GILBERT +TOBIN

SECURING THE INTERNET OF THINGS: A Global Overview of a Global Challenge

ALBERT YUEN AND ERICA CHAN

This article was first published in the Privacy Law Bulletin (2018, Volume 15 No. 5).

2018

GTLAW.COM.AU

Last year, Internet of Things (IoT) devices officially began to outnumber the world's human population.[1] While connecting devices to the internet is not a new thing, the scale of the IoT is changing our relationship with data. In addition, greater attention has been given recently to the development and use of IoT devices and services to ensure they consider privacy and security issues. However, regulatory approaches and standards relating to privacy and security issues of IoT devices have varied. With Australia's new mandatory data breach regime[2] and the European Union's (EU) new and border-crossing General Data Protection Regulation (GDPR)[3] having come into effect recently, now is an important time for Australian companies to assess their strategy around privacy, security, the IoT and the global position on the IoT.

KEY TAKEAWAYS

+ The proliferation of IoT devices and service adoption by corporates and consumers have heightened concerns around consumer privacy and security. As there is increased use of IoT data, corporations face challenges in managing, transmitting and sorting these huge volumes of data securely as well as meeting privacy challenges raised by IoT devices, including where data is collected in a "passive" way (eg, through monitoring devices such as mobile apps).

+ While Australia principally regulates the IoT through Australian privacy laws, consumer laws, and industry-specific laws and codes for IoT providers, there aren't any specific IoT-focused regulatory regimes. This is generally similar to the IoT regulatory approach in major jurisdictions worldwide.

+ There are many initiatives underway in Australia and overseas to formulate guidelines, industry codes and areas of good practice for the supply and use of the IoT and other data-driven services. Industry-led initiatives within Australia and globally have provided good frameworks for under-standing the best approach to how IoT regulation, principles, guides and codes are developing. As such, this article aims to take a global stocktake of key markets in how they deal with IoT privacy and security issues. All companies, especially those looking to operate internationally, should consider the increasing consumer concern, different regulatory regimes and industry initiatives when developing their IoT privacy and security strategies.

1 L Tung "IoT devices will outnumber the world's population this year for the first time" (7 February 2017) www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/.

2 Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)(came into effect on 22 February 2018). See also M Fai and L Baranov "Mandatory Data Breach Notification laws are coming … are you ready?" (8 January 2018) www.gtlaw.com.au/insights/mandatory-data-breach-notification-laws-are-coming-are-you-ready.

3 The GDPR represents a complete overhaul of EU data protec-tion law. The GDPR applies across the EU from 25 May 2018, with extraterritorial application. See further information avail-able through the European Commission's GDPR Portal at www.eugdpr.org. See also P Leonard "GDPR: a guide for Australian businesses" (May 2018) www.iot.org.au/wp/wp-content/uploads/2016/12/GDPR-a-guide-for-Australian-businesses.pdf.

KEY IOT PRIVACY AND SECURITY CHALLENGES

WHAT IS THE INTERNET OF THINGS?

The IoT can be defined simply as "the networking of physical objects connecting through to the Internet"[4] and each other. However, this definition belies the increasing complexity and impact of the IoT. We can find a more powerful metaphor from Kevin Ashton, known as the "father of IoT", who has compared the IoT to the human nervous system.[5]

It's a surprisingly apt comparison. Firstly, it reflects the incredible scale of the IoT and its connections: research firm Gartner predicts that by 2020, we will have approximately 20.5 billion IoT devices.[6] Secondly, it gives us a useful perspective of the IoT in practice. After all, like our own nervous systems, IoT devices are constantly collecting and transmitting information to be used in analysis and decision-making.[7]

Lastly, just like our nervous systems, the IoT is open to serious attack. The connectivity and number of IoT devices mean that breaching the security of a single device can infect every single other device in the network, allowing criminals to launch distributed denial-of-service (DDoS) attacks to steal data or bring down online services.[8]

The power and disruptive promise of the IoT is the exponential scale of its data. As the number of devices capable of internet connectivity increase, and as IoT device manufacturing, connectivity and data costs are reduced, there is an unprecedented scalability of IoT solutions. However, the proliferation of data collection, storage and transmission and use from the IoT also raises increased concern about privacy and security risks, as well as consumer confidence around the IoT design process.
Together, these elements of the IoT showcase the primary challenges that our increasingly connected world poses: protecting privacy and securing the IoT.

