Horizon Scanning Series

The Internet of Things

Legal, social and human rights challenges of the Internet of Things in Australia

This input paper was prepared by Kayleen Manwaring and Cachelin Hall

Suggested Citation

Manwaring, K and Hall, C (2019). Legal, social and human rights challenges of the Internet of Things in Australia. Input paper for the Horizon Scanning Project "The Internet of Things" on behalf of the Australian Council of Learned Academies, www.acola.org.

The views and opinions expressed in this report are those of the author and do not necessarily reflect the opinions of ACOLA.

A. Introduction

This paper responds to questions raised by the Australian Council of Learned Academies (ACOLA) regarding the social impact of the Internet of Things (IoT). The questions received include*: is it likely that privacy protections will be needed to govern IoT and interactions with individuals and groups? What are the specific privacy and security considerations for the internet of things? Are there specific human rights considerations for IoT? Will there be considerations for specific population groups or individuals? What civil or criminal liability considerations are required to govern the use of IoT technologies? What protections, if any, may be needed for businesses, industry, citizens etc?*

The emergence of the IoT and related technologies has already brought about significant sociotechnical change, and this is likely to continue. This change brings with it some significant benefits for society, particular in the areas of: assisting those with disabilities live more independent lives; in healthcare; in aged care; and in more efficient and sustainable infrastructure, transport, industry and agriculture. However, with this change has come the potential for 'regulatory disconnection', that is, where existing regulatory frameworks become disconnected from societal expectations due to the new things, behaviours and relationships made possible by emerging technologies. While the IoT may lead to benefits in our daily lives, people (particularly individuals) are exposed to a number of risks by the use of IoT devices, ranging from disclosure of private information, unwanted surveillance by the state and by corporate interests, physical injury, harassment and stalking, defects in the devices themselves, and risks to human rights, such as the potential for discrimination and barriers to the right to freedom of expression. Australia has no specific laws aimed at addressing IoT issues, and current laws intended to protect customers and citizens have gaps and uncertainties when dealing with IoT devices.[1]

B. Problems of definition

Despite the popularity of the term, the 'Internet of Things' has no agreed definition. Its meaning can differ widely amongst different interested parties, and it has evolved over time.[2] The lead author of this paper undertook an analysis of the history and evolution of this term and associated terms in 2015.[3] Since that time, use of the term has significantly increased in Australia and globally, particular in popular literature, but no real clarity or consensus has emerged. Scholarly work has tended (although not exclusively) towards a narrower definition, concentrating on the relevant enabling infrastructure, while the popular view tends to be broader in its scope and includes 'smart' devices, as well as incorporating (usually only by implication rather than expressly) related technologies as ubiquitous and pervasive computing, ambient intelligence, and smart environments. Common examples of the 'Internet of Things' (such as electronic door locks) sometimes do not even use do not use the TCP/IP Internet protocols, but simpler communication protocols such as Bluetooth and infra-red.[4]

We do not yet have the benefit of the Expert Working Group's decision as to the scope of an IoT definition. Therefore, in this paper the lead author has deliberately deviated from the narrower definitions, and adopted a more extensive approach[5], to give the broadest possible view of the issues that may arise. Consequently, the *applicability* of the issues discussed in this input paper will depend on the scope of the definition adopted by the Expert Working Group's Full Report.

For the purpose of this input paper, 'IoT devices' consist of objects (including buildings and living things) that are not inherently computerised, but into which have been embedded one or more *computer processors* with *data collection*, *data handling* and *data communication* capabilities. IoT devices may have interactions with living things, the physical world, other IoT devices and other computing devices or systems. Many IoT devices also have one or more the following attributes: **active capacity** (capability to act on the physical world), **adaptability** (context-awareness), **addressability** (unique address), **associability** with living beings, **autonomy**, **dependency** (on remote services or infrastructure), **geo-locatability**, **identifiability** (unique device identifier/s), **mobility** or **portability**, **operational, economic and social impact**, **network locatability**, **prevalence**, **use pattern**, **visibility**, **volatility** and **vulnerability**.[6] (More details on these attributes can be found at **Schedule 1**.) It is worthwhile noting that some definitions of the 'Internet of Things' exclude smartphones and tablets. However, when considering the social impact of the IoT, the role of these devices, particularly smartphones, cannot be ignored. These devices and the applications installed on them form an integral part of many systems in which other IoT devices participate, primarily as a remote controller and often the device to which data is transmitted and delivered to humans in an intelligible form.

When identifying the challenges for consumers, citizens, business and the public sector, it is important to consider the underlying complex and interrelated nature of IoT devices and the systems in which they participate. All IoT devices comprise a physical object or living thing, hardware in the form of a computer processor and software. Many IoT devices are also components of 'product–service packages', where services are provided alongside the IoT device as essential or optional elements of the functionality provided. Many IoT devices may be nested within a larger IoT device, or form elements of a larger, distributed system. Issues arising out of IoT devices may relate to a single IoT device, or to the whole or some elements of the 'ecosystem'[7] in which the IoT device participates.

Any or all of these elements of hardware, software, object or service may be supplied by different entities, as part of a private sale, such as in a smart home, or as part of systems used by the public, such as in smart cities. Other actors may also be relevant when assessing challenges to consumers, such as designers, component manufacturers, assemblers, importers, distributors, those providing software integration services and testers. This input paper uses the term 'provider network' to indicate the multitude of different actors involved in the provision of an IoT device and associated system, and use the term 'provider' to indicate an entity in the provider network.[8] Providers may include both private actors and those in the public sector, such as federal, state and local governments who are involved in the provision of IoT devices and systems. Customers can be individual consumers, corporate entities, not-for-profits, or public sector agencies.

C. Is it likely that privacy protections will be needed to govern IoT and interactions with individuals and groups? What are the specific privacy and security considerations for the internet of things?

Privacy and security aspects are undoubtedly important. However, there are also other areas where IoT can have a social impact. Therefore, this section not only deals with privacy and security, but also other challenges for customers, citizens, businesses and the public sector arising out of new things, activities and relationships made possible by IoT devices. These are classified into 5 areas: 1) imperfection; 2) provider control and support; 3) significant post-supply value; 4) complexity; and 5) choice (although note these categories may overlap).

1 Imperfection

Suppliers with low profit margins and limited experience in manufacturing computing products may have little incentive or capability to ensure IoT devices operate reliably. For example, many are vulnerable to remote security breaches, and where an IoT device (or something that it is connected to) has **active capacity**, it can cause *physical* or *psychological* harm, as well as *economic loss*. These sorts of losses may also occur from **volatile** access to resources, inaccuracy of data, and **autonomous** decision-making by IoT devices. How providers ultimately manage, or fail to manage, these risks may also be a challenge for consumers, citizens, business and the public sector.

1.1 Security incidents and other risks of failure

Vulnerability is an important attribute of IoT devices. Evidence is emerging that IoT devices are more prone to physical interference and remote attacks than conventional connected computers. Security vulnerabilities have been identified in IoT devices as diverse as: smart city lights;[9] smart meters;[10] security cameras;[11] shipping scanners;[12] smart home hubs;[13] fitness trackers;[14] smart televisions;[15] sex aids; medical devices such as insulin pumps, heart defibrillators, CT scanners, drug infusion pumps, X-ray systems and blood refrigeration units;[16] bathroom scales;[17] Internet-connected kettles;[18] baby monitors; children's toys[19] and location trackers;[20] sniper rifles[21] and cars.[22] Such measures are ripe for exploitation by criminal networks and terrorists, with potential to cause physical and mental injury, as well as economic loss.[23]

The increased risk of security exploits arises from security vulnerabilities in both the IoT devices themselves and the systems to which they are connected. These include: insecure network services; insecure interfaces; insecure software and firmware; lack of encryption; insufficient authentication and authorisation; insufficient security configurability; the storage of personal data; and the lack of physical safeguards.[24] The nature of many IoT devices manufacturers as consumer goods specialists rather than ICT specialists, the small size of many devices, and design flaws prohibiting software patches have all been cited as reasons why security problems arise so commonly in IoT devices.[25] Ransomware also offers a financial incentive to threaten harm. The rise and increased availability of 'hacking as a service' also makes it easier for more people to undertake cyber attacks.

Security attacks enabled by these vulnerabilities include unauthorised remote operation of the IoT device ('hacking') and/or the delivery of malware. When these attacks occur, sensitive data might be disclosed or modified, or the IoT device could be used to attack other IoT devices or conventional computers. Of course, such attacks are also delivered using conventional computers; what is more particular to IoT devices is the physical harm that might occur to the IoT device, surrounding objects and/or living things. The biggest potential for *physical* harm is likely to emerge when the attribute of **vulnerability** interacts with that of **mobility** and/or **active capacity**, such as when a security flaw is exploited allowing remote access to the controls of large mobile devices (such as cars), or the safety shutdown systems of industrial plant and equipment.

Many, if not most, IoT devices or their associated systems have the attribute of **volatility**: that is, limited or intermittent access to resources needed to operate, particularly network connections, energy sources and processing power. This constraint is a particular challenge for users of mobile IoT devices, where the size, weight and form of the IoT device dominate design decisions, for example the minimisation of power usage, which can negatively affect processing power and speed. For simple applications, this constraint may matter little; but for healthcare IoT devices, the draining of a power source or the loss of connectivity leading to loss of control can cause serious harm, even death. The strength of security measures that can be put in place also depends on the level of volatility.

