BUSINESSCLASS
KNOWLEDGE ▪ SEMINARS ▪ INSIGHTS

Blakes

IoT: Minimizing Your Privacy and Security Risks in an Interconnected World

By Wendy Mee and Kristin Ali

Please see our practical steps for creating a safer and more privacy-protective IoT environment.

Your printer. The water cooler. The thermostat. What do these things have in common? All of them can be connected to the Internet of Things (IoT).

The IoT continued its meteoric rise in 2017 with a vast array of everyday devices joining networks around the world. Technology research company Gartner Inc. predicts there will be over 20 billion devices on the IoT by 2020, and intelligence firm International Data Corporation estimates that the Canadian IoT market will be worth more than US$4.9-billion in 2018.

The IoT is having, and will continue to have, a massive impact on how organizations across all industry sectors are doing business. Businesses that do not prepare their digital environments for the IoT are missing an opportunity to leverage the vast quantities of data generated by the IoT and exposing themselves to competitive threats from businesses that are embracing the IoT.

Cisco has calculated that by 2019, IoT devices will create over 500ZB of data. For context, one zettabyte is more than a trillion gigabytes. This big data provides opportunities for organizations to identify important patterns and insights through advanced analytics. This can help organizations analyze past performance and forecast future trends, which can in turn improve operational efficiencies and enhance corporate decision-making.

In the retail sector, for example, the combined data from IoT devices can present a detailed profile of a consumer's lifestyle, preferences and habits, allowing marketers to more effectively influence consumer decision-making and create more personalized consumer experiences. Further, consumers are increasingly demanding the convenience and functionality that IoT devices provide, which means organizations that do not capitalize on the IoT may lose consumers and business overall.

While the IoT is still in its early stages and businesses are grappling with how to derive meaningful content from the mass quantities of IoT-generated data, the IoT promises significant benefits for companies, which will benefit from having an IoT strategy.

Of course these benefits do not come without risks. Where big data collected from IoT devices is associated with an identified or identifiable user, it will constitute personal information and therefore any collection, use, disclosure or other processing of that data must comply with applicable privacy laws. This includes obtaining informed consent from the user, limiting collection, use and retention of personal information to what is reasonable and necessary, and providing users with rights of access, correction and the ability to withdraw consent, among other requirements.

Compliance with these requirements can be challenging in the IoT space. In particular, compliance with limiting collection and retention principles may impact the utility of data obtained from IoT devices. As privacy law principles only apply to personal information and will not apply to data that has been effectively de-identified, organizations wanting to obtain maximum value from big data should engage appropriate de-identification experts.

Canadian privacy laws also require that personal information be protected with safeguards that are appropriate, having regard to the sensitivity of the information. Even where the data collected by IoT devices is not inherently sensitive, the sheer volume of the information — which creates very detailed profiles of individual users — may mean that the data should be treated as highly sensitive and protected with commensurately robust security.

Big data is an attractive target for cyber criminals. As with any device connected to the Internet, IoT devices and networks can be hacked, and in an IoT environment where devices, applications and networks are interconnected, the attack surface is much larger.

IoT devices also pose unique challenges from a security perspective because many traditional security measures (such as those used to protect networks) often cannot be applied to IoT devices. Further, device security encompasses more than data security. With many devices — like connected cars, connected medical devices and connected home security systems — inadequate device security can also cause loss or theft of property as well as physical harm or even death.

These privacy and security risks have not gone unnoticed by regulators. Regulators in Canada and the United States have issued warnings and guidance on privacy and security risks with IoT devices.

PRIVACY

Privacy concerns arising from the IoT have been a significant focus of the Office of the Privacy Commissioner of Canada (OPC). In its *2016-2017 Annual Report to Parliament on the* Personal Information Protection and Electronic Documents Act *and the* Privacy Act, the OPC identified IoT, big data, connected cars and smart homes as some of the topics where additional or updated guidance would be issued.

This will add to the work that the OPC has already done in this space. In 2016, the OPC participated in the Global Privacy Enforcement Network's sweep of IoT devices. The OPC's focus was on connected health devices, such as fitness trackers, thermometers and heart monitors. A key issue identified by the sweep was the lack of effective privacy communications. The OPC found that even though the devices swept were collecting a great deal of sensitive

data, the privacy communications were generic and did not adequately inform users about what personal information was actually being collected by the device and how it would be used.