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" (February 2016) www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/ 2016/iot_201602/.

5 LG CNS "From I.T. to I.O.T.: how the best companies transition to the internet of things" (22 April 2015) www.lgcnsblog .com/features/entrue-world-2015-kevin-ashtons-keynote-speech/#sthash.3nWo00su.dpbs.

6 M Hung "Leading the IoT: Gartner insights on how to lead in a connected world" (2017) www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

7 M Heflin "The nervous system of the IoT" (16 August 2016) www.machinedesign.com/iot/nervous-system-iot.

8 A D Rayome "DDoS attacks increased 91% in 2017 thanks to IoT" (20 November 2017) www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/.

THE CHALLENGE OF CONSUMER PRIVACY

The everyday use of IoT devices is inescapably eroding individual privacy. To demonstrate this, journalist Kashmir Hill recently converted her apartment into a "smart home" to run a privacy experiment with her colleague Surya Mattu.[9] Hill bought a number of IoT devices, including a smart bed, a smart television, smart lights, and even a smart coffee maker. Mattu used a router to capture all of Hill's IoT device activity. Only a few months of monitoring revealed a treasure trove of data. For example, Mattu could track exactly when family members were going to bed and when they left the apartment through their smart lights and Amazon Echo. Mattu also found that Hill's smart television was collecting second-by-second information about every-thing the family watched, from commercials to DVDs, and selling that data to advertisers.

Hill's article describing her IoT and privacy experiment touched a nerve. In the flood of commentary following it, many raised concerns that none of this information is necessarily recognised as "personal information" and protected by privacy laws. That's certainly true in Australia, where the Full Federal Court held last year that metadata — even location data allowing companies to track where individuals live and how they go to work — is not necessarily personal information unless it passes the threshold question of whether it is directly "about" an individual.[10] Companies providing or utilising IoT devices or services will need to be fully compliant with the law (including managing Australian Consumer Law (ACL) issues around any defective IoT devices, with indications that Australian regulatory bodies are determined to ensure consumer laws keep pace with developing technologies such as the IoT)[11] and need to carefully manage these risks, including running afoul of consumer ire and public activism.

9 K Hill and S Mattu "The house that spied on me" (8 February 2018) www.gizmodo.com.au/2018/02/the-house-that-spied-on-me/.

10 Privacy Commissioner v Telstra Corp Ltd (2017) 249 FCR 24; 347 ALR 1; [2017] FCAFC 4; BC201700165.

11 ACL, s 3. The definition of "consumer" is extremely broad and is likely to capture a wide variety of IoT devices and services. See also M Swinson, W Osborn and S Swan "There's a glitch in the matrix — the application of consumer guarantees to the IoT" (2017) 21(8&9) IHC 176.

THE CHALLENGE OF SECURITY

The second challenge of the IoT is security. IoT devices often have many vulnerabilities, including problematic infrastructure, improper authentication mechanisms and lack of encryption, resulting in the well-founded fear that IoT devices are the greatest threat to individual security today.[12]

Companies face another level of complication. In her experiment, Hill ran into an unforeseen problem: compatibility. To run all of her devices, she had to download 14 different applications, and not all of her IoT devices were compatible with each other.

For Hill, this was frustrating. But at a business level, it means that companies that manufacture, supply, or use IoT devices are finding themselves in an increasingly complicated supply chain with multiple parties, ranging from data analytics providers to third-party software developers.

The first wave of IoT commercialisation saw vendors trying to provide end-to-end solutions to cut down on such complexity. However, the consumer-driven market has led to more fractured, mix-and-match, and multi-vendor approaches. For our clients, we have seen that these approaches provide both customisation and challenges, including:

+ determining data breach liability and response management between multiple vendors
+ managing clashing privacy policies and data practices in coordinating critical responses to data breaches
+ the reality that the privacy and data security of the whole supply chain is only as strong as its weakest link, which may be a subcontractor in another jurisdiction

Such challenges show that there needs to be renewed focus on user preferences and the IoT design process relating to a user's awareness of the collection, processing, use and transmission of information (including potential personal information) in IoT solutions.[13]

12 InfoSec Institute "The top ten IoT vulnerabilities" (February 2018) https://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/#gref. See also S Weagle "The rise of IoT botnet threats and DDos attacks" (30 January 2018) www.corero.com/blog/870-the-rise-of-iot-botnet-threats-and-ddos-attacks.html and N Fearn "What the Internet of Things (IoT) means for data security" (28 March 2018) www.itpro.co.uk/internet-of-things-iot/30844/what-the-internet-of-things-iot-means-for-data-security.