Examples:

- in 2015 Fiat Chrysler recalled 1.4 million vehicles because security researchers proved they could break into smart cars' systems remotely and control brakes, steering and transmission.[26]
- In September 2016, the website of security journalist Brian Krebs experienced a distributed denial of service attack delivered primarily through IoT devices
- In October 2016, an estimated 100,000 hacked IoT devices, including a number of cameras and DVRs infected with the "Mirai botnet" malware, generated multiple DDoS attacks against servers owned by DNS services provider Dyn, bringing down many sites including Twitter, The Guardian, Netflix, Reddit, CNN and many others[27]
- In January 2017, a university was attacked by its own connected light bulbs, lamp posts and vending machines, slowing down its internet service. [28]
- the US Federal Trade Commission (FTC) has brought a number of actions, including:
  - in 2014 against SecurView, a baby monitor and security system, for allowing access to the video feed and audio remotely via Web interface or mobile application transmitted login and password information in clear format. The system was hacked in 2012 and the feeds of 700 cameras were posted online; [29] and
  - in 2017 against D-Link alleging that the IP camera and router manufacturer did not meet reasonable security standards, resulting in customer vulnerability (no incident was reported) [30]

1.2 Risky decision-making: inaccuracy and autonomy

All IoT devices can **collect**, **handle** and **communicate** data. However, data may be or become inaccurate during the IoT device's performance of any of these processes. Sensors can be misled by physical phenomena; algorithms can be wrong; data records can be corrupted.

Customers, the provider network and others who rely on accurate data (for example, users and receivers of insulin injections) are, of course, at risk of physical or other harm if such data is inaccurate. This is particularly the case where the IoT device has **autonomous** decision-making capabilities: decisions may be made for the user without adequate notification and/or capacity for manual override. Even before IoT devices were produced, risks were identified in autonomous objects with active capacity. In the mid-80s, two people died and others were injured when computerised radiotherapy machines in hospitals administered massive overdoses of radiation to patients, partially due to an incorrect zero value in a failsafe counter. Although the risks are not new, the increased prevalence of autonomous IoT devices can potentially increase the likelihood of such incidents occurring, particularly when such objects are also vulnerable to security breaches. For example, an error in the results of a continuous glucose monitor could lead to a dangerous overdose of insulin, or no insulin at all.

Even when data is accurate, IoT devices with some autonomous decision-making capability are risky. Decision-making algorithms could be programmed to result in outcomes not desired by the user. Customers rarely have access to such algorithms, and most are not equipped to understand them even if they did. Additionally, there are some machine learning technologies in development where even the original programmers may not be able to predict the results.

The existence of **autonomous** decision-making also raises a fundamental question of liability: for example, who should be liable for harm caused by a machine, or an unfavourable and unwanted contract entered into by a machine, which was not foreseeable by the machine's user (or indeed its programmer)? The application by judges of private law principles (such as in contract and tort) will mean that liability will be allocated in some form, but it may not be one that lives up to societal expectations around accountability.

Example:

- The accuracy of accelerometers,[31] fitness trackers,[32] and sleep trackers[33] have been challenged. Nevertheless, the data from such wearables has been used in criminal proceedings, including that for murder.[34]

1.3 Risk shifting and management

Risk management is complicated by the **complexity** of many IoT devices (see discussion at **section C.4.2** below), particularly when there are multiple players in the provider network. There are three main challenges when dealing with potential failures of IoT devices and systems:

- Proactive management of risk: what are the provider network's obligations in relation to monitoring and updating of software?
- When things go wrong: who is responsible for fixing problems with the IoT device?
- What contractual limitations will entities in the provider network attempt to place on their obligations regarding risk management?

Customer judgment on the adequacy of answers to these questions may be essential when choosing between competing products. Information that is not readily available, or is unintelligible or imprecise, may lead to customers making purchases for products without adequately understanding or being capable of dealing with the attendant risk. This harm is likely to be exacerbated by the practice, common in ICT contracting, of significant contractual limitation of liability by the supplier.

See related discussion in **section C.4.2** below.

2 Provider control and (lack of) support

The capacity of IoT devices for **data-handling** and **data communication**, and in some cases their **dependency** on remote services and infrastructure, exposes customers to a number of challenges. In many IoT devices the programmable computers they contain may be remotely accessed. As a result, their functionality, content and interoperability with other devices and other features can be controlled or modified remotely without the intervention, consent or even knowledge of the owner/user. In many circumstances, modifications (and certain types of control) cannot be put into effect by the customer, but only by a provider.

A connected IoT device can be remotely disabled from working, for example where a purchase instalment or a related service fee has not been paid. For example, starter interrupt devices (installed in approximately 2 million cars in the US by late 2014)[35] allow lenders or their agents to remotely disable a vehicle using their mobile phone, which they are contractually entitled to do when owners are late on car repayments. This ability to remotely disable an IoT device gives the provider network powerful new private enforcement capabilities, without the protections offered to a defendant in court proceedings.

Other forms of disablement are less direct, and much less likely to be subject to overt customer agreement or understanding. A provider may issue an upgrade to firmware or other software that reduces the speed of the IoT device's data-handling capabilities to a level that makes the hardware unusable. Or a service provider may go into liquidation or simply decide to discontinue a service, such as cloud data storage and processing. This can make the IoT device worthless to the customer, for example where the IoT device was designed to communicate only with a proprietary service. In the end, a customer may have no choice but to buy a new device with upgraded hardware, or to pay a premium price for an upgraded service. Other than the impact on individual customers, this adds to IoT's contribution to the world's e-waste problems.

Digital content that is resident in or accessed through IoT devices may also be blocked to protect rights holders; such as when there is no record of a user holding a licence to that content, but also in cases where the customer has not been involved in a breach of contract or any wrongdoing. It is worthwhile noting that in these situations, the IoT device as originally supplied to the user may well have been fit for purpose. It may be only afterwards, by a deliberate or inadvertent act by the supplier or someone else in the provider network, that the case becomes otherwise. Providers' ability to act in this way are often supported by non-negotiable contractual terms explicitly granting the right to such modifications.

Examples:

- Revolv's smart home hub hardware and application was shut down less than two years after release, after Revolv was acquired by Nest (a Google/Alphabet group company), who consequently refused to support the product.[36]
- in 2009, Amazon remotely deleted copies of the novel 1984 from customers' e-book readers when Amazon discovered it had been made available in its store by an unlicensed vendor;[37]
- the remote triggering of a starter interrupt device allegedly (1) prevented a mother from taking her asthmatic child to the hospital; and (2) forced a woman off the road when her car powered down;[38]
- owners of the Pebble smartwatch sold the intellectual property in their software to Fitbit and closed down the company, effectively invalidating warranties, as well as reducing competition in the smartwatch space.[39]

3 Significant post-supply value

The **use pattern** of IoT devices can mean that significant post-supply value can be exploited: for example, in reuse or sale of the data collected by the IoT device, or in the long-term recoupment of contractual premiums for licences or other services provided. Where End User Licence Agreements (EULAs) or Acceptable Use Policies (AUPs) are in place, providers may attempt to recoup value in contractual conditions that affect the use of the software or digital content in ways that the relevant intellectual property legislation does not.

For example, an IoT device may deliver post-sale value to a supplier in the following ways:

- data collected may be used to develop or market a provider's goods or services, or traded to third parties;
- ongoing service fees, such as for software maintenance and updates, or cloud data processing and handling;

- commissions for automatically ordered goods or services from a third party; and
- where data portability is restricted, customers can be effectively 'locked-in' to a particular brand.

3.1 Increased data collection: impacts on privacy

IoT devices enable increased data gathering and access to more intimate information.[40] Many IoT devices are **mobile**, and even for those that are embedded rather than mobile, the mobility of people interacting with the embedded object can increase the amount and variety of data collected, especially considering the increasing **prevalence** of IoT devices. The value of **geo-locational** and **data-collection** technologies for both corporates and the public sector has been enhanced by the **use pattern** of IoT devices, as they are likely to be 'personal'; that is, intimately associated with an individual. This personal use pattern greatly enhances both the value of the geo-locational functionality and the utility of the data gathered and communicated by the IoT device. The accuracy of geo-locational data is also assisted by the emerging use of 5G technologies.[41]

Data utility is also increased by the **adaptability** attribute (also known as 'context-awareness'). Adaptable IoT devices identify in real time some part of user context, and vary their responses accordingly. As the use of IoT devices becomes more widespread, this increases the likelihood that a greater quantity of data – and data that is more intimate and personalised in quality – can and will be collected and processed. However, often users' knowledge is limited as to: *what* and *how much* data is being collected; the *uses* of the data; *who* is receiving the data and for *how long* that data will be used.

The most common form of non-monetary consideration for IoT devices is a requirement of consent to the provision of personal data. Demand for data did not of course begin with the IoT, but the greater amount of data made available by IoT devices, based on the **prevalence** and **mobility** of such objects, considerably increases the likelihood of providers requiring data as a mandatory part of the consideration for the supply contract. Even when consent is ostensibly 'given' by the user, this is usually done in the context of 'take it or leave it' contracts, with vague, incomprehensible or overly long privacy policies, negating any real choice by the user.

