mcmillan

Cybersecurity and the Internet of Things

Article reprinted from the May 2016, Volume 13, Number 6 issue of
Canadian Privacy Law Review

* This article was first published in Canadian Corporate Counsel, a Thomson Reuters Canada publication.

Canadian Privacy Law Review

Article reprinted from May 2016, Volume 13, Number 6 issue

• CYBERSECURITY AND THE INTERNET OF THINGS •

Lyndsay Wasser, Co-Chair Cybersecurity, Mitch Koczerginski, Associate,
and Rohan Hill, Associate, McMillan LLP

Lyndsay Wasser

Mitch Koczerginski

Rohan Hill

The "Internet of Things", commonly referred to as the "IoT", is a phrase that loosely describes the growing body of Internet-connected devices, gadgets, and other items that do not fit the traditional concept of a "computer". Examples of IoT device types include wearable technology (*e.g.*, health monitors), networked home appliances, IP security cameras, connected vehicles, environmental controls, smart watches, and even smart light bulbs. Homes and offices now frequently have an array of different devices and

device types simultaneously communicating with and exchanging data over the Internet.

Consumers and developers of IoT technology appear willing and anxious to add connectivity to almost anything with a logical reason to have it. Whether it involves Internet — enabling an existing class of item or appliance, or developing an entirely new category of device, it appears that the IoT is ushering in an era where a traditional computer no longer serves as the sole or even primary conduit for our interaction with the Internet.

Many commentators, as well as regulators in Canada, the United States and Europe, have noted that the IoT presents a number of challenges and concerns from a privacy law perspective. For example, the lack of user interface on many IoT devices, and automatic interaction between connected devices that is often invisible to users, makes it difficult to meet legal consent requirements. However, a thorough analysis of the privacy implications of the IoT is outside the scope of this paper.

From a cybersecurity perspective, the IoT presents a number of unique considerations, challenges and risks. This paper examines these issues in the context of the Canadian legal framework applicable to private sector organizations.

LEGAL OBLIGATIONS AND LIABILITY

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[1] governs protection of personal information in the course of commercial activities in all jurisdictions that do not have substantially similar legislation, as well as protection of personal information related to employees of federally-regulated organizations. Substantially similar legislation currently exists in Alberta, British Columbia and Quebec.[2]

Some may question the application of privacy legislation to IoT technology on the basis that the abstract information that a particular IoT device collects (*e.g.*, temperature in a house) does not easily fit within the concept of "personal" information, which is generally defined as information about an identifiable individual.[3] However, the Ontario Court of Appeal has found that "personal information" has an elastic definition and should be interpreted accordingly.[4] Further, by its nature, the IoT involves connectivity of a number of devices that each collects different types of information. When such information is combined, it can present a detailed profile of an individual's lifestyle, habits, health, etc., which would undoubtedly qualify as personal information. The Federal Privacy Commissioner recently observed that in the context of the IoT, "it is not enough to look at specific pieces of data in isolation, but rather one must also look at what the data can reveal."[5]

From a cybersecurity perspective, the most relevant statutory obligations applicable to IoT, under PIPEDA, are as follows:

- Personal information must be protected by security safeguards appropriate to the sensitivity of the information.[6]
- Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification, regardless of the format in which it is held.[7]
- 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.[8]

- The methods of protection should include (*a*) physical measures; (*b*) organizational measures; and (*c*) technological measures.[9]
- An organization continues to be responsible for personal information it handles, even where that information has been transferred to a third party for storage or processing, and contractual or other means must be used to ensure that comparable levels of protection exist while the information is being processed by the third party.[10]

In addition, when recent amendments to PIPEDA come into force, organizations will be obliged to maintain a record of any breach of security safeguards[11] involving personal information under their control, and notify the Office of the Privacy Commissioner of Canada and affected individuals of such a breach if it is reasonable to believe that it poses a "real risk of significant harm"[12] to the affected individuals.