13 This view was raised in R Bosua "Privacy by design in the era of the Internet of Things (IoT)" (2016) 3(1-2) MTC 3.

THE GLOBAL IOT PRIVACY & SECURITY LANDSCAPE

Faced with both the inherent insecurity of IoT devices and the complex commercial relationships surrounding them, it is no wonder that Gartner has predicted that worldwide spending on securing the IoT will reach$1.5 billion this year.[14]

Such expenditure is a sign of how the landscape has shifted to meet the monumental privacy and security challenges of the IoT. Only a short time ago, it was a common lament that consumers either were not aware of, or simply did not care about, how using technology affected their privacy. That is no longer the case. The Economist Intelligence Unit recently released a report showing that 92% of global consumers surveyed wanted to control the scope of automatic collection of personal information and 92% wanted heavy punishments for companies that violated their privacy.[15]

Recent and well-publicised privacy scandals involving Facebook and Cambridge Analytica have certainly contributed to such views.

In response, governments and industry organisations around the world are taking a number of different approaches.

AUSTRALIA

Australia currently has no specific legislation which specifically regulates the IoT. Instead, the IoT in Australia is governed under privacy legislation (as it relates to the collection, storage, use and transmission of personal information or "sensitive information" of individuals), and the ACL (as it relates to the use of IoT products and services for domestic consumer purposes).[16] The use of IoT devices in certain industries may also fall under regulation, such as the Telecommunications (Interception and Access) Act 1979 (Cth) requiring telecommunications companies to retain certain data for 2 years. The Office of the Australian Information Commissioner (OAIC) has also recently published guidance to assist organisations to identify and take steps to address privacy issues related to data analytics, including the use of the IoT.[17]

The responsibility for direct regulation of the IoT seems to have shifted to industry, with the IoT Alliance Australia (IoTAA), the peak Australian industry body for the IoT, leading the charge. Its work includes the introduction of an IoT device security certification and the publication of the "Internet of Things security guideline" and "Good data practice: a guide for business to consumer Internet of Things services for Australia", the latter of which aims to assist suppliers of IoT business to consumer (B2C) devices and services to design fair and appropriate privacy and security features to promote take-up, confidence and acceptance by Australian consumers of IoT services and devices. [18] Independent body Standards Australia has also kept Australia in touch with international movements on the IoT in its position on the International Organization for Standardization (ISO) and the International Electrotechnical Commission's (IEC) IoT subcommittee around the development of global standards.

However, the Australian Government has recently announced a 4-year plan to overhaul data regulation, including establishing a National Data Commissioner[19] and new Consumer Data Right (CDR) legislation aimed at providing consumers with open access to and control of their personal data.[20] While the draft legislation has not yet been released, the intent of the CDR appears to mirror the EU's GDPR in many ways. By prioritising data transparency and consumer control, such legislation will necessarily have an impact on businesses manufacturing, supplying and using the IoT.

14 Gartner "Gartner says worldwide IoT security spending will reach $1.5 billion in 2018" (21 March 2018) www.gartner.com/newsroom/id/3869181.

15 The Economist Intelligence Unit What the Internet of Things Means for Consumer Privacy (2018) https://perspectives.eiu.com.

16 As IoT solutions communicate over a telecommunications or radio network, a service provider of the IoT connectivity may be regulated by applicable Australian telecommunications or radio communications laws such as the Telecommunications Act 1997 (Cth) or the Radiocommunications Act 1992 (Cth). Many IoT devices are low-powered devices that are permitted to operate in designated spectrums under the Radiocommunica-tions (Low Potential Interference Devices) Class Licence 2015 (Cth). Mobile phone users are permitted to use their mobile phones and devices that use SIM cards by the Radiocommunica-tions (Cellular Mobile Telecommunications Devices) Class Licence 2014 (Cth). Subject to exemptions, where the IoT device passing over a telecommunications system has commu-nications interception capabilities, the Telecommunications (Interception and Access) Act 1979 (Cth) may also need to be considered.

17 OAIC "Guide to data analytics and the Australian Privacy Principles" (March 2018) www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-data-analytics-and-the-australian-privacy-principles.pdf.