The developmental tendency of the design of many IoT devices towards reduced **visibility** can also affect this situation, to the detriment of the customer. Unobtrusiveness of the data-gathering function in many IoT devices can intensify existing problems around data collection, storage and redistribution. The IoT device may be effectively invisible, or just its data-gathering function. This level of visibility may also reduce or exclude any real choice for consumers or citizens in controlling the collection, use or third-party distribution of their information.[42]

Examples of breach of privacy:

- Consumer electronics company Vizio recently agreed to pay US regulators US$2.2 million, after allegedly failing to get appropriate consent from users to track their smart TV viewing habits[43]
- in February 2019 Google revealed that its Nest Secure home security systems contained a microphone capable of picking up voice commands and other sounds. This feature was not included in the specifications of the product since its launch in 2017.[44]
- private conversations recorded by smart home hubs such as Amazon's Alexa have been inadvertently sent as voice files to third parties[45]

- In 2016, a class action was brought against Standard Innovation (US) Corp, the manufacturer of the 'We-Vibe' vibrator. Customers and their partners can pair the We-Vibe via Bluetooth with a smart phone to allow for remote control of the device. The plaintiff alleged that the manufacturer programmed the smartphone app to:

  > *secretly collect intimate details about its customers' use of the We-Vibe, including the date and time of each use, the vibration intensity level[,]… mode or pattern selected by the user … and … the email address of We-Vibe customers … allowing [Standard Innovation] to link the usage information to specific customer accounts.*

  The complaint alleged this was done without customers' consent or knowledge. The litigation was settled on 9 March 2017, for CAD5 million.

3.2 Post-supply restrictions

Post-supply restrictions on the customer may arise in many different ways. For example, customers may be required to enter into an ongoing service contract, such as for cloud data processing and storage, which provides an additional revenue stream. All IoT devices contain some form of software, and some types, such as e-book readers and networked media players, will also contain a substantial amount of digital content aside from software. Therefore, intellectual property constraints may also be leveraged by the provider to protect potential revenue streams. For example:

- the IoT device may not be 'sold' to the customer, in the sense of granting full transfer of property rights – the supply contract may be a lease or licence, imposing an obligation to return the IoT device on breach or termination;
- the supply may be subject to restrictive licence terms for the software or other digital content, such as those restricting copying, modification or particular types of use (included in separate agreements such as End User Licence Agreements (EULAs) or alternatively in the supply agreement itself).; and
- the original set-up of the IoT device may impose mandatory and irreversible personalisation of the IoT device (such as usernames, inability to delete data).

Such post-supply restrictions may pose challenges for customers such as:

- post-supply notification: customers may not be aware at the time they ordered the IoT device that the post-supply obligations would apply or be mandatory, such as when an agreement to a EULA is required as part of set-up;
- greater restrictions on use compared with a non-IoT device version;
- greater restrictions on resale by customers even when the physical IoT device is owned and not leased or licensed, as the EULA on software essential to the functionality of the IoT device may be non-transferable; and
- more significant penalties for breach of use restrictions, such as those contained in anti-hacking and/or copyright legislation, as opposed to civil remedies for contractual breach.

For example, if customers wish to make their own repairs to an IoT device, such as a connected vehicle, they may need to access integrated software, and face both legal and technical barriers to do so (as providers may rely on revenue from after-sale services). Software modification without provider consent will in many cases be a breach of the EULA and/or copyright legislation. Modification may also be technically impossible without circumventing technological protection mechanisms (TPMs), usually an illegal act in itself. Providers might also use their remote disablement capacity (see **section C.2**) to lock down software for a perceived breach of copyright law or contract[1]ual conditions.

These types of post-supply obligations can severely restrict a customer's choice, not necessarily of the first purchase of the IoT device, but as to third-party service providers and the subsequent purchase of other products. As a result, competition may be fettered.

Example:

- For several years, US farmers have been disputing the attempts of Deere & Company (John Deere) and other manufacturers to restrict their rights to repair their Internet-connected agricultural machinery, which contains embedded software and TPMs. In 2015, against the objections of John Deere and others, the US Copyright Office granted a three-year exemption for vehicle software modification to the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA). A year later, John Deere issued a licence agreement which prohibits almost all software modification and circumvention of TPMs, in what appears to be an attempt to replace its DMCA rights with contractual rights and ensure that all repairs are done by John Deere contractors.

4 Complexity

Two types of complexity produce significant challenges:

- the complexity of the technology itself; and
- the complexity of the contractual arrangements associated with supply.

Most IoT devices are inherently complex, due to their interactions with living things, the physical world, other IoT devices and/or other computing devices and systems. Many IoT devices are hybrids of object, software, hardware and service/s, as functionality often requires associated services to be acquired, such as access to cloud data handling facilities and a website interface. Even more complexity arises when IoT devices' embedment in larger systems is considered. Many entities can be involved in providing the hardware, software, object and services involved. Systems with nested and/or multiple IoT devices, or multiple IoT devices interacting with conventional computing, such as smart homes, can be very complex, both technically and in terms of associated service contracts.

The nature of IoT device ecosystems promotes the likelihood of numerous actors in the provider network. A complex network means complexity in contractual arrangements and therefore liability allocation. Even a basic IoT device such as a thermostat may require many separate contracts dealing with hardware, software development, software licences, installation, website and app usage, payment services, connectivity provision, sale, distribution and rental. These contracts may be with separate entities, some having no connection with (or knowledge of) others in the network.

The complexity of contractual arrangements within a network can make it difficult to identify all applicable contracts, let alone interpret them for end-customers (including enterprises) and network actors.

[1]

4.1 Making an informed choice

A customer entering into a contract requires sufficient, accurate and intelligible information on the nature, features and dependencies of the product or service. A supplier of a simple product needs only provide minimal information to fulfil this requirement. The complexity of IoT devices, particularly product-service packages, dictates that more than minimal information is required to sufficiently inform a customer. And mere provision of information by one supplier is insufficient—the customer's knowledge of alternatives on offer and their judgment of the price and quality differences are also required.

Customers face three main challenges to receiving adequate Information:

- the type of information required (content);
- whether the customer can adequately understand the information provided (intelligibility); and
- when and how the information is provided (delivery mechanism).

(a) Content

Customer knowledge of the IoT device's functionality is important, as is its suitability for the customer's particular purposes. Knowledge of 'normal' functionality is usually insufficient, particularly for IoT devices with significant **volatility** and/or **dependencies**: such IoT devices face significant limitations on functionality in particular situations.

Knowing exactly what the IoT device does enables customers to assess whether it meets their needs. This knowledge is also important because the post-supply value of IoT devices (particularly data collection) can incentivise suppliers to include features that benefit the supplier or others in the provider network but are a disbenefit to customers and therefore affect their purchasing decision. Such functionality may be invisible or unobtrusive; overt disclosure of this 'dark' functionality may need to be formally required, otherwise customers may remain unaware of it.

Aside from functionality, the attribute of **dependency** and the nature of IoT device interactions mean specific information on *interoperability* is often critical. Particular systems may only allow add-in of particular brands of IoT devices, thereby restricting customers' freedom of choice.

Clear information on price is fundamental to any customer contract. This includes not just the price of initial supply, but also follow-on costs, such as purchase of additional applications, subscription fees for service agreements and costs of consumables. Customers should also be aware of non-money considerations, such as post-supply obligations, for example in relation to data and use restrictions.

Ascertaining payment terms and the consequences of failure to pay may also be problematic, particularly when billing is done by more than one provider network entity. Payment terms, such as due dates and price increases, may vary greatly between entities.

(b) Intelligibility

An additional information challenge inherent in complexity is that 'customers cannot make well informed decisions when they are presented with information that is incomplete, misleading, overly complex or too voluminous'. Opaque wording and technical terms are the norm for software and hardware contracts, and initial research indicates this has not changed for IoT devices. The content provided may be accurate, but if it is not intelligible to the average customer, it is insufficient to enable an informed choice.

Careless drafting adds to this problem. Researchers have identified terms and conditions in contracts involving IoT devices that contain wording obviously written for older technologies, or wording drafted for one jurisdiction in contracts made for another.

(c) Delivery mechanism

An IoT device or associated system may be designed so that interactions are **invisible** or at least unobtrusive. This is often achieved by removing or miniaturising text-supporting interfaces such as screens. Such interfaces cannot practically be used to deliver most contractual terms and conditions. Clear delivery of full terms before purchase of IoT devices is not ubiquitous. Customers may be given the price upfront on purchasing the product, but not be presented with other terms and conditions (such as EULAs, service agreements and maintenance agreements) until well into the set-up process—that is, after the product has been ordered, delivered, unpacked and partially or even fully set up.

These contractual processes may encourage customers to enter into contracts with significantly limited access to terms and conditions and, consequently, a reduced ability to understand the bargain.

Therefore, customers may face challenges in finding out the terms and conditions applicable to their IoT device, particularly in relation to data usage. A common provider's right to unilateral amendment may exacerbate this problem.

