Privacy In The IoT Age

January 28, 2019

The expanding Internet of Things represents an outstanding businesses opportunity for Canadian companies. But along with potential gains comes more than a little risk. What's the best way to prepare?

If you've ever received a notification on your phone telling you it's time to buy more mayo, thank the Internet of Things. This network of internet-enabled devices is making it easier to do a growing list of tasks, be it listening to your favourite playlist, adjusting the thermostat and yes, knowing when it's time to head to the grocery store.

But as we interact with all these smart devices, they are collecting ever-larger amounts of data about us. How that data is secured and used is one of the most pressing policy issues of our time.

What Makes a Smart Fridge So Smart?
While internet-enabled machinery is revolutionizing manufacturing, where most of us interact with the IoT is right in our own homes. Smart fridges feature tablet-like screens in the front door and can be controlled remotely using your phone. By scanning barcodes or radio-frequency identification tags, the smart fridge monitors expiry dates and automatically places a grocery order when supplies are running low. It will even suggest recipes based on the ingredients on hand.

Consumers have a growing awareness around the value of data and how it can be manipulated. That realization, coupled with a slew of recent high-profile data breaches, is raising public concern about whether enough is being done by smart-device manufacturers to protect a customer's privacy.

A Shifting Regulatory Landscape

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal law that governs how private sector organizations in Canada collect, use and disclose personal information. Introduced in April 2000 – seven years before the advent of the iPhone – this legislation is not as robust as more recent regulations coming out of Europe.

The General Data Protection Regulation (GDPR), introduced by the European Union in May 2018, aims to return control of personal data to consumers. Canadian media

considerably covered the GDPR and its more restrictive approach, so consumers are now expecting higher privacy protection from Canadian companies and organizations. Recent privacy breach scandals have also made consumers more aware of their rights regarding their personal information.

If a company runs afoul of the GDPR, it could be fined up to 20,000,000 EUR or up to 4% of the preceding year 's total global annual turnover.

What's more, the GDPR prohibits European organizations from sharing personal data with non-member states that have weaker privacy protection laws. With that in mind, Canadian legislators are taking steps to fortify PIPEDA. Case in point: PIPEDA as it was originally written was a complaint-driven process. That changed November 1, 2018, when new mandatory breach-notification and record-keeping obligations went into effect, with fines of up to $100,000 for failure to comply. It's expected that by 2020, the Canadian government will do more to bring PIPEDA's consumer protections up to the GDPR standard.

The Issue of Consent

Canadian privacy law, as it stands now, requires that companies obtain the transparent and informed consent of individuals for use of their data. But recent guidance issued by the Office of the Privacy Commissioner of Canada suggests that, even with properly obtained consent, a company could still run into trouble if their data usage does not meet the reasonable expectations and social norms of Canadians. This is a significant potential hurdle for the emerging IoT industry.

On the surface, obtaining consent seems simple enough, but when viewed through an IoT lens, things get more complicated: Your smart fridge is continuously collecting data about your shopping habits – data that could be shared with retailers or other service providers. If they then use that data to send you targeted ads, does that meet the reasonable expectations and norms of Canadians?

Smart cars come with even bigger privacy concerns. Insurance companies could use the driver-related data these cars collect to risk-adjust insurance premiums. But collecting such data without informed consent would likely infringe on a driver's privacy rights. Take this scenario a step further and consider the insurer who might want to increase a customer's rates if they do not consent to sharing their personal driving data. That's the kind of uncharted territory that legal experts can help insurers and other data collectors steer through.

Class Actions Gain Traction

Compared to the U.S., Canada has never been fertile ground for class-action law suits, but when it comes to breaches of data protection laws, that's changing. There are more than 80 class-action suits involving alleged privacy breaches pending or certified in Canada.

In one recent case, the federal government agreed to pay $17.5 million[1] to 583,000 Canada Student Loan recipients after Human Resources and Skills Development Canada (now Employment and Social Development Canada) lost an external hard drive

that contained their personal information. Developments in this area should be followed closely by any company in the IoT field.

What Canadian Companies Should Do Next

As the IoT expands and Canadians become more engaged on the topic of privacy, responsible companies should be redoubling their privacy efforts. Complying with the the Office of the Privacy Commissioner of Canada's new *Guidelines for obtaining meaningful consent* which will be enforced as of January 1, 2019 is an excellent first step.

[1] CBC, "Liberals agree to settle class action lawsuit over student loan privacy breach," December 2017.

Expertise

Cybersecurity, Privacy & Data Protection, Technology
