The Internet of Things and Australian Privacy Law

We are beginning to see the next big thing in Internet-related innovation. From Fitbit to Google Glass, the so-called 'Internet of Things', or the 'IoT', is poised to revolutionise the way we interact with the world. Inevitably, though, this innovative leap in consumer technology will present significant headaches for Australia's legislature and judiciary – in particular its potential to rapidly disrupt long-standing social and legal norms with respect to privacy. While this paper highlights the shortfalls of Australia's privacy law regime in light of the IoT, lawmakers should not impulsively and unnecessarily restrict these technologies. Rather, they must find the 'Goldilocks Zone', so to speak, between incentivising innovation and protecting privacy rights. That is, where any preemptive regulation is not too hard, not too soft, but just right.

What is the Internet of Things?

There is currently no universally accepted definition of the IoT, which, in itself, underlies the complexity faced by lawmakers around the world. According to the EU Commission, the concept is generally understood to be:

> *A long term technology and market development based on the connection of everyday objects to the Internet. Connected objects exchange, aggregate and process information on their physical environment to provide value added services to end-users, from individuals to companies to society as a whole.* [1]

In short, the IoT involves any 'thing' and every 'thing' connected to the Internet (and/or to other things and people) that allows the transfer of information without the need for personal computers. These wirelessly networked 'things' collect data, monitor activities and customise a user's experience to their needs or desires. The IoT is often synonymous with 'smart' technology, such as smart phones, smart homes and smart appliances.

By way of example, imagine your future refrigerator automatically ordering more milk for you the next time you are running low. Similarly, your toaster may one day be capable of deciding to sell itself after evaluating that you do not eat enough toast to justify having it.[2] While this example may sound ludicrous, it illustrates that the possibilities of the IoT are

[1] EU Commission, *Report on the Public Consultation on IoT Governance* (16 January 2013) http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746 (last accessed 26 April 2016)

[2] Philip Branch, 'How Will Data Retention Laws Cope With The Internet Of Things?' *Sydney Morning Herald*, 2005 <http://www.smh.com.au/digital-life/consumer-security/how-will-data-retention-laws-cope-with-the-internet-of-things-20150202-134gfd.html> (last accessed 28 April 2016)

endless. What will be commonplace items in the future could well be unimaginable today. It is estimated that by the year 2020, 50 to 100 billion devices will be connected in the IoT.[3]

New Threats to Privacy

There is some disagreement about what privacy means, what sort of rights it should include, and where those rights come from.[4] Historically, one's privacy was preserved because it was simply impossible to track a person's every move; however, this is becoming less and less the case.[5] Nevertheless, the IoT raises many difficult questions in relation to our contemporary view of privacy, such as who owns the data generated by these devices, where is the data stored, how secure is the data generated, what laws (domestic and international) regulate the IoT, and who can use the data and to what extent.

Today, it is common for corporations to collect data from individuals in exchange for free or lower-priced access to good and services,[6] such as Flybuys cards. However, the average consumer has no knowledge that this transaction is taking place, or, if they are, simply do not care. Given the all-encompassing nature of the IoT, it is likely more data about our speech, movements and bodies will be collected and stored by third parties without our knowledge and consent than ever before. Perhaps of particular concern in this respect are wearable technologies, such as Fitbits. While most Fitbit users may not care that their data is being stored, it is important that they have a clear understanding as to the extent that they are exposing their private information and how this information could be used in ways that affect them. For example, data generated by a Fitbit has already been used in a Canadian court case. [7] While the user in this case voluntarily produced the data to benefit her case, it is easy to imagine future cases where people are forced to disclose particular data generated by wearable technology to their detriment.