4.2 Redress and liability allocation

The complexity of IoT device ecosystems can hamper the allocation of liability for faults. Where a single supplier provides the hardware, software and associated services, liability allocation is relatively simple, limited only by whether the type of harm is legitimately excluded under the contract. But where there are multiple providers, the issue becomes uncertain. The complexity of the technology and the contractual arrangements produces a significant challenge for customers. Defects in an IoT device ecosystem causing detriment to customers can arise in several places, including physical faults in the dominant object or embedded computer hardware, bugs in the software, corruption or deletion of data or failure of network connections. And the overall detriment may arise from a combination of defects, as where a network failure corrupts data, causing the IoT device to fail to recognise critical inputs.

Even where liability is clear, the mobile nature of IoT devices and the differing locations of provider network actors can make practical enforcement difficult. Australian customers are particularly affected, as most IoT devices they purchase are imported, with contracts likely to contain foreign jurisdiction and foreign law clauses. Contract drafters for provider networks also inevitably attempt to avoid liability, using favourable jurisdiction and choice of law clauses, or arbitration and class action waivers—practices already common in conventional ecommerce. These impediments, combined with the usually low value of a customer claim relative to legal costs, often hinder customers achieving redress.

All of these uncertainties are likely to obstruct proper redress for both public and private sector customers, particularly in relation to low-value contracts. However, customers are not the only ones facing detrimental effects. Uncertainty about the legal liability of provider network actors may hinder investment and innovation in IoT devices.

Examples:

- the Nest thermostat system is sold subject to at least 13 different documents containing information on the 'rights, obligations and responsibilities of the various parties' in the provider network.[46]

- the sets of terms and conditions purported to apply to sales of the Amazon Dash Button contain limitation of liability clauses that conflict with each other. One clause attempts to limit liability to zero,[47] the other to USD50.[48]

5 Adverse effects on choice

Some attributes in IoT devices can remove or impede customers' freedom of choice. For example, an IoT device with significant autonomy may make decisions that cannot be overridden (or not easily so) or are not even obvious to the user due to the invisibility of the device or the decision-making process.

5.1 Data-based discrimination

See **section D** below.

5.2 Customer 'lock out'

The **prevalence** of IoT devices and their post-sale value as data collectors, may lead to a scarcity problem: non-IoT device versions of customer products may become unavailable. Customers with legitimate concerns about the disbenefits of IoT devices, such as in the areas of privacy and security, may find it practically impossible to opt out.

Where dependency on remote resources is essential to the functionality of a particular IoT device, this can also lock certain customers out. Regional and rural areas may not have the connectivity required for particular IoT devices. If it is not profitable to make non-IoT device versions, then rural and regional residents may have to function without the object at all.

5.3 Digital consumer manipulation

In 2015, evidence presented to a US enquiry asserted that existing smartphone sensors could be used to infer:

> a user's mood; stress levels; personality type; bipolar disorder; demographics (eg gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.

In 2017, access to databases containing contact details of 'wheelchair and insulin users, of people addicted to alcohol, drugs, and gambling, as well as ... suffering from breast cancer, HIV, clinical depression, impotence, and vaginal infections' were offered on a commercial basis.

This type of information can be very valuable to a marketer attempting to persuade customers to buy their products. In fact, a number of attributes present in IoT devices are helpful to such a marketer, particularly when viewed in conjunction with the development of sophisticated data-processing techniques. Use of IoT devices in data collection, as marketing delivery mechanisms, and as purchasing devices may give firms an enhanced ability to engage in forms of 'digital consumer manipulation': not only targeting customer preferences but exploiting customers' cognitive biases and individual vulnerabilities. For example, advertisers may filter the available information; they may target customers at the time when their willpower is lowest; or they may craft their advertisements to act upon known purchasing triggers of particular individuals, for example, feelings of guilt or obligation, or concerns about missing out, or a desire to emulate friends or celebrities.

Currently, most examples of digital consumer manipulation have been identified in conventional ecommerce. However, the utility of IoT devices in these practices is obvious, particularly with their potential for increased capacity and intimacy of data collection. Customers have always been on the receiving end of persuasive tactics from advertisers, but data collected by IoT devices will arguably provide significant advantages to marketers in accuracy, scope, scale and effectiveness. The impact of scale in particular may be amplified by the implementation of software that allows tracking across different customer devices, particularly if done without the knowledge of the customer. The key question is 'at which point digital marketing practices, and in particular if they are based on intrinsic data analysis, opaque algorithms and sophisticated forms of persuasion, turn the normally "average" customer into a vulnerable one'.

Generally, society accepts that a marketer's job is to convince a customer to do something: but it is unclear when this type of behaviour would cross over from 'normal' marketing practice into something that is considered to be unacceptable to society. Should those with particular 'vulnerability profiles' be able to claim greater protection than the 'average' customer? Someone who is persuaded to buy a face cream just because his favourite celebrity's voice is used on a dynamic advertising screen to persuade him to take advantage of a discount as he passes the cosmetics aisle in his local department store may be considered as not worthy of protection; but in contrast, there may be an opposite attitude towards the targeting of a habitual gambler with an offer of an extended limit on her credit card as she passes a betting shop.[49]

Examples:

- Beacon implementations use indoor positioning devices and systems with small low power sensors to track when subscribers carrying their smartphones enter a particular physical space (such as the shoe aisle in a department store). This geolocational tracking triggers an action by applications in the mobile phone, such as notifications as to nearby items which are then offered at a discount. Beacon implementations have the potential to be programmed to act in accordance with copious research on how customers actually make purchasing decisions.[50] in October 2018, a member of Chemist Warehouse's IT architecture team announced that the pharmacy business was 'considering' installing thousands of sensors to track foot traffic within its stores and where consumers 'dwell in particular areas [and] … pick up products and look at them'.[51]
- The ACCC has identified addressable television advertising through use of smart televisions as a risk factor for digital consumer manipulation;[52]
- A European study into the specific health applications concluded that independent decision-making was likely to be circumvented due to the framing of economic choices in health applications as health or welfare choices[53]

D. Are there specific human rights considerations for IoT?

In July 2018, the Human Rights Commission (**HRC**) released an issues paper as part of its Human Rights and Technology Project, which mentioned briefly that IoT devices could 'present … platforms for cybercrime'.[54] However, the challenges raised by IoT devices in relation to human rights extend well beyond cybercrime. As this paper shows, the introduction of IoT devices may have negative implications for human rights to privacy, safety, security, non-discrimination and equal treatment,[55] as well as civil political rights such as freedom of information, opinion and expression, freedom of assembly, and the right to take part in public affairs.

Section 3 above discusses challenges for citizens and consumers in relation to privacy and security. This section will discuss other human rights issues.

Discrimination and equal treatment

1 Commercial services

Data can be used to decide whether to offer particular products or services to consumers, or to vary the conditions on which those products or services are offered, dependent on the attributes of the individual consumer.

For example, in the US, health insurers already provide discounts to those who give access to their fitness tracker data, in effect charging a premium to those who do not. Further, discriminatory practices may extend well beyond pricing. Insurers may well refuse cover – or only offer limited cover – to those who refuse access to install a telematics device in their car, which generates personalised data about their driving behaviour (as they do already with discount car insurance). Economically disadvantaged consumers may not be able to afford the relevant product or service without the discount, and therefore will find it impossible to opt out of providing their data. Insurers already have access to a lot of data, but the nature of this data is significantly different, in particular because it is intimate, intensive and timely.

Some forms of data-based discrimination are already unlawful in many jurisdictions, such as refusing to supply goods or services, or supplying them on less favourable terms, to people of a particular race. However, other forms of discriminatory conduct, such as price discrimination[56] based on data provision conditions, can be engaged in without legal restrictions. The possibility that fundamental human rights can be undermined by both lawful and unlawful discriminatory conduct is real and urgent.

Data-based discrimination can be deliberate or unintended. One area of particular concern is that of 'algorithmic discrimination', where the often relatively small and/or selective datasets used in machine learning contain societal biases. For example, there is a significant literature emerging relating to algorithmic discrimination on the basis of data collected on race, gender, health status, socio-economic status and other variables, affecting areas such as employment opportunities, housing, policing and sentencing policies. In early 2017, Amazon abandoned its use and further development of a recruiting tool that used machine learning because they had discovered it 'was not rating candidates for software developer jobs and other technical posts in a gender-neutral way'. Allegedly, this was due to the nature of the training dataset used.

While different forms of discrimination have a long history, the challenge for consumers lies in the fact that inferences drawn from data are often inscrutable or difficult to perceive. Providers may conceal or obfuscate the reasoning behind their decisions without any real prospect of the consumer finding out the 'real' reasons. Additionally, in some cases the inscrutability of the inferences extends even to providers themselves. Providers may use third party products or services where the third-party refuses to reveal their data collection techniques or processing to protect their commercial investment. It also may be due simply to the design of the process, as machine learning algorithms generally not only do not, but arguably cannot, provide explanations that humans can understand. So, a provider may refuse, or be unable, to reveal the real reasons behind inferences based on data collected by IoT devices.

