Internet of Things
Some legal and regulatory implications

February 2016

This paper is based on an earlier paper prepared for the Communications Alliance in Australia, in July 2015. It was prepared to assist the general discussion about the IoT and does not advocate any specific regulatory response to this phenomenon. It should not be relied upon for the purposes of legal advice by any person and does not necessarily represent the views of any client of the Firm.
Executive summary

There is no widely accepted definition of the Internet of Things (IoT). It has been variously described as "the third wave of the internet", "a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction"\(^1\), and as "the concept of basically connecting any device with an on and off switch to the internet (and/or to each other)".\(^2\) It has also been referred to as "physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community".\(^3\)

The inability to clearly articulate exactly what the IoT is and what it encompasses, underlies the complexity generated by its accelerating growth which requires regulators to respond to the latest developments in a way that protects individuals but does not stifle the innovative potential of this important technological advancement.

The growth of the IoT is producing ever increasing volumes of data, demanding more processing power and requiring more complex analytics. It is also presenting challenges to our existing legal framework. Some predict there will be 50 billion connected devices by 2020 (there are currently about three billion) with machine to machine communications generating about US$900 billion in revenues by that time.\(^4\)

---

1. [http://whatis.techtarget.com/definition/Internet-of-Things](http://whatis.techtarget.com/definition/Internet-of-Things)
5. The authors would like also like to acknowledge the contributions of Patrick Fair in preparing this article.
Risks and benefits of the IoT

The IoT provides tremendous value to users by offering convenient solutions that not only save time and money, but can also save lives and help governments allocate resources more efficiently.

The IoT also carries the risk of intrusive monitoring, an unacceptable invasion of privacy and the misuse or unauthorised access to intimately personal information. Detailed information about an individual's behaviour, circumstances, family background and personal attributes may lead to discriminatory practices.

All this newly accessible information will need to be stored somewhere. However, the storage of the data will only be as valuable as the analytics that can be performed on it. The future of IoT is dependant on robust infrastructure including ubiquitous broadband connectivity and sensor based technologies but the question is whether these enabling technologies can keep up with the demand to successfully support the growth of the IoT.

Regulation of the telecommunications industry has, in some cases, not always anticipated the rise of machine-to-machine (M2M) communications and does not cater for all aspects of the IoT. In this paper we have had regard to a variety of interest groups and the issues that may be of most concern to them. We have listed the issues potentially faced by each stakeholder group below.

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Potential issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry and service providers</td>
<td>Carrier business model</td>
</tr>
<tr>
<td></td>
<td>Interoperability, interference and standards</td>
</tr>
<tr>
<td></td>
<td>Numbering plan issues</td>
</tr>
<tr>
<td></td>
<td>Roaming</td>
</tr>
<tr>
<td></td>
<td>Spectrum allocation policy</td>
</tr>
<tr>
<td>Content providers/controllers</td>
<td>Net neutrality</td>
</tr>
<tr>
<td>Government and law enforcement</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>Mandatory data retention</td>
</tr>
<tr>
<td>Personal and community</td>
<td>Discrimination and the digital divide</td>
</tr>
<tr>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td>Consumer law</td>
</tr>
<tr>
<td></td>
<td>Product liability</td>
</tr>
</tbody>
</table>
Defining the IoT ecosystem

Increasingly, the internet is becoming "commoditised" or "industrialised" where the abundance of information about a person's attributes, preferences and behaviour is leading to the "datafication of society". Data can be captured, analysed and stored by data brokers who provide the information to private companies that use the information for marketing, product development and other business purposes.

The IoT is not homogeneous but extremely diverse and involves a range of technologies with a wide array of applications for both individuals and businesses. Some of the technologies exist in industries more regulated than others (e.g. health and transportation) but some are not directly regulated by any industry-specific rules (e.g. exercise and diet trackers). It is clear that any regulation of the IoT cannot adopt a one size fits all approach but must take into account the complexity of the IoT environment.

For example, on one hand there are devices which are used to provide a service directly to a consumer or business (e.g. baby cams, exercise and diet trackers, personal alarm sensors, heart monitors and other biological monitors). Devices can also automatically water plants, send reminders to take medication, assist in finding the closest parking space, remote control the temperature and lighting in homes and automatically update shopping lists. In these examples, the IoT serves as a seabed for innovative solutions to everyday problems and inconveniences.

