesses differentiate. As consumers are becoming increasingly aware of commercial abuses of personal data, they will likely re-assess the value they gain from their smart wearables versus the increased risk to their privacy. Businesses that have built-in privacy protection will have competitive advantage. Cavoukian (as cited in Privacy Analytics) argues that "data privacy is the minimal cost of doing good

business." The costs of ignoring security (data breaches) or having to build in privacy after the design phase can be staggering (as cited in Jones).

Data Ownership

Discussion around control of personal information and personal data bring forth questions of ownership. Canadians, as a group, have a low level of personal data awareness; they have a limited understanding of how their personal data may be used by third parties (International Institute of Communications 14). Confusion around data in the IoT ecosystem is not limited to Canadians. A survey of 465 American adults who employed the use of smart wearables to collect health data reported that approximately half of the individuals believed they "owned" the personal health data collected, and 30% believed that ownership was shared between them and the company that collected their data ("Survey Reveals Consumer Views" 13). Uncertainty regarding data ownership may in part be attributed to an absence of Canadian legislation that provides a property right in data (Scassa 16).

Canadian legislators have been deliberate in taking an approach that relies on existing laws such as copyright, confidential information, and personal information protection laws to protect interests around data rather than passing data ownership laws. Canada is not unique in its approach to data ownership. The United States of America and the EU have both taken similar approaches to data ownership, preferring to rely on existing property laws that intentionally exclude an ownership right in data (Farkas 15; Determann 55). Scassa and Farkas are both hesitant to recommend the creation of an ownership right in data and employ a cautious approach, recommending that existing property laws could be amended to address current shortcomings (17) (15). Determann, on the other hand, is hostile to the notion that data ownership would provide any benefit and lists several harms that such a law would precipitate

including “suffocat[ion] of free speech, information freedom, science, and technological progress” (55).

Determann’s concerns about an ownership right in data are not without merit. Providing a property right in data would clearly disadvantage one or more groups in the IoT ecosystem, which would serve as a deterrent and result in decreased stakeholder participation. Given that the majority of calls for a property right in data come from business and government, rather than consumers, it is unlikely that consumers would be advantaged, and smart wearable attrition rates would further increase. Data ownership rights would serve as a catalyst for decreased efficiency in the IoT ecosystem.

Data ownership rights should not be pursued as an avenue to improve consumer adoption and retention rates for smart wearable devices. Robust privacy legislation can address concerns around security, collection, consent, use and disclosure that are frequently raised around smart wearables. Canada’s existing PIPEDA legislation is currently inadequate to protect consumers in the IoT environment; however, amendments could be made to bring the legislation into alignment with the needs of today’s digital economy.

Conclusion

The IoT offers endless possibilities to improve daily life in society. Smart wearables provide solutions that can facilitate healthier living and independent lifestyles. Despite the advantages, consumer acquisition and retention of IoT products and services remain a challenge. Consumer demands for assurances of privacy and security must be met if the IoT ecosystem is to function effectively. Comprehensive privacy legislation can address consumer concerns and serve as a more effective solution than data ownership laws in creating an environment that fosters trust and consumer participation in today’s digital society.

Canada's PIPEDA legislation currently governs consumer privacy protection in the private sector; however, the legislation has become outdated and in its current form is inadequate to provide protections in today's digital society. Significant changes to the legislation are necessary to address the considerable advances in the capabilities of technology. As it is currently written, PIPEDA is quite permissive, and departures from the spirit of the Act by commercial companies further erode consumer confidence in the IoT ecosystem. Updating PIPEDA and granting authority to the OPC to take proactive measures to ensure compliance with the Act are essential to build and maintain trust with consumers. The EU has recently updated its privacy legislation to address the new digital environment and ensure continued consumer privacy protections, positioning it as a leader in data privacy. Canadian legislators must act swiftly to ensure Canadian competitiveness in the digital economy. While businesses may be concerned about the consequences of tighter privacy restrictions, they will ultimately benefit from increased user trust and the ability to use privacy as a differentiator. Robust privacy legislation will lay the necessary groundwork for gaining consumer confidence, increasing participation in the IoT ecosystem, and maximizing benefit to society.