18 IoTAA "Strategic plan to strengthen IoT security in Australia" (September 2017) www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Strategic-Plan-to-Strengthen-IoT-Security-in-Australia-v4.pdf; IoTAA "Internet of Things security guideline" (November 2017) www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf; IoTAA "Good data practice: a guide for business to consumer Internet of Things services for Australia" (November 2017) www.iot.org.au/wp/wp-content/uploads/2016/12/Good-Data-Practice-A-Guide-for-B2C-IoT-Services-for-Australia-Nov-2017.pdf. See also AYuen "Seizing the IoT opportunity: IoTAA good data practice guide for B2C IoT services" (10 November 2017) www.gtlaw.com.au/insights/seizing-iot-opportunity-iotaa-good-data-practice-guide-b2c-iot-services.

19 P Bhunia "Australian Government announces A$65 million investment to reform country's data system" (2 May 2018) www.opengovasia.com/articles/australian-government-announces-a-65-million-investment-to-reform-countrys-data-system.

20 S Venkat "Australia mulls over new Consumer Data Right legislation" (29 November 2017) www.cerillion.com/Blog/November-2017/Australia-new-Consumer-Data-Right-legislation.

US

In contrast to Australia, the US has introduced multiple Bills aimed at regulating the IoT, including the Developing Innovation and Growing the Internet of Things (DIGIT) Act S 88 (US) and the Securing the Internet of Things Act of 2017 (US).[21] Much of this legislation has stalled; however, the debate continues about the best path forward. Outside of legislation, the government has also implemented other cybersecurity initiatives. The Federal Communications Commission (FCC) has approved new rules impacting how IoT equipment suppliers conduct their businesses.[22] The Federal Trade Commission (FTC) has also taken enforcement action against IoT providers, including taking D-Link Corporation, one of the largest manufacturers of IoT products, to court. [23] Moreover, the National Institute of Standards and Technology (NIST) has released several reports and recommendations on the IoT, including in relation to cybersecurity standards and a draft IoT-Enabled Smart City Framework around interoperability.[24]

Nevertheless, even in the US there has been some reticence around regulation, with NIST officials making clear statements that such standards are voluntary and insisting the private sector take the lead on adoption.[25]

EUROPE

With the introduction of the GDPR, Europe has cemented its position as having the strongest data privacy framework worldwide. The GDPR is aimed at protecting the personal data of EU residents, and sets out significant penalties for companies in breach. Europe has also had an independent European Data Protection Supervisor for many years that provides monitoring and advice around protecting personal information and the impact of new technology such as the IoT.[26] Addition-ally, in November last year, the European Parliament introduced the "objective conformity criteria" aimed at regulating IoT device manufacturing, interoperability and trade.[27]

However, even in Europe there is continued uncertainty about how best to regulate privacy and the IoT. At this year's Computers, Privacy and Data Protection (CPDP) conference, a European Parliament member argued that law enforcement should never have access to certain types of data, and that states should never mandate IoT data retention. Such a stance may lead to conflict with the EU's Police Directive, which governs information collected in a criminal investigation. Some have also criticised the apparent disconnect between Europe's strong privacy laws and the stance of some reports from bodies such as the IoT Security & Privacy Workshop and the European Commission's Digitising European Industry framework, both of which appear to focus more on IoT standardisation and network capacity as challenges to advancing the IoT in Europe.[28]

21 K Goodloe "Covington IoT update: U.S. legislative roundup on IoT" (9 May 2018) www.natlawreview.com/article/covington-iot-update-us-legislative-roundup-iot.

22 R Quirk "High-level overview of the FCC's equipment regu-lation changes — IoT device suppliers beware" (21 July 2017) www.iotforall.com/overview-fcc-equipment-regulation-changes/.

23 K C Halm and A Reynolds "IoT vendors beware: FTC's latest enforcement action signals further scrutiny of the industry" (23 January 2017) www.privsecblog.com/2017/01/articles/dataprotection/iot-vendors-beware-ftcs-latest-enforcement-action-signals-further-scrutiny-of-the-industry/.

24 NIST "What is the Internet of Things (IoT) and how can we secure it?" www.nist.gov/topics/internet-things-iot.

25 D B Johnson "Why is no one raising a hand to regulate the internet of things?" (16 March 2018) https://fcw.com/articles/ 2018/03/16/iot-regulation-ispab-johnson.aspx.