In general terms:

- For consumer transactions, the existing consumer law framework will mostly apply. 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 (potentially, but not always including an IoT operator) collects, uses or discloses personal information about a consumer; and

- Where an IoT service involves the supply of a content service over a carriage service, then the supplier will be a 'content service provider' for the purposes of the Telecommunications Act 1997 (Cth) and therefore subject to the service provider rules contained in that Act.

However, while the consumer protection/privacy framework will typically apply to the supply of IoT services to consumers, the nature of IoT presents unusual challenges for regulators. This is in part because the nature of the services being provided often includes the ongoing transfer of data to and from the consumer. The types of data being transmitted may vary over time, as may the uses to which it is put. It is difficult for a data collector to accurately "disclose" all such possible future uses to a data subject in a meaningful way at the outset.

The other type of services offered by the IoT involve the collection of information for use by a business or government (e.g. inventory management, transportation monitoring, energy usage and equipment repair sensors) which do not directly involve a transaction with, or the supply of a service to, a third party consumer. Therefore, the consumer protection framework will not typically apply to the operation of these services. However, the operation of these services may still create a range of important policy implications which are described further below.

The Telecommunications Act 1997 (Cth)

In Australia, telecommunications is centrally regulated by the Telecommunications Act 1997 (Cth) (Telco Act). The Telco Act removed all legislative barriers to entry into the telecommunications market and established an industry-specific access regime and anticompetitive conduct framework.

---

As well as the Telco Act, the industry is regulated by the Telecommunications (Consumer Protection and Service Standards) Act 1999 and a series of related codes, determinations and regulations.

The main stated objectives of the Telco Act are to provide a regulatory framework which promotes:

- the long-term interests of end-users of carriage services, or of services provided by means of carriage services; and
- the efficiency and international competitiveness of the Australian telecommunications industry.

The Telco Act seeks to regulate the telecommunications sector by addressing the activities of two main entities: carriers and service providers.

The Australian regulatory framework is a co-regulatory model, requiring carrier licensing only where a person owns a network unit which is used to supply carriage services to the public.

Operators of IoT devices will generally not (at least during the early stage of IoT) be carriers or carriage service providers because they will not be providing carriage services to the public. However, in most cases IoT communications need to pass over communications networks operated by private users (e.g. a local wifi network) and carriers. As mentioned above, where an IoT operator provides a content service over a carriage service, then that operator will also be a "service provider" for the purposes of the Telco Act and subject to the relevant service provider rules.

Experience from other technological developments suggests that over time, IoT operators may vertically integrate and therefore may in some cases end up operating proprietary networks used to support IoT services.

Issues for key stakeholders

We have set out below some of the main concerns that key stakeholders may have with the IoT.

Industry and service providers

Interoperability, interference and standards

Most industry members including the likes of Google, Huawei, HP, Samsung and IBM have already responded to the opportunity that the IoT brings but as Intel IoT group senior vice president and general manager recently said, the "IoT is a significant opportunity but one that needs interoperability and scale to fulfil industry predictions of billions of connected devices". For example, Cisco has just released details of its IoT system which is supposed to provide a comprehensive set of IoT technologies and products that simplify and accelerate the deployment of infrastructure for the IoT.

Should industry standards be developed to ensure devices do not interfere with each other?

Numbering plan issues

As a practical matter, there are currently two types of IP addresses in active use: IP version 4 and IP version 6. IPv4 was deployed in 1983 and is still the most commonly used version. Given the numeric basis for IP addresses, Asia, Europe and the US have already run out of IPv4 addresses. IPv6 which has been available since the 1990s caters for trillions of IP addresses and offers more efficient network management, better security and interoperability for mobile networks. Organisations that have been slow in upgrading their hardware for the new version, risk disrupting their ability to be able to serve new customers.

---

7 CommsWire No. 150701, 1 July 2015.
8 https://www.iana.org/numbers
Neither the Asia Pacific Network Information Centre (the regional internet registry for the Asia Pacific region) nor the Internet Assigned Numbers Authority (responsible for the global coordination of IP addresses) appear to have published explicit policy on the impact that the IoT will have on the demand, service levels and fee structures applicable to IP addresses.