Commissioner Daniel Therrien said: "With the proliferation of the Internet of Things, the activities, movements, behaviours and preferences of individuals are being measured, recorded and analyzed on an increasingly regular basis. As this technology expands, it is imperative that companies do a better job of explaining their personal information handling practices."

Other issues identified included lack of information about how information would be stored, lack of clear instructions on how to delete data and instances where more personal information was required to be provided than reasonably necessary given the function of the device. However, on a positive note, the OPC was pleased to see a number of devices providing real-time notice of the collection of certain data elements.

SECURITY

Cyber-attacks facilitated through poorly secured IoT devices have been making major headlines. Most notable was the Dyn Inc. attack in October 2016 in which criminal hackers launched a massive cyber-attack against major consumer websites by compromising hundreds of thousands of unsecured IoT devices. The hackers infected Internet-connected DVRs, webcams, and cameras with malware through vulnerabilities such as outdated and un-updatable firmware and default usernames and passwords, which were never changed by the end user. The hackers then ordered the infected IoT devices to attack the servers of Dyn, a company that controls much of the Internet's domain name system infrastructure. This was enough to shut down many major websites, including Twitter, Netflix, Spotify and Amazon. The cyber-attack on Dyn was not a black swan event. Stroz Friedberg, a leader in cybersecurity risk management, predicts that cyber-attacks on IoT devices will continue to be a major cyber threat.

In the U.S., the Federal Trade Commission (FTC) has urged manufacturers of IoT devices to protect consumers, both during the device life cycle and afterward, and issued detailed guidelines in its 2015 reports: *Internet of Things: Privacy & Security in a Connected World* and *Careful Connections: Building Security in the Internet of Things*.

In particular, the FTC recommended that manufacturers build security into devices at the outset; train employees about the importance of security; provide reasonable oversight of third-party providers' security practices; consider using multiple layers of security to defend against a particular risk; employ measures to keep unauthorized users from accessing a consumer's device, data or personal information stored on the network; monitor connected devices throughout their expected life cycle; and provide security patches where appropriate.

The U.S. Food & Drug Administration (FDA) is also concerned with IoT security as it relates to medical devices. In its 2016 report, *Postmarket Management of Cybersecurity in Medical Devices*, the FDA warned that hackers are "continuously" targeting medical devices and hospitals. Like the FTC, the FDA emphasized that manufacturers must consider cybersecurity of IoT devices throughout their life cycle — during the design, development, production, distribution, deployment and maintenance of the device.

The FDA report warned that cybersecurity vulnerabilities can result in compromised device functionality, loss of medical and personal data, and exposure of security threats from other connected devices, which in turn has the potential to result in patient illness, injury or death.

The FDA guidance urges device manufacturers to implement a structured and comprehensive program to manage cybersecurity risks that addresses cybersecurity issues in both pre-market and post-market phases of medical devices, and directs manufacturers to apply the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

So what can businesses do to manage the privacy and security risks associated with the IoT? Consider the following practical steps to create a safer and more privacy-protective IoT environment:

PRACTICAL STEPS TO MANAGE PRIVACY AND SECURITY RISKS

Prepare

- Identify the information that the device collects, where it comes from, what it is used for, with whom it is shared and for what purposes.
- Classify the information as either critical (necessary for device functionality) or optional (something that may be useful, or that could provide enhancements, but not critical to the device's function).
- Conduct a privacy impact assessment to identify privacy risks and consider ways that the risks can be addressed or managed.
- Familiarize yourself with the data protection laws in place where the device will be used.
- Consider whether any other laws could apply to the device or to the persons or industries that will be using the device.
- Understand any technical limitations in the device that may impact security.
- Understand the existing threat environment.

Implement

- Limit collection, use and disclosure of personal information to what is reasonable and necessary to operate the device.
- Ensure that any collection, use or disclosure of personal information for non-critical purposes is optional.
- Describe personal information handling practices in a simple and clear manner and obtain consent. Use real-time notices and other enhanced consent mechanisms as appropriate.
- Implement appropriate security controls with regard to the nature of the device, the nature of the information collected, how information is stored and the identified threats.
- Limit retention of personal information to what is necessary for device functionality.
- Engage experts in de-identification of personal information to ensure it is done effectively.

Evaluate

- Regularly review existing security measures and update as necessary in light of changes to the threat environment or industry standards, or based on experience with the device.
- Review privacy policies and consent language regularly, and any time a change is made to the device or applicable data protection laws.

CONTACT US

Wendy Mee
Partner
416-863-3161

Kristin Ali
Associate
416-863-2678