Examples:

- In the US, some health insurers provide discounts to those who give access to their fitness tracker data, in effect charging a premium to those who do not.[57]

2 State services, surveillance and civil and political human rights

Example

- The current protests in Hong Kong provide a potent illustration of perceived problems with IoT devices in relation to civil and political rights to freedom of expression and opinion, freedom of assembly and the right to take part in public affairs. Protesters are shunning the use of smart cards for public transport, with their **identifiability** leading to the fear they will be tracked by law enforcement. Protesters are also wearing masks and tearing down smart lampposts, reportedly in fear of the use of facial recognition technology embedded in IoT devices. The government has denied that such technology is being used in the lampposts, but the limited **visibility** of exactly what technology is being used in these particular IoT devices has led to significant distrust.[58]

E. Will there be considerations for specific population groups or individuals?

Children

Security, privacy and manipulation for commercial purposes Children as a vulnerable group nevertheless appear to be the target of digital consumer manipulation enabled by IoT devices. The Norwegian Customer Council (NCC) has published research showing the Bluetooth connection for Genesis Toys' 'My Friend Cayla' and 'i-Que Robot' dolls was completely insecure (no authentication mechanism) and some queries were using insecure HTTP connections (subject to a man in the middle attack). The NCC also found that these dolls recorded anything said to them by children and sent the recordings to US-based Nuance Communications, a specialist in speech recognition. The company reserved the right to share and use the data for a broad range of purposes. Additionally, the NCC found that the toys were programmed with standard phrases endorsing commercial products, such as Disney movies.[59]

Women

Security, physical and mental harm There have been reports both in Australia and overseas of the use of IoT devices to facilitate intimate partner/family violence.[60]

Those with disabilities, the ill, the elderly, and those at a socioeconomic disadvantage

Dependency and the impact on choice The increased dependency of those with disabilities on particular health, communication or mobility IoT technologies may make them more ready to accept adverse terms, such as overreaching data collection, use and processing terms, or overcharging. They may also be more susceptible to digital consumer manipulation.

Minority populations

There is the possibility that IoT devices might be used to deny services to minorities, based on residence, race, ethnicity, socioeconomic status. For example, facial recognition software could be used to deny access to certain geographical areas. Also, flawed data sets and algorithms for facial recognition technologies have already been blamed for the inability of facial recognition technologies to properly recognise people of colour, particularly women. This can lead to problems such as additional screening at airports.[61]

F. Are there specific considerations with respect to citizen and business access to data?

With the advent of smart cities, and additional IoT devices used in government-monitored facilities such as airports and welfare agencies, local, state and federal public sector agencies are likely to collect, use and distribute a large amount of data. Both state and federal governments have recently encouraged the substantial sharing and release of public data. For example, in 2015, NSW passed the *Government Information (Public Access) Act 2009* (GIPA Act). The GIPA Act also covers local councils. More recently, the Federal government, has reflected that interest and is currently in the consultation phase for drafting a *Data Sharing and Release Act* that is proposed to cover federal agencies, and also the agencies of those states and territories who wish to join.

The specific considerations that are likely to be applicable for data arising from IoT devices use, particularly in an environment where data sharing and release are encouraged, include:

- how to ensure the privacy of those whose data has been collected;
- the need for secure environments for data storage and transmission all along the sharing chain;
- the use of de-identified data sets, with the understanding that anonymisation has some limits and re-identification of anonymised datasets can be possible;
- the extent to which public data should be allowed to be made available for commercial use;
- accountability for problems, such as data breaches, unauthorised disclosures, and re-identification.

It is worth noting that the Federal government's current position is that consent will *not* be required for all uses of public data.[62] Additionally, it has not yet made a decision on whether commercial use will be allowed.[63]

In August 2019, the government passed the Treasury Laws Amendment (Consumer Data Right) Act 2018 (Cth). The Consumer Data Right (CDR) is intended to provide a right for consumers to require data portability from commercial entities in order to 'improve consumer control over the data which businesses hold about [them,] … make it easier for them to find a better deal and share their information only with partners they trust'.[64] However, the CDR in its currently proposed form provides a very limited right. The CDR has been introduced to the banking sector first, with the energy and telecommunication sectors to follow. This is proposed to be followed by other sectors 'over time'.[65]

G. What civil or criminal liability considerations are required to govern the use of IoT technologies? (e.g. the device manufacturer, network provider platform operator, the application provider)? What protections, if any, may be needed for businesses, industry, citizens etc?

These are significant question that is far too substantial to be answered in a report of this type.

There is as yet no IoT-specific legal rules that apply in Australia, and very few in other jurisdictions. This is not to say that IoT is not regulated. There exists a substantial amount of legislation general enough in application, and sufficiently adaptable common law and equitable principles, to apply to a variety of new products, activities and relationships brought about by IoT devices.[66]

However, there are still likely to be legal problems arising, or gaps in appropriate protection, in many different areas of law, all of which will need to be examined *in detail* to establish the precise nature of these gaps. Problems are likely to arise in one or more of these 4 categories in relation to existing legal and regulatory frameworks:

(1) uncertainty of application;

(2) over- or under-inclusivity;

(3) obsolescence; or

(4) new harms that have not yet been addressed.[67]

Significant *potential* for legal problems, or *actual* legal problems, in Australia have already been identified in a number of legal areas. Usually, this has been in the context of protecting citizens, consumers and businesses against the risks outlined earlier in this report. These problem areas include:

- Data protection and privacy (particularly in the *Privacy Act 1988* (Cth));[68]
- Consumer protection (particularly in the *Australian Consumer Law*, and common law and equitable principles governing business-to-consumer contracts, especially consumer guarantees and product liability,[69] misleading and deceptive conduct and false representations, unconscionable conduct,[70] unfair contract terms[71]);
- Criminal prohibitions and enforcement in relation to cyber attacks (particularly in relation to the criminal codes in each state, territory and federally); [72]
- Intellectual property (particularly the *Copyright Act*, and its interaction with contract and licensing law); [73]
- Dataveillance of: 1) citizens by the state; and 2) consumers by corporate interests;[74]
- Competition law (*Competition and Consumer Act 2010* (Cth), particularly in relation to the potential declaration of roaming IoT services[75]
- Spectrum allocation[76]
- Product liability law and insurance law (particularly around automated vehicles and other machines with autonomous decision-making capabilities)[77]
- Ethics (for example, in autonomous decision-making)[78]
- Network neutrality[79]
- Discrimination[80]
- The definition of 'goods' in sale of goods legislation and other legislation[81]
- Retention of metadata[82]
- Fairness and validity of private enforcement of legal rights through remote disablement and similar provider control mechanisms[83]
- Liability allocation and enforcement issues against providers due to privity of contract and the use of subsidiaries with limited equity as contracting parties[84]
- Validity of evidence derived from IoT devices in investigations and litigation[85]

Examples:

- **'Hacking'**: Although unauthorised remote intrusion is already a criminal offence in many jurisdictions, technologically-specific drafting may mean that criminal legislation may be under-inclusive of IoT devices.[86] For example, the WA Criminal Code confines hacking offences to unlawful access to *password-protected* computer systems.[87] Many IoT devices (particularly inexpensive ones) are *not* password-protected, and the buyer (be they customer, business or public sector) usually has no capacity to implement password protection for themselves, usually due to product and system design.[88] Furthermore, even when rules do cover all relevant conduct, they may nevertheless be ineffective if they cannot be enforced. A hacker may well be in breach of a 'no access without lawful excuse' rule, but hackers may be undiscoverable or located out of the jurisdiction, making it difficult to enforce criminal penalties.[89]

- **Privacy breaches:** a recent examination of the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth) stated that 'the APPs have significant regulatory uncertainties or gaps when it comes to [IoT] privacy'[90] and that '[t]he APPs are too weak to meet [IoT] challenges and based upon current OAIC strategy and government under-resourcing, are unlikely to exert a positive influence over the promotion of privacy into the future'[91]
- **Digital consumer manipulation:** a recent analysis has concluded that Australia's consumer protection laws are inadequate to protect against this practice, due to the existence of legal problems of *uncertainty* and the failure to protect against a *new harm* (that of corporate secrecy)[92]

H. Progress to date

Industry initiatives in Australia

In 2017, Australia's peak industry body associated with the IoT, IoT Alliance Australia (**IoTAA**), issued a guide for business[93] and two successive versions of an Internet of Things Security Guideline[94] in an attempt to deal with emerging concerns about IoT devices and systems.

The IoTAA was particularly concerned with issues around: multiple parties and separation of parties (customers are unaware of how to reduce security vulnerabilities and other risks, they are also unaware of data use and collection); reach (IoT has access to intimate environments without full disclosure of data use and collection); undue reliance upon consumers to understand and mitigate risks; and IoT security concerns (may lead to unacceptable security vulnerabilities).

The IoTAA have developed a Good Data Guide, suggesting principles by which businesses should abide in dealing with consumers. These principles include:

- **accountability:** eg for data flows, for the implementation of privacy by design and security by design principles; for compliance with laws; for adequate disclosure
- **customer empowerment:** unfair or unreasonable risk-shifting to customers
- **cyber protection:** eg implement security by design; processes for updates, data breaches
- **data transparency**: full and fair disclosure, provide comprehensible information
- **data minimisation**: collection and handling limited, de-identification if possible, guard against re-identification; and
- **customer data control:** portability, disclosure of IP/confidentiality limits, log of disclosures (especially to state agencies).[95]

These are useful principles: however the lead author suggests that these should not be left up to providers (both private and public sector) to implement. Approaches beyond the self-regulatory must be considered, including co-regulatory approaches and legislative change where appropriate.