**How should the industry respond to the demand that the IoT will have on IP addresses?**

**Roaming**

Roaming is an inherent issue associated with the IoT, since the vast majority of devices and sensors will be mobile and will therefore cross over network boundaries. Given that the rise of the IoT will place pressure on network capacity effective inter-carrier roaming services are a pre-requisite to its success. Domestic roaming is currently not regulated in Australia but governed by inter-carrier agreements. The need to implement an effective inter-carrier fee structure will be a precursor to the continuing growth of the IoT.

The ACCC last looked at whether it should declare mobile domestic inter-carrier roaming services in December 2004. Relevant to its conclusion that it was premature to declare the service was the view that the competition in the market for retail mobile services was not yet fully effective and that there were geographic barriers to achieving nationwide coverage (e.g. availability of spectrum, economies of scale and sunk costs).

The ACCC recognised that inter-carrier services were supplied through GSM and CDMA and that the competitive conditions were more favourable in the GSM inter-carrier roaming market than for CDMA, so that the declaration of GSM inter-carrier roaming services would be likely to promote competition at that time.

The ACCC was also not convinced (at that time) that declaring CDMA inter-carrier roaming services would promote competition as there was no data indicating that the terms and conditions in the market were unreasonable.

At a consumer level, the Australian government proposed an unrelated (to IoT) attempt to regulate international roaming charges (at least across the Tasman) and planned to introduce the *Telecommunications Legislation Amendment (International Mobile Roaming) Bill 2014* (IMR Bill) in 2015 but it is yet to be introduced into parliament and seems to have stalled. The major carriers (i.e. Optus, Telstra and Vodafone) made their objections to the IMR Bill clear.

If passed into law, the IMR Bill would permit the ACCC to determine price-control arrangements for (i) carriage services that are supplied by carriers or carriage service providers using Australian telecommunications networks to telecommunications businesses in specified foreign countries; and (ii) carriage services that are supplied to telecommunications businesses in those foreign countries which supply their customers with roaming services for their mobile devices while they are in Australia. Although this Bill is unrelated to IoT, it provides an example of how government may consider approaching regulation of roaming services more generally.

---

10 [http://www.pcmag.com/article2/0,2817,2376887,00.asp](http://www.pcmag.com/article2/0,2817,2376887,00.asp)
13 Section 151B TB.
What is the best way of ensuring inter-carrier roaming arrangements facilitate the growth of the IoT?

Spectrum allocation policy

Many personal IoT devices will send data to a smartphone or tablet via bluetooth with the smartphone or tablet then using a fixed or cellular network to send the data to the cloud. The increasing amount of traffic already passing through these networks (especially wireless) combined with the possible surge in demand from the IoT adds further demand to the ever increasing need for more mobile bandwidth.

For the IoT to be allowed to grow, the ISM band must be sufficiently large and fit for purpose to cater for the large number of devices that are likely to use the IoT. Large volumes of data (albeit in small packets) must be able to flow without constraint.

The current spectrum licensing regime largely grants licensees exclusive access to spectrum and has a relatively firm delineation between the class, apparatus and spectrum licence types. ACMA is presently considering ways to create a more flexible framework for spectrum access to balance the diversity and increasing number of uses and users.

Similar to its counterparts in the US and Europe, one of the options ACMA has been reviewing is the concept of spectrum sharing which could mean that wireless carriers would share spectrum with the federal government or spectrum would be shared on a geographic basis for machine-to-machine technology.

What changes (if any) are needed to spectrum allocation to ensure the growth of the IoT is not constrained?

Facilities sharing and installation of low impact facilities

Schedule 3 of the Telco Act allows carriers to install "low impact" facilities where the carrier provides the facilities generally for the purposes of supplying a carriage service. Low impact facilities are facilities which, because of their size and location, are considered as having a low visual impact. Examples include some radio communications facilities, the underground and overhead optical fibre installations undertaken by the NBN, some aerial cables, public payphones and emergency facilities.

A licence from ACMA is required if a carrier operates facilities (i.e. a network unit) used to supply telecommunications services to the public.

In most cases an IoT sensor will not be a network unit or a facility and so will not be specifically regulated by these parts of the Telco Act. This is because, in most cases, IoT sensors do not in themselves provide a carriage service but rather communicate with existing network units to transmit data.

There may however be in the future some IoT devices whose social utility justifies installation of dedicated network units to ensure uninterrupted communications, such as priority assistance, medical or security applications.