As discussed in more detail below, these legal obligations present unique issues and challenges when applied to the IoT. Indeed, the Federal Privacy Commissioner has even questioned whether Canada's privacy law framework is presently compatible with the IoT.[13] For example, the Commissioner acknowledged the perception that the consent requirements and concept of personal information are outdated and overly simplistic in the IoT context.[14]

In addition to these statutory obligations, as discussed in our earlier article, "Cybersecurity – The Legal Landscape in Canada", privacy and data breaches have given rise to a large number of class action lawsuits in recent years, and the common law in this area continues to evolve.

In this regard, interesting questions arise regarding attribution of liability when an IoT device is involved. For example, when damages result from the functioning (or malfunctioning) of an IoT device, who is ultimately liable? Is the device's owner responsible? The manufacturer? What if a device fails while interacting with a cloud-based service provider, or a 3rd party application, or another IoT device?

It may not be practical for a developer to comprehensively test all possible IoT device interactions for compatibility issues. Where an IoT device causes harm on the basis of decisions or actions that were made or coordinated with other IoT devices, there may be challenges in determining questions of liability. Determining fault for incorrect dosing from a medication pump is more complex if the device makes decisions about dosage by first communicating with other connected devices to obtain health and environmental data. Determining fault for a traffic accident may be complicated by the fact that a connected vehicle reacts to communication from, for example, other connected vehicles, devices carried by pedestrians, or networked sensors.

Existing negligence, product liability and privacy laws may provide some guidance, but several issues will require novel consideration by the courts. Given the rise in privacy and data breach litigation in Canada, and the unsettled state of the law, it is likely that plaintiffs' lawyers will cast their nets widely when searching for liability for damages caused by IoT devices.

ENHANCED RISKS IN A CONNECTED WORLD

The legal obligations described above raise a number of unique considerations for IoT, including:

- Heightened risk of harm;
- Increased sensitivity of personal information;
- More vulnerabilities and difficulty of patching; and
- Vulnerabilities created by third parties.

Each of these issues is addressed in more detail below.

Heightened Risk of Harm

As indicated above, organizations are required to implement security safeguards to protect the personal information that they collect, use, store and disclose. The importance of such safeguards is amplified by the increase in adoption of IoT devices, the increase in

variety of device functions, and the related increase in responsibility that is being entrusted to such devices.

Early IoT devices may have handled relatively non-critical tasks, but as the pervasiveness of IoT technology has grown, these devices have increasingly been charged with more significant tasks, from tracking an individual's health, to piloting vehicles, and even monitoring the security and safety of property and infrastructure. While the evolution in IoT device capability promises many benefits to consumers and businesses, the greater responsibility and power delegated to IoT devices also creates a greater risk of negative privacy implications, injury, or property damage, if IoT devices fail, mishandle personal information or operate in an undesirable manner. A fitness tracker that fails to accurately record a user's daily step count may not trigger dire consequences, but a medical device that administers the wrong amount of insulin, an autonomous vehicle that malfunctions and causes an accident, or an e-wallet that inadvertently discloses an individual's banking information and transaction history, could have serious implications.

This heightened risk of harm suggests that more stringent security safeguards will be required for many IoT devices, in order for such devices to comply with legal obligations. Additional implications may arise when the new breach reporting requirements come into force under PIPEDA.

Increased Sensitivity of Personal Information

Organizations must also be aware that PIPEDA requires the application of more stringent security safeguards to protect personal information that is of a sensitive nature.

Some of the information that is collected by IoT devices is inherently sensitive, such as information about sleeping patterns, credit card information, or health and fitness data. In addition, even data that may seem non-sensitive in isolation may be rendered sensitive when combined with other sensitive or non-sensitive information. Past cases indicate that collecting a vast amount of personal information can render such information more sensitive.[15] The IoT allows personal information to be collected from a number of different devices, and the complete picture of an individual's life that can be gleaned from the aggregation of such data could reveal a more intimate picture of the individual than he or she ever intended to make known. This has both privacy and security implications, including potentially increasing the risks of identity theft.

Security measures for IoT devices will need to take into account the enhanced sensitivity of vast amounts of real-time information collected in a connected world.