Regulatory and government initiatives

The government has commissioned two reports that provide useful assistance in establishing the issues arising around IoT devices and systems. The Productivity Commission's 2017 report on data use and availability mentioned the increasing use of IoT devices as sources of data collection,[96] and contained a case study which included some examples of IoT devices and potential disbenefits.[97]

The Australian Competition and Consumer Commission (ACCC) in its recent *Digital Platforms Inquiry* recognised a number of challenges posed by IoT devices as part of the recent Digital Platforms Inquiry, but found that the 'wider impact'[98] of such technologies was still too unclear to form a foundation for specific recommendations to government other than that policymakers should 'actively engage with the implications of these developments when formulating policy, and considering regulatory reform'.[99] Its recommendations were confined to digital platforms, but nevertheless some may be helpful in assisting with some of the issues raised by IoT devices and systems, in particular digital consumer manipulation and other data-based harms.

There are some significant problems with the Privacy Act in relation to the IoT, in particular:

- threshold requirements exclude many businesses from its operation.[100] There are also other important exemptions from some of its provisions, such as disclosures to related bodies corporate,[101] acts or practices outside Australia[102] and employee records;[103]
- many types of consumer data may not be subject to the Privacy Act due to a narrow judicial interpretation of the meaning of 'personal information';[104]
- enforcement mechanisms are weak, particularly for consumers. No direct right of action is available to consumers, although under section 36 of the Privacy Act they may make a 'complaint' to the regulator, the OAIC. OAIC decisions relating to complaints are only subject to appeal where the OAIC makes a 'determination' under section 52 of the Privacy Act. Few such determinations have been made under this provision,[105] and this has resulted in a paucity of appellate jurisprudential development.
- historically, sanctions have been insubstantial (for example, enforceable undertakings and small compensation amounts). Where compensation has been awarded, the amounts have been too small to have any meaningful deterrent effect.[106] No civil penalties (available up to AUD2.1 million) have been awarded since their introduction in 2014.[107]
- insufficient funding and resourcing of the OAIC, restricting its capacity to bring actions, has also been the subject of public criticism.[108]

Further, and most importantly, 'consent' overrides most safeguards for consumers in relation to the use of consumer data, and its transfer to third parties. The consent required is weak, and its adequacy to protect data subjects has been vigorously contested.[109] Commercial entities are permitted to deal with consumer data even though in most cases the nominal consumer consent obtained is not informed, is non-negotiable, and is subject to unilateral interpretation and extension at the will of the commercial party. In some cases, such as in direct marketing, where it is 'impracticable to obtain consent',[110] even the requirement of weak consent is disregarded. This problem is exacerbated by forms of consent and privacy policies that are lengthy, difficult to understand, ambiguous, hard to find, vague and/or overly broad.[111] Empirical evidence suggests this encourages consumers not to read most policies or to helplessly accept unfavourable terms because '[i]t [is] the only way to access the product or service'.[112] For all of these reasons, the Privacy Act is limited in its protections against data-based harms.[113]

However, some of the relevant ACCC recommendations for reform in the *Digital Platforms Inquiry* addressing some of the above shortcomings are also relevant to data-based harms arising in the context of IoT devices and systems. Properly implemented, they are likely to be helpful in addressing some of the above concerns. These recommendations are:

In the Privacy Act 1988 (Cth)[114]

1 Recommendation 16(a):

- broader definition of 'personal information';

2 Recommendation 16(c):

- The imposition of an *informed* consent requirement, in particular where collection, use or disclosure of the data is not necessary for the performance of a contract (or as a result of a legal or public interest reason); and
- the introduction of default settings for consent that are pro-consumer and not bundled;

3 Recommendation 16(e):

- a direct right of action for individuals; Recommendation 18:
- greater information requirements that align more closely to what consumers want to know, including a requirement that the name and contact details for each third party to whom personal information will be disclosed;
- more sophisticated user control, including the use of personalised and global opt-in and opt-out controls; and
- additional restrictions on children's personal information collected or used for targeted advertising or profiling purposes

In the Competition and Consumer Act 2010 (Cth)[115]

4 Recommendation 21: further prohibitions on unfair practices, including:

- Collection or disclosure of consumer data without express informed consent;
- Inducing consent by 'relying on long and complex contracts, or all or nothing click wrap consents, and providing insufficient time or information that would enable consumer to properly consider the contract terms'[116]

I. Conclusion

The emergence of the IoT has enabled and will continue to enable significant social impact, with a wide range of new devices, conduct and relationships emerging. The relevant technologies are still developing, and may still take divergent paths. However, in navigating this change, society must deal with risky and imperfect technologies, a loss of control and choice for consumers, citizens and other users, possibilities of exploitative conduct by corporate interests, the dangers of overzealous state surveillance and blind acceptance of autonomous decision-making by machines despite their potential for error and discriminatory practices. It must deal with the introduction of new complexities, not only in the technologies themselves, but in the legal and social arrangements surrounding their use. The potential for disconnection between these challenges and current legal regimes adds to these problems, as well as threats to human rights.

This input report aims to contribute to flagging the danger areas for consumers, citizens, businesses and the public sector and to make a call for thoughtful engagement by policy makers, judges and legislators with the challenges posed by the IoT. Initial ignorance of the effects of IoT is now giving way to a body of consumers and citizens who are both fearful and disempowered. Time and again over the course of researching IoT since 2012 the lead author of this input report has seen reactions to sociotechnical change as one of 'Hobson's choice'. Consumers feel that they must accept a technology with all of its attendant problems, or refuse to use it at all. If this distrust is taken to extremes for the IoT, this may lead to a denial of the great potential of some of these technologies to actually make life significantly better: for example, in assisting those with disabilities, in healthcare, in aged care, in efficient infrastructure, transport, industry and agriculture.

A lesson can be learned from the history of consumer protection law, which has been a continuing war against the dangers of a 'caveat emptor' approach. When consumer protection battles have been won, the resulting safety net for and consequent increasing trust by consumers has actually encouraged the development of new products and industries. In the past, society has been able to reach some form of consensus on what types of conduct is unacceptable by state and corporates, and regulate accordingly. The use and abuse of the IoT may currently fit only awkwardly within our current regulatory regimes, but there is no reason why this fit cannot be made better. The 'change' in sociotechnical change is also a crucial consideration: one-off solutions will likely be insufficient to deal with the continuing evolution of these technologies, so effective mechanisms for continuing evolution in law and policy must also be put in place. These mechanisms should include pro-active and swiftly reactive policy and rule-making bodies and processes, the use of appropriate language and interpretative principles in legislation and judicial decision-making, and well-resourced, informed and activist regulators.

Lead Author: Kayleen Manwaring,[117] Senior Lecturer, School of Taxation & Business Law, UNSW Sydney; Associate, The Allens Hub for Law, Technology & Innovation; Member, Cyber Security Law and Governance Network; Member, Centre for Law, Markets & Regulation

Cachelin Hall,[118] Research Assistant, School of Taxation & Business Law, UNSW Sydney also provided valuable research and writing assistance. However, all opinions are those of the lead author's.

Schedule 1 – Core and common attributes of IoT devices

Core Attributes

Object: physical object, natural or artificial, inert or living

Computer: contains one or more general-purpose programmable computers

Embedded: one or more computers physically embedded

Data collection: contains one or more sensors that can collect or generate data

Data handling: capability to process data

Data communication: can communicate with other nodes inside the same object, or with other objects

Common Attributes

Active capacity: can act on physical world

Adaptability: context-aware

Addressability: has a unique address

Associability with living beings: humans, plants, animals

Autonomy: decision-making capabilities

Dependency: remote services or infrastructure

Geo-locatability: can be found in physical space

Identifiability: has an identifier for the physical object

Network locatability: locatable in virtual space

Mobility: eObjects may be operational while moving within a physical space, when used by a person on the move or acting autonomously

Operational, economic and social impact: eObjects have both benefits and detriments

Portability: object can be moved but no connectivity while mobile

Prevalence: pervasive or ubiquitous

Use pattern: used by an individual, or small numbers, or large numbers

Visibility: can be unobtrusive or invisible, or contain different levels of implicit human-computer interaction

Volatility: connectivity, energy, storage and processing capabilities may be limited or intermittent

Vulnerability: risk of security breaches, theft, and physical damage or destruction

Schedule 2 – Additional resources

Australian perspectives

Australian Competition and Consumer Commission, Digital Platforms Inquiry: Final Report (June 2019), section 8.2 (New devices, new data)

Bosua R and others, 'Privacy in a world of the Internet of Things: A Legal and Regulatory Perspective' (2017) Networked Society Institute Research Paper 6

Manwaring K, 'Emerging information technologies: challenges for customers' (2017) 17 Oxford University Commonwealth Law Journal 265

—— , 'Kickstarting reconnection: an approach to legal problems arising from emerging technologies' (2017) 22 Deakin Law Review 51

—— , 'Surfing the third wave of computing: Consumer Contracting with IoT devices in Australia' (PhD thesis, UNSW 2019) available from the author

—— , 'Will emerging information technologies outpace customer protection law? The case of digital consumer manipulation' (2018) 26 Competition and Customer Law Journal 141

Manwaring K and Clarke R, 'Surfing the third wave of computing: a framework for research into IoT devices' (2015) 31 Computer Law & Security Review 586

Mathews-Hunt K, 'customer-IOT: where every thing collides. Promoting customer internet of things protection in Australia' (SJD minor thesis, Bond University 2018) available at https://pure.bond.edu.au/ws/portalfiles/portal/29084291/THESIS_FINAL_30_SEPT_2017.pdf