Consideration should therefore be given to whether the network infrastructure necessary to support these applications can be deployed so as to assist the IoT achieve the reliability, speed and reach that is required to help it reach its full potential.
How can industry be proactive in managing these infrastructure issues?

**Content providers**

As the IoT develops and involves increasing amounts of data, networks risk becoming congested. This raises the question of whether some data flows should be prioritised over others e.g. whether data associated with health monitoring devices such as (say) heart rate monitors or glucose readings should take priority over data flows updating a user’s calorie intake.

**Net neutrality**

The internet is broadly based on the principle of Net Neutrality which requires there be an open internet that allows users to go where they want, when they want.

In support of this principle, in February 2015, the US Federal Communications Commission (FCC) adopted a set of Open Internet rules which seek to protect and maintain open, uninhibited access to legal online content and prohibit ISPs from being allowed to block, impair or establish fast/slow lanes to lawful content.¹⁴

There is no equivalent rule in Australia, although there is a telecommunications interconnection access regime for declared services which is administered by the ACCC. This regime aims to facilitate third party access to certain services to promote the economically efficient operation and use of investment in infrastructure, and promote the effective competition in upstream and downstream markets. The declared services regime does not currently impose net neutrality rules on Australian carriers.

In contrast, the US FCC Open Internet rules apply to both fixed and mobile broadband service and involve three key principles:

1. **No blocking** – ISPs must not block access to legal content, applications, services or non-harmful devices.
2. **No throttling** – ISPs must not impair or degrade lawful internet traffic on the basis of content, applications, services or non-harmful devices.
3. **No paid prioritisation** – ISPs must not favour some lawful internet traffic over other lawful traffic in exchange for consideration of any kind (including from their affiliates).

The FCC has taken the position that bandwidth services are considered utilities (like water and gas) and therefore subject to considerable regulatory restrictions. These restrictions prevent ISPs from requesting additional fees for faster connection services or for blocking some types of content. Complaints for overcharging are investigated by the FCC.

The Open Internet rules do not have any specific IoT parameters yet, so it is uncertain how they would apply to situations where there may be a legitimate reason to prioritise certain enterprise traffic over others e.g. health monitoring applications or public safety applications or to de-prioritise certain non-essential services when traffic is congested.

The EU is taking a different position to the US and considering a more flexible approach which would allow ISPs to charge additional fees for special services. Some commentators suggest these different regulatory approaches may result in investments in Europe being more profitable than those in the US.

---

¹⁴ [https://www.fcc.gov/openinternet](https://www.fcc.gov/openinternet)
Should the IoT (or some aspects of it) be prioritised differently to other classes of traffic?

Government and law enforcement

Cybersecurity

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

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. 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. 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. The recommendations largely contain standard security protocols e.g. encryption, limited permissions, two-factor authentication and regular security evaluations but 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.

The FTC guidelines recognise that there is no one-size-fits all approach to guarantee the security of connected devices and that those companies which take the lead in providing consumers with confidence about how their data will be used, are the ones that are most likely to flourish the most 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 and 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 (see section on privacy below).

---

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”. 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.

In the absence of any specific legislation dealing with breaches of security for IoT devices, after a man hacked into a baby monitor in 2013, the FTC took its first action against an IoT firm on the basis of misleading or deceptive conduct. The FTC accused TRENDnet - a web enabled camera manufacturer for promising customers that its cameras were secure when they were not. The claim was settled on terms which 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.

Do the cyber security risks created by the IoT require a specific response?

International agreements

On a global scale, the US is spearheading a number of international treaties including the Trans-Pacific Partnership Agreement (TPP), 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, concerns regarding cybersecurity and privacy are exacerbated given the limited ability to control what another jurisdiction does with the data.

The TPP is a regional, regulatory and investment treaty involving the US and 11 other countries (i.e. Australia, Canada, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam). After five years of negotiations, the TPP was signed by the 12 member nations on 4 February 2016 in New Zealand. The member nations now have two years to ratify the agreement.

The stated objective of the TPP is to unlock opportunities for American manufacturers, workers, service providers, farmers and ranchers to support job creation and wage growth. The TPP also aims to promote e-commerce, keep the internet free and open, boost competitive access for telecommunications suppliers and set digital trade rules-of-the-road.

In particular, the TPP seeks to implement requirements that support a single, global internet, including ensuring cross-border data flows, consistent with governments’ legitimate interest in protecting privacy.