More Vulnerabilities and Difficulty of Patching

Any device that connects to the Internet can potentially be compromised by malicious actors. Therefore, as the IoT becomes more prevalent, the number of vulnerabilities that can be exploited by the pool of increasingly sophisticated malicious actors will also continue to grow.

Of particular concern is that IoT devices are often designed by less experienced product developers, many of whom are not focusing upon security considerations. The rapid growth of interest in connected devices has attracted a great deal of attention to the IoT space, and various start-ups and crowd funding initiatives have formed for the purpose of creating single, freshman product offerings. While this may be seen as positive in terms of the health of the IoT industry, the degree of security expertise behind an IoT device may vary significantly depending on its origin and the team behind it.

In fact, in its recent report, "The Internet of Things. An introduction to privacy issues with a focus on the retail and home environments", the Office of the Privacy Commissioner of Canada cited research findings indicating that approximately 70% of IoT devices have vulnerabilities that could be exploited.[16] Such vulnerabilities included: "... 80% of devices, including cloud and mobile apps, failed to require strong passwords, 70% of devices did not encrypt communications, 60% lacked encryption for software updates and another 60% had insecure web interfaces."[17]

Another security challenge arises with respect to the provision of software updates that may be necessary to maintain and strengthen the security of an IoT device over time. While it is important for developers to ensure that a device continues to remain secure, their ability to access the device to install software updates may be limited in the IoT context. Canada's Anti-Spam Law ("CASL")[18] contains provisions governing software installation in the course of commercial activities. These provisions prohibit the installation of computer programs on another person's computer system without express consent. Given that an IoT device often does not contain an interface that allows communication between a device and the owner, developers must consider alternative ways to obtain express consent for the installation of software updates.

A lack of frequent updating is particularly problematic in the IoT context given the combination of (A) the high degree of responsibility that is increasingly entrusted to IoT devices, (B) the fact that these devices often have "always-on" IP connections to the Internet, and (C) the reality that there is a significant group of individuals and organizations tirelessly searching for exploits and vulnerabilities in any systems they can access on the Internet.

While users are largely accustomed to updating their computer or smartphone OS, it remains to be seen how amenable individuals will be to adopting a similar practice for connected light bulbs, coffee makers, thermostats, deadbolts, fitness monitors, and other IoT devices. Some IoT devices may even lack practical security update and patching mechanisms, may lack interfaces as discussed above, or may ultimately be abandoned by their original developers (*e.g.*, because they are too expensive to maintain or because a start-up business fails and the developer is no longer operating). The lack of an interface also creates a risk that security credentials on IoT devices will be less frequently changed from their defaults.

Since IoT devices will often use customized software or firmware, if the developer is not diligent in issuing updates, the user may be unable to correct security deficiencies. This challenge is exacerbated by the fact that while a computer OS will often have a relatively short deployed lifespan thanks to Moore's law and the fast obsolescence of traditional computer hardware, IoT devices that are integrated into homes, vehicles, or businesses, may be deployed for comparatively long periods of time before replacement. In other words, although many people may replace their laptop computer every few years, very few people are in the habit of regularly replacing their deadbolts.

Vulnerabilities Created by Third Parties

While the integration of IoT devices into day-to-day life offers exciting benefits, reliance on this technology also requires placing a tremendous amount of trust in both the device's embedded cybersecurity systems and the security safeguards of devices developed by third parties with which they interact. IoT devices often interact with third-party and cloud service providers, and are increasingly interacting with each other. When multiple devices are connected, there is a risk that a weak link in any of them can be exploited to compromise them all.

Furthermore, while loss of privacy, injury or property damage may result solely from the failure of an IoT device, in other cases it may result from a combination of IoT device vulnerabilities and the intentional malicious exploitation by a third party. In 2015, various media reported on demonstrations conducted by attackers who were purportedly able to disable brakes and interfere with steering on Internet connected vehicles.[19] Other media have reported on security experts being able to hack into a secured wireless network through "smart" light bulbs.[20] While there has been debate about the practicality of specific exploits, it is reasonable to expect that an expanding base of Internet integrated devices will attract an expanding base of individuals looking to exploit those systems for nefarious purposes.