Most service providers online have terms and conditions which users agree to merely by using or by clicking on a gateway. The *Australian Consumer Law* to some extent protects

[3] Dr W Charlton Adams Jr, *Wired* <http://www.wired.com/insights/2014/12/iot-connected-person/> (last accessed 26 April 2016).
[4] Matt Moore and Kelly Tall, 'The Internet of Things: A Primer for Information Professionals' (2015) 29 *OLC* 7, at 10.
[5].Ibid.
[6] Ibid at 11.
[7] Parmy Olson, 'Fitbit Data Now Being Used in the Courtroom', *Forbes*, 2014 <http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#26691aa5209f > (last accessed 27 April 2016)

consumers from unfair bargains and pro forma contracts which exploit inequality of bargaining power. To the extent privacy rights exist, these agreements typically remove or limit them to the maximum extent. It remains to be seen how far Australian Courts will go in protecting privacy rights where consumers have contracted out of them.

The IoT also presents new opportunities for cybercriminals to access personal information. For example, in 2014 hackers hacked into household 'smart' appliances to implement a bot-network in order send spam emails via those appliances.[8] This scenario illustrates the potential security and privacy problems with having multiple devices interconnected with different IT-systems.[9] In this respect, it is impossible for all IT-systems to have strong, uniform security systems, particularly where the connection is international.

Further, consider the much-hyped Google Glass. These computerised glasses look like ordinary glasses except for a slim touchpad along an arm and a miniature see-through display screen; however, the Google Glass allows its user to record what he/she sees. This has prompted many places around the world to ban Google Glass, including casinos[10], cinemas[11] and bars[12]. Google has attempted to allay some privacy concerns about Google Glass by installing a light that turns on when the device is recording and banning any application capable of facial recognition.

The thought of ubiquitous surveillance is alarming for most Australians, which may prompt lawmakers to preemptively act against technologies like Google Glass. Indeed, it is arguable that privacy is as much about emotional reactions as it is about legal doctrine.[13] That is, while it may be more inconspicuous to take voyeuristic photographs with Google Glass than

[8] Julie Bort, 'Refrigerator Hacked: Here's the Biggest Problem Facing the Internet of Things', *Business Insider Australia*, 2014 <http://www.businessinsider.com.au/hackers-use-a-refridgerator-to-attack-businesses-2014-1> (last accessed 27 April 2016).
[9] Joachim Scherer and Caroline Heinickel, 'Regulating Machine-to-Machine Applications and Services in the Internet of Things (2014)2 *ENLR* , at 150.
[10] Wayne Parry, 'Casinos Ban Gamblers From Using Google Glass', *The Sydney Morning Herald*, 2013 <http://www.smh.com.au/digital-life/digital-life-news/casinos-ban-gamblers-from-using-google-glass-20130606-2ns3v.html> (last accessed 27 April 2016).
[11] James Vincent, 'Google Glass Banned From US Cinemas', *Independent*, 2014 <http://www.independent.co.uk/life-style/gadgets-and-tech/google-glass-banned-from-us-cinemas-9827833.html> (last accessed 27 April 2016).
[12] Carlos Castenada, 'Google Glass Wearers Banned From San Francisco SoMa Bar', *CBS*, 2014 <http://sanfrancisco.cbslocal.com/2014/03/04/san-francisco-soma-bar-bans-patrons-from-wearing-google-glass/> (last accessed 27 April 2016)
[13] Brian Wassom, 'Augmented Reality Law, Privacy and Ethics: Law, Society and Emerging AR Technologies (2014) *Syngress*, at pg 43.

a smartphone, Google Glass does not cause this behaviour. Unsolicited voyeuristic photographs were a problem before the advent of Google Glass, but Google Glass has heightened the public's insecurity about this pre-existing problem.[14] Accordingly, some commentators argue that devices such as Google Glass and other IoT devices do not create any privacy issues that have not previously long existed.[15]

Australia's Statutory Privacy Regime

The main Australian statute dealing with privacy is the *Privacy Act 1988* (Cth). While the *Privacy Act* applies to most Australian federal government agencies and most private organisations, it does not provide comprehensive privacy protection for Australians. The *Privacy Act* does not apply to a number of groups, including small businesses with an annual turnover of less than $3 million, political organisations, media organisations, and individual citizens acting in their personal, family or household affairs. For those bodies falling within the scope of the *Privacy Act*, they must abide by the 13 'Australian Privacy Principles' established by the *Privacy Act*.