Works Cited

AginginPlace.org (April 2019). “IoT and Seniors” *Aging In Place.* https://www.aginginplace.org/iot-and-seniors/ Accessed 16 April 2019.

Awazade, Shubham. “IoT in Intelligent Mobile Health Monitoring System By Smart Textile.” *Textile Mates: Your All Time Partner*. 11 March 2017. https://www.textilemates.com/iot-intelligent-mobile-health-monitoring-system-smart-textile/. Accessed 22 October 2018.

Brusco, Sam. (2015 October 22). “A Rather Attractive Solution to Urinary Incontinence.” *ECN*. https://www.ecnmag.com/blog/2015/10/rather-attractive-solution-urinary-incontinence

CBS Interactive Inc. “Judge Orders Amazon to Produce Echo Recordings in Double Murder Case.” *CBS News.* 12 November 2018. https://www.cbsnews.com/news/amazon-echo-judge-orders-company-produce-alexa-recordings-double-murder-case-2018-11-12/

Cranor, Lorrie Faith, and Aleecia M. McDonald. “The Cost of Reading Privacy Policies” *I/S: A Journal of Law and Policy for the Information Society,* vol. 4, no. 3, 2008, pp. 543-568. https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf?sequence=1

Determann, Lothar. “No One Owns Data.” *UC Hastings research paper,* no. 265, 14 February 2018, pp. 1-44. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123957. Accessed 9 November 2018.

Emrich, Tom. “Wearable Market in Canada Expected to Explode, IDC Canada Says.” *Betakit*. 3 June 2014. https://betakit.com/wearable-market-in-canada-expected-to-explode-idc-canada-says/ Accessed November 18, 2018.

Epstein, Daniel A., et al. “Beyond Abandonment to Next Steps: Understanding and Designing for Life After Personal Informatics Tool Use.” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 2016 May, pp. 1109-1113. https://doi.org/10.1145/2858036.2858045.

Farkas, Thomas J. “Data Created by the Internet of Things: The New Gold Without Ownership?” *Revista la Propiedad Inmaterial,* no. 23, 1 August 2017, pp. 5-17. http://dx.doi.org/10.18601/16571959.n23.01 Accessed 9 November 2018.

Garg, Radhika. “Open Data Privacy and Security Policy and its Influence on Embracing the Internet of Things.” *First Monday.* vol. 23, no. 5-7, 2018. http://firstmonday.org/ojs/index.php/fm/article/view/8166/7211 https://dx.doi.org/10.5210/fm.v23i5.8166

Gartner. “Gartner Says it’s the Beginning of a New Era: The Digital Industrial Economy.” *Gartner Press Release*, 7 October 2013. https://www.gartner.com/newsroom/id/2602817 . Accessed 24 October 2018.

International Institute of Communications. “Personal Data Management: The User’s Perspective.” *International Institute of Communications.* 2012*,* pp. 1-46. www.iicom.org/images/iic/themes/Qual_Report_pdm_final.pdf

Jones, Hessie. “Dr. Ann Cavoukian: Why Big Business Should Proactively Build for Privacy.” *Forbes*. 17 August 2018. https://www.forbes.com/sites/cognitiveworld/2018/08/17/ann-cavoukian-why-big-business-should-proactively-build-for-privacy/#7b302fae2e3d Accessed 21 November 2018.

Kerr, Don, et al. “Security, Privacy, and Ownership Issues with the use of Wearable Health Technologies.” *Wearable Technologies: Concepts, Methodologies, Tools, and Applications,* edited by M Khosrow-Pour et al., Information Resources Management Association (IRMA), 2018, pp. 1068-1083). https://doi.10.4018/978-1-5225-5484-4.ch048

McGrath, Jenny. “Lack of Regulation Means Wearables Aren’t Held Accountable for Health Claims.” *Digital Trends.* January 19, 2019. https://www.digitaltrends.com/wearables/wearable-devices-leading-to-over-diagnosis/ Accessed February 10, 2019.

