Internet of Things – Is it Hype or the Next Big Thing? Part II

James Halliday and Rebekah Lam provide the second and final instalment in a two-part series which examines the legal and policy implications of the Internet of Things (IoT).

The IoT reflects the maturity or industrialisation of the internet and is being enabled by rapid improvements in sensor technology, bandwidth and mobile technology generally and big data analytics. The IoT therefore creates unprecedented opportunities as well as risks. In Part I which appeared in Volume 3 of the 2015 CAMLA Bulletin we looked at some of the issues arising for industry including interoperability and standards; numbering plan and roaming implications; and spectrum allocation policy and net neutrality issues.

Having to provide the required notice and obtain the relevant consent at each juncture is in many cases impracticable

We now turn our attention to a range of law enforcement and consumer issues arising out of the IoT in Australia, and in particular what the IoT means in the context of cybersecurity, personal privacy and general consumer law. While a single IoT device in itself is most likely harmless, when aggregated together in the millions these devices pose considerable challenges and potential harm, whether intangible, inadvertent or malicious.

CONSUMER LAW

In (very) general terms, the existing Australian consumer law framework will mostly apply to IoT applications supplied to consumers. This framework prohibits misleading or deceptive conduct, implies statutory guarantees into certain consumer contracts, establishes a product liability regime and may also void unfair or unconscionable contracts. The existing privacy protection framework will also apply where a regulated person (such as an IoT operator) collects, uses or discloses personal information about a consumer. These are valuable protections for consumers.

THE AUSTRALIAN CONSUMER LAW

Consumers who purchase IoT products receive general protection under the Australian Consumer Law (***ACL***). Although not specific to the IoT, the ACL protects consumers from misleading or deceptive conduct, unfair contract terms and unconscionable conduct. The ACL also contains statutory consumer guarantees (e.g. goods must be of acceptable quality, match their description, be fit for purpose) which is a further, albeit n indirect way of enforcing privacy and security compliance.

For example, in the USA, after a man hacked into a baby monitor in 2013, the FTC (the Federal Trade Commission) took its first action against an IoT firm for misleading or deceptive conduct. The FTC alleged that TRENDnet – a web enabled camera manufacturer promised customers that its cameras were secure, when they were not.[1] The claim was settled by the parties and the terms of the settlement required TRENDnet to address the security risks, help customers fix their software and obtain an independent assessment of their security programs every year for 20 years. TRENDnet was also prohibited from misrepresenting the security of its cameras or the security, privacy, confidentiality or integrity of the information that its cameras or other devices transmit and the extent to which a consumer can control the security of information stored, captured, accessed or transmitted by the devices.[2]

In Australia, under the ACL, "consumers", are broadly speaking, persons who acquire goods and services that are priced less than $40,000 or goods or services of a kind ordinarily acquired for personal, domestic or household use or consumption. Equivalent legislation exists at the State and Territory level.

The ACL is administered by the Australian Competition and Consumer Commission (***ACCC***), which (in addition to its general enforcement powers) has special powers under the *Competition and Consumer Act 2010* (Cth) (***CCA***) to promote competition within the Australian telecommunications industry and ensure consumers' interests are protected.

PRIVACY LAW

Australian privacy law regulates the way that personal information (information about an individual who is identified or reasonably identifiable) is collected, used, stored and disclosed. The privacy laws include 13 Australian Privacy Principles (***APPs***) which apply to most government agencies, private organisations with an annual turnover of $3 million or more, health organisations, bodies that trade in personal information and parties that contract with the Commonwealth.

1 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.

2 https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

CONSENT REQUIREMENT

The privacy regime imposes a transparency framework for general personal information and a consent requirement for the collection of sensitive information. Under this regime an organisation that collects personal information (***APP Entity***) must notify the data subject about specified matters such as what information is being collected, how it is collected and how it will be used and disclosed.