The *Telecommunications Act 1997* (Cth) (**"Telco Act"**) also contains some data protection provisions. These provisions stipulate the way carriers, carriage service providers and other bodies must use and disclose personal information obtained during the supply of telecommunication services. It is an offence under the *Telco Act* for participants in the telecommunications industry – namely, carriers, carriage service providers, telecommunications contractors and their employees, and emergency call persons – to use or disclose certain information relating to communication carried by a carrier or carriage service provider, including the personal particulars of another person. Furthermore, the *Telco Act* requires carriers and carriage service providers to record certain disclosures of personal information.

The *Privacy Act* and *Telco Act* create a framework for the transparent collection, use and storage of personal information. Under this regime, collectors of your personal information are supposed to notify you about particular matters, including what information is being collected, how it is collected, and how it will be used and disclosed. In theory, a person who wants to control the collection and use of their personal information could consult the

[14] Whitney Erin Boesel, 'Google Glass Doesn't Have a Privacy Problem. You do'. *Time*. 2014 <http://time.com/103510/google-glass-privacy-foregrounding/> (accessed 27 April 2016).
[15] Ibid.

relevant public disclosures made by each respective service provider and elect to use their preferred provider. In reality, however, people have limited options in choosing their service providers and even less choice in negotiating the privacy terms of engagement with those providers. Consequently, consumers have little control over the collection and use of their personal information, except in circumstances where that personal information constitutes 'sensitive information' pursuant to the *Privacy Act*.

One of the main issues with the statutory privacy regime, particularly in relation to the rise of the IoT, are the regulatory loopholes caused by the small business exemption under the *Privacy Act*. As mentioned above, the *Privacy Act* generally does not apply to businesses with an annual turnover of $3 million or less. While telecommunications service providers with an annual turnover of less than $3 million must still comply with the privacy provisions under the *Telco Act*, these provisions merely regulate the use, retention and disclosure of information. Unlike the *Privacy Act*, the privacy provisions of the *Telco Act* do not regulate the collection and storage of personal information. Furthermore, it is possible for smaller organisations that are similar to telecommunications service providers to fall outside the scope of both the *Privacy Act* and *Telco Act*. This is particularly concerning given the development of communications technologies and e-commerce, which will continue to result in more businesses, including small to medium businesses, handling larger amount of personal information.[16] The risks to privacy are determined by the nature of the personal information, rather than the size of the business holding that personal information. It is, therefore, important that privacy regulations extend to small businesses.

Issues may also arise in protecting privacy in relation to data which does not initially contain personal information, but later does. For example, a location device, in isolation, would not normally generate personal information; however, if this data was combined with other data, such as mapping, the combined data may be able to generate a profile of the user. Over time, this profile may identify a user and reveal personal details, such as that person's residence, work address, health and other information. As it currently stands, Australia's statutory privacy regime does not contemplate increments of data capable of later constituting personal information.

[16] Australian Law Reform Commission, *Review of Australian Privacy Law*, (2007), [63.151]

Moreover, the rise of the IoT will leave the *Telco Act* significantly out of date. When the *Telco Act* first came into force, telephony was the only widespread and available communications service. Subsequent amendments to the *Telco Act* have done little to change this concept. As a result, there is some confusion as to how new technologies, such as voice over internet protocol (VoIP) among others, will apply to the *Telco Act*. VoIP enables verbal conversations to be conducted in real time over the internet. While VoIP services usually operate over a telecommunications network and are therefore covered by the *Telco Act*, many VoIP services only operate over Internet networks. In these circumstances, the service provider may fall outside the scope of the *Telco Act*. Furthermore, it is possible to access voices services from providers outside Australia. This may impact on the standards of protection for personal information disclosed during a VoIP call.[17]

Australia's Common Law Right to Privacy?