Physicians For Safe Technology. “Wearable Wireless Devices.” Ca. 2018. Accessed November 10, 2018. https://mdsafetech.org/wearable-devices/

Office of the Privacy Commissioner of Canada (OPC). “Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act.” 2018. https://www.priv.gc.ca/media/4831/ar_201718_eng.pdf

Office of the Privacy Commissioner of Canada (OPC). “Fair Information Principles.” 9 January 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/ Accessed October 29, 2018.

Office of the Privacy Commissioner of Canada (OPC). “PIPEDA Fair Information Principle 3 – Consent.” 8 January 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/ Accessed October 24, 2018.

Office of the Privacy Commissioner of Canada (OPC). “The Internet of Things: An Introduction to Privacy Issues with a Focus on the Retail and Home Environment.” February 2016 https://www.priv.gc.ca/media/1808/iot_201602_e.pdf

Office of the Privacy Commissioner of Canada (OPC). “The Strategic Privacy Priorities.” 9 September 2016. https://priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/ Accessed November 2, 2018.

Office of the Privacy Commissioner of Canada (OPC). “Wearable Computing: Challenges and Opportunities for Privacy Protection.” 2014, pp. 1-21. https://www.priv.gc.ca/media/1799/wc_201401_e.pdf

Perera, Charith et al. “The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey.” *IEEE Transactions on Emerging Topics in Computing*, vol. 3 no. 4, 2015, pp. 585-598. https://doi.org/10.1109/TETC.2015.2390034

Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000b, c. 5, s. 2(1), pp. 3-4. Retrieved from https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf Accessed 24 October 2018.

Pringle, Ramona. “Data is the New Oil:” Your Personal Information is Now the World’s Most Valuable Commodity. *CBC News*, Technology & Science. 25 August 2017. https://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677. Accessed 20 October 2018.

Privacy Analytics. Embed Data Privacy Proactively to Win Big Time. 29 August 2018. https://privacy-analytics.com/de-id-university/embed-data-privacy-proactively-to-win-big-time/. Accessed 21 November 2018.

Puri, Arjun. “Acceptance and Usage of Smart Wearable Devices in Canadian Older Adults.” 2017. University of Waterloo. https://uwspace.uwaterloo.ca/bitstream/handle/10012/11861/Puri_Arjun.pdf?sequence=5 Accessed April 2, 2019.

Scassa, T. “Data Ownership.” *CIGI papers.* no. 187, 2018. https://www.mdpi.com/2624-6511/1/1/6/htm

Accessed 16 October 2018.

“Survey Reveals Consumer Views on Data Ownership.” *Journal of AHIMA,* vol. 85, no. 5, 2014, p. 13.

Thompson, Dennis. “Pediatricians Say No to Wearable Smartphone Baby Monitors.” *HealthDay News*. (24 January 2017). https://www.upi.com/Health_News/2017/01/24/Pediatricians-say-no-to-wearable-smartphone-baby-monitors/4181485293107/ Accessed November 10, 2018.

Tzafestas, Spyros G. “Ethics and Law in the Internet of Things World.” *Smart Cities,* vol. 1 no. 1, 2018, pp. 98-120. https://doi.org/10.3390/smartcities1010006 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251542

Vinke, Nikkie. “Smart Cities, Smart Transit: Bike Shares as Urban Transport Solution.” *Finch & Beak*. 6 Feb 2015. https://www.finchandbeak.com/1108/smart-cities-smart-transit-bike-shares.htm Accessed 14 January 2019.

Waggot, George and Wilson McCutchan. “Canada: Fitbit Evidence: Coming to a Court Near You.” *Mondaq.* 21 November 2014.

http://www.mondaq.com/canada/x/355492/employment+litigation+tribunals/Fitbit+Evidence+Coming+Soon+To+A+Court+Near+You Accessed 30 October 2018.

Wissinger, Elizabeth. "Blood, Sweat, and Tears: Navigating Creepy Versus Cool in Wearable Biotech." *Information, Communication & Society,* vol. 21, no. 5, 2018, pp. 779-785. https://doi.org/10.1080/1369118X.2018.1428657

Biographies

Emily Speight holds a CRM designation through the ICRM as well as a CIAPP-P designation through the CIAPP. She is currently working towards acquiring her Master's Degree in Information Management from Dalhousie University.

List of Abbreviations

EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	Personal Information Protection and Electronic Documents Act