In theory, a data subject wishing to control the collection and use of his or her information could consult the relevant public disclosures made by each relevant service provider and elect not to deal with a provider that does not propose to use personal information in an acceptable manner. However, this is difficult to achieve in practice since data subjects usually have little scope for negotiating privacy terms and have limited control over the collection and use of their personal information. In certain circumstances, due to the pervasive nature of IoT devices, it is possible for an IoT service provider to collect information about an individual without the individual's knowledge (e.g. facial recognition technology, public wi-fi spaces).

Where personal data is collected with an individual's knowledge, the APPs require IoT service providers to provide details of who owns the data collected by an IoT device, exactly what data a device collects, how the data is protected, who the data is shared with (including any overseas recipients) and the specific purposes for which the data is used. However, in many cases this is impractical or impossible, particularly where there is no transaction with the data subject and therefore no means of directly communicating with them. As there is no tort of privacy in Australian law, a data subject presently only has a legal complaint if they can demonstrate a breach of a duty of confidence, as set out in the Lenah Game Meats decision. This is typically difficult or impossible where the data subject has been subject to 'surveillance' in a public space.

Also, because the IoT industry is evolving a further complexity arises. Quite often, the type of data initially collected by an IoT device is put to different uses over time. Whilst an individual may have consented to the initial uses of the data, the consent will generally only apply to subsequent uses if the secondary use is directly related to the initial use. Having to provide the required notice and obtain the relevant consent at each juncture is in many cases impracticable.

In summary, consent in the context of the IoT may therefore not always be a feasible way of managing privacy expectations. What is perhaps more important is for the individual affected to understand the use to which the data is put and the opportunities, if any, to access and review that data.

AGGREGATION OF DATA

Issues also arise when data sets that do not initially contain personal or sensitive information (and are therefore not regulated) are subsequently aggregated with other data sets and become regulated. For example, information regarding the location of a particular mobile device over time combined with mapping and other public database information could reveal an individual's home address, work address, age, health, faith and many other personal details including name and phone number. This would convert non-personal information to personal information that is subject to privacy law.

This aggregation of data was highlighted in the case brought by Ben Grubb against Telstra when Telstra denied him access to his metadata (e.g. geo-location data). By failing to provide the journalist with this information, the Privacy Commissioner found that Telstra had breached the Privacy Act. In its defence, Telstra had argued that metadata was not personal information about a customer because on its face, the data was anonymous. The Privacy Commissioner rejected that argument on the basis that the cross matching of that geo-location data with different data sets could identify the customer, therefore converting the geo-location data into personal information.

DATA MAINTENANCE

Under APP 11, an APP Entity is required to destroy or de-identify personal information when it no longer needs the information and must, on request, give an individual access to his/her personal information within a reasonable period unless an exception applies e.g. it could be said that the granting of access would reveal commercially sensitive information or compromise the privacy of another person. (APP 12). If an individual's request is denied, the collecting entity must explain the reason for the refusal and the mechanisms available to the individual to complain about the refusal.

consent in the context of the IoT may therefore not always be a feasible way of managing privacy expectations

In the IoT context this requirement could involve thousands of requests from data subjects creating an enormous administrative burden and one which IoT service providers would be ill-equipped to handle. It is also likely to be difficult to provide this data in a way which is meaningful to an individual, as much of the data's value is derived from aggregating it with other information.

Concerns have also been expressed regarding whether some IoT sensor data can truly be de-identified given the unique fingerprints of many devices and the ability to re-identify the data. It may be impossible for data captured by some IoT applications to comply with the de-identification requirement since is it unclear whether these data sets can be truly anonymised.

Another concern is the 'portability' of data. There is no common or required standard for how data is stored and practically it would be difficult to introduce one. However, if an individual changes service providers they will typi-

>

> cally want their data to be ported to the new service provider, which is often difficult or impossible, thereby creating barriers to choice.