As part of the TPP, parties have committed to allowing service suppliers to electronically transfer information across borders if it is part of their business activity (subject to public policy objectives). The Australian government does not consider this commitment to affect Australia’s existing privacy framework. In addition, TPP parties have agreed to not impose requirements on service suppliers when they seek to use or build a local data centre in order to conduct business in a TPP party’s territory. Agreement has also been reached to not impose customs duties on electronic content.

---

20 http://www.fischer.senate.gov/public/_cache/files/2b3ad47d-f4df-4cb8-b6e3-877de18be0a8/ern15061.pdf
The TPP also contains some consumer protection measures for the online environment including adopting a legal framework to protect personal information of e-commerce users.

The TISA is another international treaty that is being jointly led by Australia, the US and the EU. There are currently 24 parties which collectively account for approximately 71% of global trade in services.26

The objective of the TISA is to supplement existing multilateral trade negotiations and set a new standard in services trade commitments to improve market access and new trade rules. The TISA will cover the financial, telecommunications and e-commerce industries, professional services, air transport and energy services, government procurement and also involve developing domestic regulation to reduce barriers to entry for those services.

The TISA negotiations are still in the early stages and are not carried out in public. It is difficult at this stage to determine the exact impact that it may have on the way information flowing across boundaries is regulated.

The TTIP is a proposed free trade agreement between the EU and US that aims to promote multilateral economic growth and in particular, open up the US to EU firms. A study by the Centre for Economic Policy Research27 estimates that EU exports to the US could increase by €187 billion and EU imports from the US could increase by €159 billion. In addition, EU and US exports to the rest of the world are estimated to increase by over €33 billion and €80 billion respectively.

In relation to e-commerce, information and communication technology services, the TTIP aims to “develop appropriate provisions to facilitate the use of e-commerce to support goods and services trade, such as through commitments not to impose customs duties on digital products or unjustifiability discriminate among products delivered electronically”. The TTIP also seeks to facilitate the movement of cross-border data flows.28

How should industry respond to these trade agreements?

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 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 may be able to tell when, how and to whom these communications have been made.

In what circumstances (if any) should an IoT device be subject to law enforcement surveillance and who should bear the costs of storing this data?

Personal and community

Privacy

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. Privacy law includes thirteen 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.

In addition to these privacy laws, Part 13 of the Telco Act contains specific data protection provisions and sets out strict rules for carriers, carriage service providers and others in the way they use and disclose the content of messages and information relating to their customers and services. Under the requirements of Part 13, carriage service providers are required to make records of all disclosures of personal information and are obliged to disclose personal information to law enforcement agencies in specified circumstances.

The privacy regime imposes a transparency framework for general personal information and a consent requirement for the collection of sensitive information, under which 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, in practice, data subjects:

- have little choice whether to deal with a particular organisation or to negotiate privacy terms; and
- have little control over the collection and use of that person’s information that is not sensitive information.

The transparency requirement regarding the collection, use, storage and disclosure of personal data under the privacy regime means that IoT applications provided by regulated persons must (in relation to personal information) provide details of who owns the sensor data, exactly what sensor 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.

Practical challenges can arise where information is collected by an IoT service provider from or regarding individuals active in a public space who are not subscribers to the service and who may become identifiable over time. In this case there is no "consent" by the affected person who is then only protected by surveillance laws and the common law.

Adding to the complexity of obtaining consent, the type of data collected by an IoT device and its uses may change over time. While consent may have been given initially for the then known uses, this 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. Consent in the context of the IoT may therefore not always be a feasible way of discharging an APP Entity’s privacy obligations.

Issues also arise in relation to the potential for data sets that do not initially contain personal or sensitive information to become regulated because over time or by combination with other data sets, the information captured becomes personal or sensitive. A good example of this is the power of location information. 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 aggregation of data was highlighted in the case brought by Ben Grubb against Telstra when it denied him access to his metadata. 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 (e.g. geo-location data) 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.

However on 18 December 2015, the Administrative Appeals Tribunal (AAT) reversed the Privacy Commissioner's decision that the metadata transmitted by Telstra was personal information, on the basis that the metadata was not "about" Mr Grubb as an individual, but rather about the way in which Telstra delivered calls or messages made by Mr Grubb. The Deputy President of the AAT was also satisfied that an IP address was not information about an individual but was about the means by which data is transmitted from a person's mobile device over the internet and a message sent to, or a connection made, with another person's mobile device. The fact that the network data relating to Mr Grubb would not have been generated without his use of Telstra's mobile network was not considered to be a relevant factor in determining whether the information was "about" Mr Grubb.