26 European Data Protection Supervisor "Internet of Things" https://edps.europa.eu/data-protection/our-work/subjects/internet-things_en.

27 D Meyer "European Parliament pushes on IoT device security and interoperability" (4 December 2017) https://internetof business.com/iot-devices-get-new-security-interoperability-obligations-eu/.

28 L Krahulcova "What the EU is getting wrong about the Internet of Things" (12 February 2018) www.accessnow.org/what-the-eu-is-getting-wrong-about-the-internet-of-things/.

ASIA

If Europe is at the forefront of IoT regulation, then Asia is at the forefront of IoT adoption. A recent Vodafone survey revealed that 36% of Asian companies use IoT devices, with 77% seeing IoT as mission-critical to their business. Interestingly, the survey revealed general optimism about the IoT and security, with 86%of respondents seeing security as an enabler of the IoT and 83% claiming to have adequate skills to manage IoT security.[29]

The IoT is also incredibly important in Asia from a governmental perspective. Singapore and Hong Kong have invested heavily in IoT-connected "smart cities", and many Asian countries are the world's primary IoT device manufacturers. This is reflected in government policy. Singapore has been particularly vocal about the importance of open IoT standards to prevent entrapment by suppliers' "walled gardens", and has published four open IoT standards relating to public area sensor net-works, smart homes, interoperability, and IoT reference architecture. [30] In addition, China's Cybersecurity Law, which took effect in June last year, focuses heavily on individual data privacy protection.[31] While the exact scope of the law is yet to be tested, it seems that many businesses that operate IoT infrastructure within China are considered network operators or part of a "critical information infrastructure", subjecting them to additional regulation.[32]

29 A Tan "Asia is pace-setter in IoT" (23 November 2017) www.computerweekly.com/blog/Eyes-on-APAC/Asia-is-pace-setter-in-IoT.

30 A Tan "Singapore government outlines its approach to IoT" (21 March 2018) www.computerweekly.com/news/252437239/Singapore-government-outlines-its-approach-to-IoT. See also, Information Technology Standards Committee "Internet of Things Technical Committee (IOTTC)" www.imda.gov.sg/itsc/technical-committees/internet-of-things-technical-committee-iottc.

31 IT Advisory KPMG China "Overview of China's Cybersecurity Law" (February 2017) https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

32 M Parsons "IoT cybersecurity and data privacy trends in Asia: be ready" (13 June 2017) www.lexology.com/library/detail .aspx?g=78e15982-230e-4990-a635-f348fd688b8e.

WHAT'S NEXT

An overview of different global approaches to IoT privacy and security reveals a number of patterns. The first is that there is a general awareness of the IoT's benefits, threats and challenges at every level, from government to enterprise to individual consumers. Secondly, there is a clear tension between consumer distrust in industry self-regulation and government fear of slow-moving laws stifling innovation. Lastly, a strong global consensus is emerging around the importance of adopting open global standards designed to increase both security and interoperability, although how such standards will interact with different regulatory regimes remains to be seen.

In such an environment, there will be no businesses left unaffected by the IoT and its privacy and security challenges. Consequently, every company needs to stay abreast of the developing legal, industry and commercial landscape and take a holistic perspective around their security and privacy strategies. It is no longer enough to simply do your best to comply with applicable regulations and have an up-to-date privacy policy. Businesses will increasingly need to navigate the risk positions, applicable regulatory and quasi-regulatory/industry frameworks, and privacy policies of their partners, suppliers, subcontractors and customers. In short, our clients will need to increasingly take a global perspective on the global opportunities and challenges posed by the IoT.

The authors would like to thank research assistants Kate Dillon, Ashlee Chapman and Natasha Liyanage.

ALBERT YUEN

Special Counsel
T +61 3 8656 3316
E ayuen@gtlaw.com.au

ERICA CHAN

Lawyer
T +61 3 8656 3406
E echan@gtlaw.com.au

GILBERT +TOBIN

SYDNEY
Level 35 International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
T +61 2 9263 4000
F +61 2 9263 4111

MELBOURNE
Level 22
101 Collins Street
Melbourne VIC 3000
Australia
T +61 3 8656 3300
F +61 3 8656 3400

PERTH
Level 16 Brookfield Place Tower 2
123 St Georges Terrace
Perth WA 6000
Australia
T +61 8 9413 8400
F +61 8 9413 8444

GTLAW.COM.AU