CYBERSECURITY

The security of captured data faces increasing risks as the IoT becomes ubiquitous and cybercriminals understand the value of the information. The range and number of devices and disparate networks that are being used expands the number of potential targets for cyber threats.

The security of captured data faces increasing risks as the IoT becomes ubiquitous and cybercriminals understand the value of the information

Low powered special purpose devices typically used for IoT do not have the processing power to maintain high levels of security. The small form factor and low power and computational capacity make adding encryption or other security measures difficult.[3] Network devices that accept connections from limited function internet-enabled devices may also have increased vulnerability.

Malicious attacks are becoming more and more sophisticated, varied and harder to defeat. A study by HP revealed that 70% of the most commonly used IoT devices contained vulnerabilities.[4] The increase in the number of devices can also mean vulnerabilities spread very rapidly.

Adding to this risk is the fact that the risk landscape is pushing well beyond the boundaries of a particular organisation, since organisations are owning less and less of the data assets flowing through their systems. Security measures must encapsulate a much wider network beyond the organisation and address the standards of security of the organisation's clients, customers, suppliers/vendors and business partners.

The FTC recently published guidance on what companies should consider when they design and market products that are connected to the IoT.[5] The recommendations largely contain standard security protocols e.g. encryption, limited permissions, two-factor authentication and regular security evaluations. They also reiterate the need to be much more vigilant given the pervasive nature of the IoT in a workplace and also at home. The guidelines centre on the principles of security, data minimisation, notice and choice. The FTC recognises that businesses and law enforcers both have a shared interest in meeting consumer expectations regarding the security of new IoT products.

The FTC guidelines reflect that IoT products are not always engineered to protect data security as they are often created by consumer goods manufacturers and not computer software or hardware firms. Many IoT products are also not designed to be re-tooled after release to the market so are not patchable or easy to update.[6]

The FTC guidelines recognise that there is no one-size-fits all approach to guarantee the security of connected devices. They also recognise that those companies which take the lead in providing consumers with confidence about how their data will be used, are the most likely to flourish from the IoT revolution.

The FTC, however, concludes that any IoT specific legislation would be premature given that the technology is still emerging and is rapidly changing. However, the FTC is calling for stronger data security and data breach notification legislation to provide some measure of protection to data subjects. It is also asking for manufacturers to engage in privacy by design i.e. building privacy safeguards in their products upfront given that many connected devices have little or no user interface.[7]

As a reflection of its commitment to harnessing the value of the IoT, the US Senate passed a resolution in March 2015 calling for a "national strategy for the IoT to promote economic growth and consumer empowerment".[8] The resolution referred to the US prioritising the development and deployment of the IoT in a way that "responsibly protects against misuse" but did not go further to mention anything about how the IoT would be regulated.

PRODUCT LIABILITY

In addition to the risk of an IoT product malfunctioning and causing damage to property or physical injury, IoT devices are vulnerable to cyberattacks which may cause damage or injury (e.g. a compromised heating system could cause fire and property damage). Liability may also arise to an IoT user if their personal data is used by a hacker in an attack on a third party or to breach that third party's privacy rights.

In situations where an IoT product causes loss, identifying who bears responsibility if the software is vulnerable to cyberattack and what role the consumer plays are not necessarily easy to define. For example, would the manufacturer or software developer bear primary responsibility, or what apportionment could be given

3 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.
4 http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/bap/6556284#.VVAuMPmqpBd
5 FTC Staff Report, internet of things, Privacy & Security in a Connected World, January 2015.
6 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.
7 Brill, Julie, The Internet of Things: Building Trust and Maximising Benefits Through Consumer Control, 89 Fordham L. Rev. 205.
8 http://www.fischer.senate.gov/public/_cache/files/2b3ad47d-f4df-4cb8-b6e3-877de18be0a8/ern15061.pdf.

to the consumer if he/she had failed to adequately protect the IoT device/system by not updating security software or using strong passwords?