The outcome of this case highlights the uncertainty of the meaning of personal information, particularly in light of the limited judicial consideration to date.

A further example of how the APPs do not contemplate the IoT stems from the prohibition on APP entities from collecting personal information unless it is reasonably necessary for, or directly related to, one of more of the APP Entity's functions or activities. This may constrain the development of the IoT since APP Entities may want to collect information for anticipated future uses but for which there is no immediate need or seek to repurpose information already collected.

The complexity of the IoT and the limited transparency behind how data is handled and used, poses difficulties for enforcing privacy compliance. Data subjects are increasingly losing control over their data and the IoT has the potential to exacerbate this problem.

To address this concern, the FTC has suggested the "Reclaim Your Name" initiative which aims to regulate data brokers and involves the creation of consumer-friendly online services that enables data subjects to find out how data brokers are collecting and using their data. This transparency would allow users to hold data brokers accountable for the data they collect and how they use it.29

Data Protection Working Party

Recognising that traditional forms of notification are not always feasible in the IoT environment, the Article 29 Data Protection Working Party (Working Party) (an independent European advisory body on data protection and privacy) recommended that device manufacturers should develop a "common protocol to express preferences with regard to data collection and processing by data controllers especially when such data is collected by unobtrusive devices."30

This idea is also supported by the FTC in its call for app developers 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.31

In the EU and US therefore, the onus seems at least at this point, to be resting on IoT service providers to modify their technologies to be able to comply with existing privacy laws rather than amend existing privacy laws to cater for IoT nuances.

29 Brill, Julie, The Internet of Things: Building Trust and Maximising Benefits Through Consumer Control, 89 Fordham L. Rev. 205.
30 Opinion 8/2014 on the Recent Development on the Internet of Things.
Overseas disclosure

Given that the IoT involves enormous amounts of data being collected, stored and analysed, it is likely that APP Entities will outsource this function to specialist data brokers that may be located outside the jurisdiction in which the data subjects reside.

Before disclosing personal information to an overseas recipient, APP 8 requires the APP Entity to take reasonable steps to ensure the overseas recipient does not breach the APPs in relation to the information since the APP Entity may remain liable for any breach of the APPs by that overseas recipient. This means that Australian privacy law could have extraterritorial application, although how this works in practice is yet to be tested.

Maintenance of data

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.

In the IoT context, this requirement could involve thousands of requests from data subjects creating an enormous administrative burden, for which IoT service providers would be ill-equipped to handle.

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 it is unclear whether these data sets can be truly anonymised.

The EU approach

In its Opinion, the Working Party acknowledges the integration of IoT into every day lives of European citizens. It recognises the need for data subjects to remain in complete control of their personal data and for them to be able to provide fully informed, specific and voluntary consent.

Similar to the APPs, the EU data protection laws are based on disclosure and transparency regarding the use of information by device manufacturers, social or data platforms, devices lenders or third party developers. The laws also limit processing to legitimate purposes i.e. where processing of the data is “necessary for the performance of a contract to which the data subject is a party”.

The EU also only allows the processing of personal data if it is necessary for the data controller to pursue its legitimate interests except where those interests are outweighed by the interests or fundamental rights and freedoms of the data subject e.g. the right to privacy. This right is not currently recognised by Australian privacy law but (if it was included) would require APP Entities to not only consider the purposes for which they seek to collect personal information, but also the interests of the data subject.

The EU also supports the “purpose limitation principle” and the “data minimisation” principles which mean that data can only be collected for specified, explicit and legitimate purposes; and that the data collected should be strictly necessary for those purposes.