In a recent statement to the United States Senate Armed Services Committee, James Clapper, the US director of national intelligence, advised that in the future, intelligence services might utilize IoT devices for identification, surveillance, monitoring, location tracking, recruitment targeting and gaining access to networks or user credentials.[21]

While less dramatic than the examples above, malicious attackers may also utilize vulnerabilities in IoT devices as vectors for network intrusion to either gain benefit from access to the network itself or to leverage the network or an IoT device's Internet connection as a tool for launching other disruptive activities such as distributed denial of service ("DDoS") attacks, or the distribution of spam.

Organizations entering the IoT space should understand the vulnerabilities at play and consider how they can reduce associated risks.

REDUCING THE RISKS

Given the legal obligations, risks, and uncertainty of liability described above, organizations should seriously consider the cybersecurity implications of the IoT.

In particular, organizations that are developing IoT devices should consider cybersecurity issues from the outset, and build security into the design and development of the product, including by:

- Conducting a security risk assessment or threat impact assessment early in the process;
- Evaluating applicable legal requirements and restrictions, such as those set out in PIPEDA and CASL (*e.g.*, CASL requirements applicable to updates as well as specific notice and consent requirements under CASL when a program causes a computer system to communicate with another computer system);
- Considering how the device will interact with other IoT devices, and options to reduce associated risks;
- Testing security measures before products are launched;
- Considering how patches and updates will handled; and
- Taking steps to confirm/ensure that any partners and services providers are appropriately addressing security issues and legal requirements, including implementing appropriate contractual arrangements.

Although privacy implications of the IoT are outside the scope of this article, developers would also be well-advised to conduct a privacy impact assessment to consider the privacy implications of their product(s) and ways to reduce privacy-related risks. In particular, some privacy principles intersect with cybersecurity considerations. For example, the data minimization principle can be applied to reduce risk. If an organization limits its collection of personal information to only what it needs in the circumstances, and disposes of such information (securely) once it is no longer required, this will minimize the amount of information that is available to malicious actors in the event of a data breach.

Building security and privacy into the design of IoT products from the outset can improve functionality and decrease costs, as well as maximizing compliance with legal requirements.

Organizations that are considering integrating IoT devices into their business should ensure that they:

- Understand potential security implications, including by conducting a security risk assessment or threat impact assessment;
- Take steps to reduce and mitigate risks, such as isolating IoT devices from systems containing highly confidential or sensitive information, where appropriate;
- Make inquiries of product developers and distributors, to ensure security has been built into the design of the products and appropriate patches and updates will be available, as necessary, and obtain contractual commitments to the foregoing, where possible;
- Ensure that auditing and analytical tools are in place to monitor for breaches of IoT devices, and that known vulnerabilities are patched in a timely manner;
- Consider impact on bandwidth, as this can affect business continuity;
- Conduct a privacy impact assessment, and also review privacy policies and procedures to determine if updates will be required.

The measures described above are not intended to be all-inclusive, but provide a good starting point when considering the cybersecurity implications of

the IoT. In its recent staff report, "Internet of Things: Privacy & Security in a Connected World", the Federal Trade Commission provides additional guidance on steps that organizations can take to address privacy and security issues related to the IoT.[22]

Conclusion

While some of the risks discussed above are not strictly unique to the IoT, many are exacerbated by the nature of IoT technology and the recent dramatic influx of participants into the IoT device space.

By their nature, IoT devices are often deployed in a diverse range of physical environments. It may not be possible for product developers to anticipate or comprehensively test IoT devices across all potential operating environments. Similarly, the "soft environment" may be equally difficult to completely anticipate and test for incompatibilities, as IoT devices may ultimately end up interacting with applications, cloud service providers, and other IoT devices in a manner that the designers did not anticipate.