Productivity Commission, Data Availability and Use (Inquiry Report No 82, March 2017) (Appendix G, Case Study: Data from your Internet activities and intelligent devices)

Richardson M and others, 'Privacy and the Internet of Things' (2016) 21 Media & Arts Law Review 336

Richardson M and others, 'Towards responsive regulation of the Internet of Things: Australian perspectives' (2017) 6 Internet Policy Review

Vulkanovski A, Home, Tweet Home: Implications of the Connected Home, Human and Habitat on Australian Customers (Australian Communications Customer Action Network, February 2016)

IoT Alliance Australia, Good Data Practice: A Guide for Business to Consumer Internet of Things Services for Australia V1.0, November 2017)

Overseas perspectives

Coll L and Simpson R, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (Consumers International, April 2016)

Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World* (January 2015)

Acknowledgements: This report drew significantly from the research conducted by the lead author for her doctoral dissertation, so thanks is given to her PhD supervisors, Lyria Bennett Moses, and Leon Trakman, Professors at UNSW Law School, and Roger Clarke, Visiting Professor UNSW Law and ANU College of Engineering and Computer Science, and Principal, Xamax Consulting. Thanks also to Peter Leonard, Professor of Practice at the Schools of Taxation & Business Law and Information Systems & Technology Management, UNSW Sydney, and Principal, Data Synergies Pty Ltd for the provision of valuable resources.

However all opinions, errors and omissions are those of the lead author's.

[1] Kayleen Manwaring, 'Six things every customer should know about the 'Internet of Things'', *The Conversation* (online, 8 June 2017) http://theconversation.com/six-things-every-customer-should-know-about-the-internet-of-things-78765.

[2] Kayleen Manwaring and Roger Clarke, 'Surfing the third wave of computing: a framework for research into IoT devices' (2015) 31 Computer Law & Security Review 586.

[3] Ibid 595-598.

[4] For example, August Smart Lock. See Bonnie Cha, 'A Beginner's Guide to Understanding the Internet of Things' (*recode,* 15 January 2015) http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/.

[5] Developed in the doctoral work of the lead author and published in Manwaring and Clarke, 'Surfing the third wave of computing: a framework for research into IoT devices' (n 2).

[6] Ibid 598-601; Kayleen Manwaring, 'Emerging information technologies: challenges for customers' (2017) 17 Oxford University Commonwealth Law Journal 265, 267-8.

[7] The term 'ecosystem' was adopted from Guido Noto La Diega and Ian Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (2016) 7 European Journal of Law and Technology and Christopher Millard, W Kuan Hon and Jatinder Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (Proceedings of the 2017 IEEE International Conference on Cloud Engineering, Vancouver, 4-7 April 2017).

[8] Manwaring, 'Emerging information technologies: challenges for customers' (n 6) 269.

[9] Danielle Correa, 'IoT lightbulb worm takes over all smart lights until entire city is infected', (*SC Magazine UK*, 10 November 2016), https://www.scmagazineuk.com/iot-lightbulb-worm-takes-smart-lights-until-entire-city-infected/article/1475933

[10] BBC News, 'Smart meters can be hacked to cut power bills', http://www.bbc.com/news/technology-29643276, Oct 2014

[11] Brian Buntz, '5 Cybersecurity Lessons Related to IP Security Cameras', (*IoT World Today*, 31 August 2019), https://www.iotworldtoday.com/2019/08/31/5-cybersecurity-lessons-related-to-ip-security-cameras/

[12] Eduard Kovacs, 'Hackers Attack Shipping and Logistics Firms Using Malware-Laden Handheld Scanners', (*Security Week*, 10 July 2014), https://www.securityweek.com/hackers-attack-shipping-and-logistics-firms-using-malware-laden-handheld-scanners.

[13] Zack Whittaker, 'Security flaws in a popular smart home hub let hackers unlock front doors', (*Techcrunch*, 3 July 2019), https://techcrunch.com/2019/07/02/smart-home-hub-flaws-unlock-doors/

[14] For example, Fitbit. Mahmudur Rahman, Bogdan Carbunar and Madhusudan Banik, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013) arXiv:13045672 [csCR]; Mario Ballano Barcena, Candid Wueest and Hon Lau, How Safe is Your Quantified Self? (Symantec Security Response Report, 11 August 2014)..

[15] Consumer Reports, 'Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds' (*Consumer Reports*, 7 February 2018) www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/.

[16] Anthony M Townsend, Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia (WW Norton & Co 2013) 269; Kim Zetter, 'Medical Devices That Are Vulnerable to Life-Threatening Hacks' (*Wired,* 24 November 2015) www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x.

[17] Vijay Sivaraman and others, *Inside job: security and privacy threats for smart-home IoT devices* (Australian Communications Consumer Action Network, 2017).

[18] Catalin Cimpanu, 'Insecure Internet-Connected Kettles Help Researchers Crack WiFi Networks across London' (*Softpedia,* 20 October 2015) http://news.softpedia.com/news/insecure-internet-connected-kettles-help-researchers-crack-wifi-networks-across-london-494895.shtml.

[19] ForbrukerRadet (Norwegian Consumer Council), 'Connected Toys Violate European Consumer Law' www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/.

[20] Lorenzo Franceschi-Bicchierai, ‘A GPS Tracker for Kids Had a Bug That Would Let Hackers Stalk Them’ (*Motherboard*, 3 February 2016) https://motherboard.vice.com/en_us/article/bmvnzz/a-gps-tracker-for-kids-had-a-bug-that-would-let-hackers-stalk-them .

[21] Andy Greenberg and Kim Zetter, ‘How the Internet of Things Got Hacked’ (*Wired*, 28 December 2015) www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/.

[22] Andy Greenberg, ‘Hackers Remotely Kill a Jeep on the Highway – With Me in It’ (*Wired,* 21 July 2015) www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Stephen Checkoway and others, ‘Comprehensive Experimental Analyses of Automotive Attack Surfaces’ (Proceedings of USENIX Security 2011, August 2011); Nick Bilton, ‘Disruptions: As New Targets for Hackers, Your Car and Your House’ *The New York Times* (New York, 11 August 2013) http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?_r=0.

[23] Kayleen Manwaring, ‘Surfing the third wave of computing: Consumer Contracting with IoT devices in Australia’ (PhD thesis, University of New South Wales 2019), Ch 5, para 3.1.1.

[24] This is a consolidated list adapted from the Open Web Application Security Project, Top 10 IoT Vulnerabilities (2014) Project Open Web Application Security Project Wiki https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_Io, cited in Kayleen Manwaring, ‘Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies’ (2017) 22 *Deakin Law Review* 53.

[25] Scott R Peppet, ‘Regulating the Internet of Things: First Steps Toward Managing Discrimination,Privacy, Security & Consent’ (2014) 93 Texas Law Review 85, 135–36; Bruce Schneier, ‘The Internet of Things Is Wildly Insecure – And Often Unpatchable’ (*Wired*, 1 June 2014) http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-ofthings-and-thats-a-huge-problem/.

[26] Kayleen Manwaring, ‘Six things every customer should know about the ‘Internet of Things’’, (*The Conversation,* 8 June 2017) http://theconversation.com/six-things-every-customer-should-know-about-the-internet-of-things-78765.

[27] KrebsOnSecurity, “Hacked cameras, DVRs powered today’s massive internet outage”, https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/, Oct 2016

[28] Verizon, ‘IoT calamity: the Panda Monium’, (*Data Breach Digest*, January 2017), http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf

[29] In Re TRENDnet, INC; FTC Matter/File Number: 122 3090, https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

[30] *Federal Trade Commission v. D-Link Corporation and D-Link Systems*, FTC Matter/File Number: 132 3157, https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link. For a list of other vulnerable devices, see Vijay Sivaraman and others, *Inside job: security and privacy threats for smart-home IoT devices* (Australian Communications Consumer Action Network, 2017).

[31] KL Dannecker and others, ‘A Comparison of Energy Expenditure Estimation of Several Physical Activity Monitors’ (2013) 45 Medicine and Science in Sports and Exercise 2105.

[32] Simon Hill, ‘How accurate are fitness trackers and does it matter? We asked an expert’, (*Digital Trends*, 18 July 2019), https://www.digitaltrends.com/wearables/how-accurate-are-fitness-trackers/.

[33] HE Montgomery-Downs, SP Insana and JA Bond, ‘Movement Toward a Novel Activity Monitoring Device’ (2012) 16 *Sleep Breath* 913.

[34] Lauren Smiley, ‘A Brutal Murder, a Wearable Witness, and an Unlikely Suspect’, (*Wired*, 17 September 2019), https://www.wired.com/story/telltale-heart-fitbit-murder/.

[35] Michael Corkery and Jessica Silver-Greenberg, ‘Miss a Payment? Good Luck Moving That Car’ *The New York Times* (New York, 24 September 2014) http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/?_php=true&_type=blogs&ref=business&_r=0.

[36] Woodrow Hartzog and Evan Selinger, ‘The Internet of Heirlooms and Disposable Things’ (2016) 17 North Carolina Journal of Law & Technology 581, 584.