Outside the statutory regime, Australia has not developed a tort of invasion of privacy at common law.[18] Unlike the United States,[19] Australia does not have any express common law cause of action with respect to:

1. intrusion upon a person's seclusion or solitude, or into his/her private affairs;
2. public disclosure of embarrassing private facts about a person;
3. publicity which places a person in a false light in the public eye; or
4. appropriation, for the perpetrator's advantage, of a person's name or likeness.

Similarly, Australia does not recognise the extended concept of breach of confidence as accepted in the United Kingdom in relation to privacy rights.[20]

However, the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*[21] overturned the long-standing position in Australia that the common law provided no protection for personal privacy. This understanding was based on comments made obiter in the High Court decision *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*.[22] *Lenah* found the position adopted in *Victoria Park* to be incorrect and that there was no

[17] Office of the Privacy Commissioner, *Submission PR 215* (2007).
[18] *Kalaba v Commonwealth of Australia* [2004] FCA 763.
[19] *Time Inc v Hill* [1967] USSC 11; 385 US 374, at 383.
[20] *Campbell v Mirror Group Newspapers* [2004] UKHL 22.
[21] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 ("*Lenah Game Meats*").
[22] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, 496 (latham CJ), 521 (Evatt J) ("*Victoria Park*").

impediment to Australian Courts creating a cause of action for invasions of privacy. Indeed, Callinan J asserted:

> *It seems to me that, having regard to current conditions in this country, and developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made*.[23]

Since *Lenah*, only two lower Courts have recognised a tort of invasion of privacy: *Gross v Purvis*[24] in the District Court of Queensland and *Doe v Australian Broadcasting Corporation*[25] in the Country Court of Victoria. It remains unclear the likely direction of the future development of the Australian common law with respect to privacy rights.

Thinking Ahead

It is easy to forget that while privacy protection is important, so too is innovation, entrepreneurialism, economic growth, price competition, and consumer choice.[26] Finding the 'Goldilocks Zone' for regulating the IoT is a delicate predicament confronted by lawmakers. On one hand, many commentators advocate for tight, immediate preemptive regulation against the IoT on the basis that the mere potential for breaches of privacy warrants an urgent response.[27] Further, it is argued that the longer lawmakers take to act against the IoT, the harder it will be to do so.[28] One of the issues with breaches of privacy is that, like defamation, once it has been committed, it cannot be undone. In this respect, it is best to try to protect one's privacy rather than remedy any breach. On the other hand, the issue with overly precautious regulation is that it aims to predict the future and its hypothetical problems, which may or may not ever materialise. The consequence of such preemptive regulation is that it risks unnecessarily limiting innovations that may yield new and better ways of doing things.[29] While Australia's privacy laws are inadequate to deal with the rise of the IoT and need significant updates, lawmakers should not quash incentives for further innovation.

---

[23] *Lenah*, above n21, 328.
[24] *Grosse v Purvis* [2003] QDC 151.
[25] *Doe v Australian Broadcasting Corporation* [2007] VCC 281.
[26] Adam D. Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation' (2014) 11(2) *Richmond Journal of Law & Technology*, 2.
[27] Scott R. Peppet 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent',(2014) 93(85) *Texas Law Review* , 71.
[28] Ibid.
[29] Adam D. Thierer, above n26.

Conclusion

The advent of the IoT will see the world's paradigm of relationships shift to encompass people and people, people and things, and things and things. This exciting development has the potential to enhance our lives with numerous social and economic benefits. Equally, though, it has the potential to significantly threaten our privacy rights. It is clear that Australia's privacy laws are unprepared to tackle the IoT. Given the predicted rapid rise of the IoT, Courts cannot be expected to swiftly develop legal doctrines to protect our privacy. This is not how Courts work. Instead, carefully considered legislative amendments to the *Privacy Act* and *Telco Act* are required to address some of the loopholes in the current privacy regime and allay the public's concerns with respect to the IoT. Perhaps an entirely new statute is needed. Whatever the response, lawmakers must not stifle the potential of this significant technological advancement to lead real innovation.