The IoT space offers unprecedented connectivity. However, the significant trust afforded to these devices also introduces an unprecedented vulnerability to various harms in the event of technical device failures or mishandling of personal information. This article has explored some of the risks associated with the operation of IoT technology and certain requirements pertaining to the security of personal information generated by these devices. In the flurry to develop devices that operate in this space, developers ought to conduct an analysis of surrounding vulnerabilities and applicable obligations. In addition, it is important for organizations to carefully consider the implications of deploying these devices in connection with their businesses.

This article was first published in Canadian Corporate Counsel, a Thomson Reuters Canada publication.

[***Lyndsay Wasser*** *is the Co-Chair of McMillan's Privacy & Data Protection Group and its Cybersecurity Group. She is a Certified Information Privacy Professional/Canada, and regularly advises and assists clients on a broad range of privacy and cybersecurity issues, including advising on access requests, legal requirements related to data security, privacy breaches, workplace privacy issues, handling personal health information, CASL compliance, and transferring personal information across borders, as well as helping organizations to develop privacy compliance programs, privacy and social media policies, data sharing agreements and consent forms. Lyndsay regularly writes and speaks on privacy-related topics, and is the co-author of Privacy in the Workplace, 3rd ed. and the Privacy chapter in the Ultimate Corporate Counsel Guide.*

Mitch Koczerginski *is an Associate in the Litigation and Dispute Resolution group in the firm's Toronto office. He is developing a broad practice in commercial litigation, privacy and data security law.*

Mitch has acted on appeals before the Information and Privacy Commissioner of Ontario with respect to freedom of information requests. He has also written on various issues at the cross section of privacy law and technology. While at law school, Mitch earned a designation in law and technology from University of Ottawa and completed an externship with the Canadian Internet Policy and Public Interest Clinic.

Rohan Hill *is a lawyer in McMillan's Vancouver office. Rohan is a member of the firm's Advocacy and Litigation group and has experience in a broad range of areas, including internet and technology, defamation, environmental regulation, administrative law, commercial disputes, cybersecurity, and cryptocurrency. Rohan has a strong interest in new and emerging technology*.]

---

1 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

2 Ontario's health sector privacy legislation has also been declared substantially similar to PIPEDA, but most of the restrictions and requirements only apply to health information custodians.

3 Barbara McIssac, Kris Klein, Rick Shields, *The Law Of Privacy In Canada*, (Toronto: Thomson Carswell, 2012) at 4.1-1.

[4] *Citi Cards Canada Inc. v. Pleasance*, [2011] O.J. No. 15, 2011 ONCA 3, 103 O.R. (3d) 241.

[5] See https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp.

[6] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1, Article 4.7.

[7] *Ibid.*, Article 4.7.1.

[8] *Ibid.*, Article 4.7.2.

[9] *Ibid.*, Article 4.7.3.

[10] *Ibid.*, Article 4.1.3.

[11] "Breach of security safeguards" means "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from failure to establish those safeguards". *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 2(1).

[12] Defined to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property". *Digital Privacy Act*, S.C. 2015, c. 32, s. 10.1(7).

[13] See https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp.

[14] See https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp.

[15] See PIPEDA Report of Findings #2015-001.

[16] See https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp.

[17] See https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.asp.

[18] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23.

[19] See http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[20] See http://www.computerweekly.com/news/2240224012/IoT-smart-light-bulbs-get-security-update.

[21] See http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

[22] See https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

About us

McMillan is a business law firm serving public, private and not-for-profit clients across key industries in Canada, the United States and internationally. With recognized expertise and acknowledged leadership in major business sectors, we provide solutions-oriented legal advice through our offices in Vancouver, Calgary, Toronto, Ottawa, Montréal and Hong Kong. Our firm values – respect, teamwork, commitment, client service and professional excellence – are at the heart of McMillan's commitment to serve our clients, our local communities and the legal profession.

Contacts

Frank Palmay, P.Eng.
Co-Chair, Financial Services Regulatory
and Cybersecurity
Toronto
416.307.4037
frank.palmay@mcmillan.ca

Lyndsay A. Wasser
Co-Chair, Privacy
& Data Protection Co-Chair, Cybersecurity
Toronto
416.865.7083
lyndsay.wasser@mcmillan.ca