---

32 Opinion 8/2014 on the Recent Development on the Internet of Things.
The Working Party has identified a number of recommendations if the existing EU legal framework is to apply to the IoT. These recommendations include:

- before any new IoT applications are launched, a privacy impact assessment (PIA) should be completed and made available to the public at large (where feasible). The privacy impact assessment should be based on a specific IoT PIA framework to ensure its unique risks are identified;
- given that the value for many regulated entities is in the aggregated and not raw data, those entities must delete the raw data as soon as they have extracted the data required for their data processing;
- users must always retain control of their data according to the principle of self-determination of data;
- device manufacturers must break down the consent obtained from data subjects to identify the type of information captured and also the time and frequency of the collection and provide data subjects with a simple and quick way to disable sensors;
- users should be provided with a user-friendly tool to export their data; and
- application developers should design IoT applications to periodically notify users to remind them that their data is being collected.

Lastly, the Working Party also suggested that standardisation bodies should develop certified standards to govern IoT applications which would set the baseline for security and privacy safeguards for data subjects.

Alternative approaches (United Kingdom)

In the UK, Ofcom, the communications regulator consulted with a number of stakeholders at the end of 2014 about how to promote investment and innovation in the IoT.33 Whilst the consensus amongst the stakeholders was that the existing data protection regulations were appropriate and applicable to the IoT environment, some stakeholders also expressed support for Ofcom to take on a co-ordinating role in developing a common framework for data privacy with industry, government (including the UK privacy regulator - the Information Commissioner’s Office) and other regulatory authorities.

However, with respect to network security and resilience, stakeholders did not consider there to be much evidence to support new, IoT specific regulation in these areas but considered that IoT security measures should form part of general efforts to protect online services against malicious attack and that risks should be addressed through existing regulations.34

Other privacy related issues

Risk allocation in contracts

Given the number of stakeholders involved in delivering an IoT project, the line between data controller and data processor can become blurred and cross jurisdictional boundaries. Under UK law, a data controller is defined a person who determines the purposes for which and the manner in which personal information is to be processed. A data processor on the other hand is a person who processes the data on behalf of the data controller.

The allocation of risk and responsibilities between the parties must be defined clearly, in particular, which party bears the liability for any damage caused to the user of an IoT and which party owns the information generated by the IoT project. As a result, warranties and indemnities regarding data protection, security and privacy will become important to help draw the line between data controller and data processor (which are not defined in data protection regimes outside the EU and made all the more complex by the large number of stakeholders involved in an IoT environment).
To what extent (if any) should the current notification and consent based approach to protecting individual privacy be modified to cater for the complexity of the IoT? What role should industry play?

Consumer Law

Privacy protection under Consumer Law

The Australian Consumer Law (ACL) offers consumers protection when they purchase IoT products and in some cases represents an indirect way of enforcing privacy and security compliance.

Under the ACL, protection is given to "consumers", who 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.

The ACL establishes general standards of business conduct and contains a range of consumer protections, the most important of which are the provisions prohibiting a person in trade or commerce from engaging in misleading or deceptive conduct, or conduct which is likely to mislead or deceive. Where an IoT provider makes representations to a consumer about the attributes of an IoT product (e.g. quality, security, or reliability), it must therefore take care to ensure the representations can be substantiated to avoid falling foul of the misleading or deceptive conduct provisions of the ACL.

The ACL also prohibits unconscionable conduct which is assessed in light of the relative bargaining powers of the parties, the use of undue influence, pressure or unfair tactics by the stronger party and the willingness of the stronger party to negotiate. For business contracts with consumers (and small businesses, from 2016), the ACL also protects consumers against unfair contract terms. A term will be "unfair" if it would cause a significant imbalance in the parties' rights and obligations under the contract, is not reasonably necessary to protect the legitimate interests of the party that would be advantaged by the term, and would cause detriment to a party if it was relied on.

The ACL also contains some statutory consumer guarantees that cannot be excluded by contract (e.g. goods must be of acceptable quality, match their description, and fit for any purpose that the consumer makes known to the supplier). Any IoT product must meet the requirements of these guarantees.

So although the ACL does not contain any provisions specifically relating to the IoT, IoT service providers must observe the requirements of the ACL or risk having an action commenced against them either by a competitor or the ACCC.

Any new technology creates an area of regulatory focus but how does a supplier provide a consumer with sufficient information about the risks associated with the IoT product, given the evolving nature of the IoT?