INTERNATIONAL AGREEMENTS

On a global scale, the US is spearheading a number of international treaties including the Trans-Pacific Partnership Agreement (***TPP***) (now consented to by Australia), the Trade in Services Agreement (***TISA***) and the Transatlantic Trade and Investment Partnership (***TTIP***) which may impact the way information flowing across jurisdictional boundaries is handled and regulated.

To the extent these international agreements promote the flow of Australian data offshore, the previously discussed concerns regarding cybersecurity and privacy are exacerbated given the limited ability to control what another jurisdiction does with the data.

MANDATORY DATA RETENTION

Under the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), telecommunications carriers, carriage service providers and internet service providers have to provide certain data to certain government bodies and agencies on request and retain this data for two years.

The mandatory data retention laws apply to telecommunications data including the type and time of a communication (e.g. when an email is sent), the size of a communication, what service was used to transmit the communication (e.g. mobile, landline, email, VoIP, http etc), the address the message was sent to and from, and the location of the device used. The laws do not apply to the content of communications, a user's web browsing history or login information. Industry is presently developing a matrix of specific data types in consultation with government as part of the implementation of the new laws.

The data retention laws apply to carriage services delivered by the carriage service provider. Therefore, many aspects of the M2M (machine to machine) communications involved in IoT applications may be captured by these laws. Whilst government bodies will not be able to access the content of these communications except for metadata (at least without a warrant), they will be able to tell when, how and to whom these communications have been made. This raises the question whether the cost and privacy implications of retaining IoT metadata lead to any tangible law enforcement outcomes or benefits.

DISCRIMINATION AND THE DIGITAL DIVIDE

The aggregation and profiling of user data may lead to marginalisation and create new opportunities for digital discrimination. "Sensor fusion" i.e. the ability to combine information from two disconnected sensing devices to create greater and more complex information[9] can lead to data controllers profiling users based on an infinite number of characteristics e.g. race, gender, level of activity, employment, economic status etc.

This can lead to users being faced with highly targeted and predatory marketing tactics that prey on a user's identified behaviours, patterns and preferences. For example, people in financial difficulty may be approached by financial institutions offering them finance at high interest rates, when they can least afford it.

People who do not use the IoT (e.g. elderly or the poor) may also find themselves increasingly sidelined. For example, in Boston, a mobile app that identified pot holes on a city's roads through the mobile phone's accelerometer and GPS data, helped the city's Public Works Department isolate problem areas and concentrate its resources. However, given the poor and elderly may be less likely to download the app, there were concerns the city's services could be diverted away from the areas that need most attention in favour of younger and wealthier neighbourhoods.[10]

It is clear that the information that can be harnessed by the IoT can be of enormous value, but measures must be put in place to ensure that no matter how well intentioned, the information does not lead to unintended consequences contrary to public policy.

Another consideration for consumers is the extent to which they can easily and cheaply transfer their data from one service provider to another. Over time the quality and quantity of information gathered by one service provider may be of such value to a consumer that he or she wants to transport it to another provider e.g. health, security or financial information. The potentially anti-competitive behaviour of a service provider could be a deterrent to that transfer.

CONCLUSION

The IoT raises a number of regulatory issues that must be counterbalanced with the need to promote and encourage the innovation of the IoT. The EU and US are currently monitoring the emergence of the IoT environment, recognising that enacting legislation whilst the IoT is in is infancy is premature.

In Australia, the existing regulatory framework needs careful review to ensure it is best placed to cope with the enormous growth of the IoT that is forecast. The role of industry also needs to be defined to ensure that the overall response to the technological developments strikes the appropriate balance between innovation and consumer protection.

JAMES HALLIDAY is a partner and REBEKAH LAM a lawyer at Baker & McKenzie. This article represents the personal view of the authors and is not necessarily representative of the views of any client of the firm.

9 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.

10 Finch, Kelsey and Tene, Omer, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town, 41 Fordham Urb.L.J. 1581 2013-2014.