Telecommunications Consumer Protection Code (TCP Code)

The TCP Code is an important industry code of conduct under the Telco Act. It contains community safeguards in the areas of sales, service and contracts, billing, credit and debt management, changing suppliers, and complaint handling. It also sets out a framework for code compliance and monitoring.
The TCP Code applies to all carriage service providers which supply Telecommunications Products to customers in Australia. Under the Telco Act, a Carriage Service Provider is a person who supplies a listed carriage service (i.e. a service that carries communications using electromagnetic energy either within Australia, or from/to a point in Australia) to the public. A Telecommunications Product includes a listed carriage service, a content service provided in connection with a carriage service, and any goods supplied by a carriage service provider for use in connection with the supply of either of them.

An IoT product will often not involve the provider acting as a carriage service provider, but the code may apply where the IoT operator supplies a carriage service to consumers. In this case, the TCP Code seek to protect consumers by requiring carriage service providers to provide consumers with specified essential information about the service, pricing and complaints handling mechanism and also places restrictions on how much and when the carriage service provider can bill.

**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 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 their 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 socially disadvantaged groups) 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 socially disadvantaged 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.

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.

35 Telecommunications Act 1997 (Cth), section 87(1).
36 Telecommunications Act 1997 (Cth), section 16.
37 TCP Code, section 2.
Do the potential social equity impacts of the IoT demand a broader policy response?

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

What is the best way of assigning liability when harm is caused by an IoT device?

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 its 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.
Appendix 1 – Additional examples of IoT applications

- Self-programming thermostats that automatically adjust the heating/cooling systems in a home based on occupant’s schedule.
- Smoke alarms that send warning messages to a user’s phone.\(^{30}\)
- Smart plugs - wifi enabled plugs which are placed between the wall socket and the plug for an appliance that can be turned on/off instantly using a smart phone.\(^{41}\)
- Wireless key locators \(^{42}\)
- Wifi controlled lighting - IP enabled lights that can be monitored, managed and controlled from any internet enabled device.\(^{43}\)
- Wireless home sensor systems - motion, light, moisture sensors that can be monitored from a computer, tablet or smartphone e.g. to detect burst water pipe, unexpected movement inside a home.\(^{44}\)
- Wireless plant monitoring - irrigation or sprinkler systems that can be triggered remotely using sensors.\(^{45}\)
- Smart rubbish bins that alert council services when the bin needs to be emptied.\(^{46}\)
- Parking space locators.
- Pollution alerts that send messages to residents to avoid polluting their waterways with raw sewerage during overflow events.\(^{47}\)
- Equipment maintenance and repair sensors that alert manufacturers if parts require maintenance or replacement.
- Fire extinguisher sensors that notify an owner when the extinguisher has not been placed in its designated location or when its pressure fails to meet safe operating levels.
- Structural integrity sensors that are embedded within concrete when it is poured to monitor the quality and integrity of the building, bridge or other structure.\(^{48}\)
- Lion tracking collars \(^{49}\)
- Environmental pollution monitors.
- River monitoring systems that track the movement of water, salinity levels and other contaminants.\(^{50}\)
- Smart pills which are ingested and monitor internal body health.
- Electronic toll collection systems
- Smart meters that provide consumers with real-time, localised energy consumption data to enhance urban electricity grids and enable utility providers to more accurately predict demand, locate power outages, resolve issues and ensure the stability and safety of the “smart grid”.\(^{51}\)
- Remote frequency identification tags on inventory
- Licence plate recognition technology
- Self-driving cars
- Wearable devices such as t-shirts, smart watches, game consoles and fitness bands that track and interpret specific and sensitive human data such as heart beat, eye movements and gait.\(^{52}\)
- Smart street lights that dim lights during hours of low activity and also track noise and pollution levels.

\(^{30}\) https://nest.com/smoke-co-alarm/life-with-nest-protect/
\(^{41}\) http://postscapes.com/wifi-locators
\(^{42}\) http://postscapes.com/smart-outlets
\(^{43}\) http://postscapes.com/wifi-key-locators
\(^{44}\) http://postscapes.com/home-wireless-sensor-systems
\(^{45}\) http://postscapes.com/wireless-plant-sensors
\(^{46}\) http://bigbelly.com/solutions/stations/
\(^{47}\) http://dontflush.me/about

\(^{49}\) http://home.groundlab.cc/lioncollars.html
\(^{50}\) http://float.berkeley.edu/
\(^{52}\) Finch, Kelsey and Tene, Omer, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town, 41 Fordham Urb.L.J. 1581 2013-2014.
Baker & McKenzie has been global since inception. Being global is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 4,200 lawyers in more than 45 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.