[37] Brad Stone, ‘Amazon Erases Orwell Books from Kindle’ *The New York Times* (New York, 18 July 2009) www.nytimes.com/2009/07/18/technology/companies/18amazon.html.

[38] Ibid.

[39] Pebble, ‘Pebble’s Next Step’ (7 December 2016) https://blog.getpebble.com/2016/12/07/fitbit/#more-1032 accessed 11 July 2018. As of 24 April 2019, this site had been shut down. The lead author acknowledges a personal interest in this: she owned a Pebble watch for two months and was just about to return it under warranty due to a fault when the announcement was made.

[40] Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report* (June 2019) 513.

[41] Ibid 514.

[42] Manwaring, ‘Emerging information technologies: challenges for customers’ (n 6) 280.

[43] https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf

[44] Sydney Fussell, ‘The Microphones That May Be Hidden in Your Home’ *The Atlantic* (23 February 2019) www.theatlantic.com/technology/archive/2019/02/googles-home-security-devices-had-hidden-microphones/583387/.

[45] Hamza Shaban, ‘An Amazon Echo Recorded a Family’s Conversation, Then Sent it to a Random Person in Their Contacts, Report Says’ *Washington Post* (Washington, 24 May 2018) www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says.

[46] Noto La Diega and Walden, ‘Contracting for the “Internet of Things”: Looking into the Nest’ (n 7).

[47] Amazon, ‘Conditions of Use’ www.amazon.com/gp/help/customer/display.html?nodeId=201909000 accessed 11 July 2018, clause entitled ‘Disclaimer of Warranties and Limitation of Liability’.

[48] Amazon, ‘Amazon Dash Replenishment Terms of Use’ www.amazon.com/gp/help/customer/display.html?nodeId=201730770 accessed 12 July 2018, clause entitled ‘Disclaimer of Warranties and Limitation of Liability’.

[49] Manwaring, ‘Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies’ (n 24) 74.

[50] Ibid.

[51] Ry Crozier, ‘Chemist Warehouse Could Create an Internet of Medicine’ (*iTnews*, 18 October 2018) www.itnews.com.au/news/chemist-warehouse-could-create-an-internet-of-medicine-514130.

[52] ACCC, *Digital Platforms Inquiry: Final Report* (n 40) 515-516.

[53] Manwaring, ‘Surfing the third wave of computing: Consumer Contracting with IoT devices in Australia’ (n 23) 245

[54] Human Rights Commission, *Human Rights and Technology* (Issues Paper, July 2018) 16.

[55] A Yu and others, *Response to Issues Paper on Human Rights and Technology* (2018) 2.

[56] ACCC, *Digital Platforms Inquiry: Final Report* (n 40) 517.

[57] Lauren Smiley, ‘A Brutal Murder, a Wearable Witness, and an Unlikely Suspect’, (*Wired*, 17 September 2019), https://www.wired.com/story/telltale-heart-fitbit-murder/

[58] https://www.scmp.com/tech/big-tech/article/3024997/why-are-hong-kong-protesters-targeting-lamp-posts

[59] ForbrukerRadet (Norwegian Consumer Council), ‘Connected Toys Violate European Consumer Law’ www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/ accessed 9 July 2018

[60] Nellie Bowles, ‘Thermostats, Locks and Lights: Digital Tools of Domestic Abuse’ *The New York Times* (New York, 23 June 2018) www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html; Paul Skelton, ‘Combating Domestic Violence: Strong Networks, Safe Homes’, (*Connected*, 21/5/2019), https://connectedmag.com.au/combating-domestic-violence-strong-networks-safe-homes/.

[61] Lauren Goode, ‘Facial recognition software is biased towards white men, researcher finds’, (*The Verge*, 11 Feb 2018), https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error.

[62] Australian Government, Department of the Prime Minister & Cabinet, *Data Sharing and Release Legislative Reforms Discussion Paper* (September 2019) 32.

[63] Ibid 26-7.

[64] Australia, Department of Prime Minister and Cabinet, *The Australian Government’s Response to the Productivity Commission Data Availability and Use Inquiry* (1 May 2018) <http://dataavailability.pmc.gov.au/sites/default/files/govt-response-pc-dau-inquiry.pdf> accessed 28 May 2018, 6.

[65] Ibid.

[66] Kayleen Manwaring, ‘Will emerging information technologies outpace customer protection law? — The case of digital consumer manipulation’ (2018) 26 *Competition & Customer Law Journal* 141, 143; Roger Brownsword, Rights, Regulation, and the Technological Revolution (Oxford University Press, 2008) ch 6; Manwaring, ‘Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies’ (n 24).

[67] Lyria Bennett Moses, 'Recurring dilemmas: the law's race to keep up with technological change' (2007) 2 University of Illinois Journal of Law, Technology & Policy 239

[68] Kate Mathews Hunt, ‘consumeR-IOT: where every thing collides. Promoting consumer internet of things protection in Australia.’ (SJD minor thesis, Bond University, 2018) 180, 192-3; Manwaring, ‘Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies’ (n 24), 76-80.

[69] Manwaring, ‘Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies’ (n 24), 68-70.

[70] Manwaring, 'Will emerging information technologies outpace customer protection law? — The case of digital consumer manipulation' (n 66) 141.

[71] Mathews Hunt, 'consumeR-IOT: where every thing collides. Promoting consumer internet of things protection in Australia.' (n 68) 129-130.

[72] Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 24) 68.

[73] Manwaring, 'Emerging information technologies: challenges for customers' (n 6) 281-283.

[74] Roger Clarke and Graham Greenleaf, 'Dataveillance Regulation: A Research Framework' (2017) 25(1) Journal of Law, Information and Science 104

[75] James Halliday and Rebekah Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part I' (2015) 34 Communications Law Bulletin 7, 9.

[76] Ibid.

[77] James Halliday and Rebekah Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (2016) 34 Communications Law Bulletin 4, 6-7.

[78] Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 24) 80-81.

[79] Halliday and Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part I' (n 75) 10.

[80] ACCC, *Digital Platforms Inquiry: Final Report* (n 40) 517.

[81] Mathews Hunt, 'consumeR-IOT: where every thing collides. Promoting consumer internet of things protection in Australia.' (n 68) 134.

[82] Halliday and Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (n 77) 7.

[83] Manwaring, 'Emerging information technologies: challenges for customers' (n 6) 275.

[84] Manwaring, 'Surfing the third wave of computing: Consumer Contracting with IoT devices in Australia' (n 23) Ch 5, para 3.5.

[85] Erik Laykin, 'IoT Evidence Analysis and Preservation in Investigations and Litigation', Conference presentation, RSA Conference 2017, San Francisco, February 13-17 2017

[86] Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 24) 67.

[87] *Criminal Code Compilation Act 1913* (WA), s 440A

[88] Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 24) 68.

[89] Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 24) 68.

[90] Mathews Hunt, 'consumeR-IOT: where every thing collides. Promoting consumer internet of things protection in Australia.' (n 68) 180.

[91] Mathews Hunt, 'consumeR-IOT: where every thing collides. Promoting consumer internet of things protection in Australia.' (n 68) 192.

[92] Lauren Goode, 'Facial recognition software is biased towards white men, researcher finds', (*The Verge*, 11 Feb 2018), https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error

[93] IoT Alliance Australia, *Good Data Practice: A Guide for Business to Consumer Internet of Things Services for Australia: V1.0* (November 2017).

[94] IoT Alliance Australia, *Internet of Things: Security Guideline: V1.0* (February 2017); IoT Alliance Australia, *Internet of Things Security Guideline: V1.2* (November 2017).

[95]IoT Alliance Australia, *Good Data Practice: A Guide for Business to Consumer Internet of Things Services for Australia V1.0*, November 2017).

[96] Productivity Commission, *Data Availability and Use* (Productivity Commission Inquiry Report No 82, March 2017) 71, 569–94.

[97] Ibid 569–94.

[98] ACCC, *Digital Platforms Inquiry: Final Report* (n 40) 503. See also Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (December 2018) 301.

[99] ACCC, *Digital Platforms Inquiry: Final Report* (n 40) 518.

[100] In particular, s 6D of the Privacy Act 1988 (Cth) excludes businesses with AUD3 million or less in annual turnover, unless they hold health information, are a credit reporting body or a Commonwealth contractor, or deal in personal information.

[101] Privacy Act 1988 (Cth) s 13B.

[102] Privacy Act 1988 (Cth) s 6A.

[103] Privacy Act 1988 (Cth) s 7B.

[104] *Telstra Corp Ltd and Privacy Commissioner* [2015] AATA 991; *Privacy Commissioner v Telstra Corp Ltd* [2017] FCAFC 4. In this case, journalist Ben Grubb sought access to metadata held by Telstra relating to his use of telecommunications services. Both the Administrative Appeals Tribunal (AAT) and the Full Federal Court on appeal proposed a narrow construction of the meaning of personal information 'about an individual'. The definition of 'personal information' in the Privacy Act has since been reworded, but the rewording did not clarify the scope of information being 'about an individual'.

[105] See Graham Greenleaf, 'Privacy Enforcement in Australia Is Strengthened: Gaps Remain' (2014) 128 *Privacy Laws & Business International Report* 1. The relevant page reference (4) is from the SSRN version https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468774 accessed 16 January 2019.

Q[106] Office of the Australian Information Commissioner, 'Determinations' www.oaic.gov.au/privacy-law/determinations/ accessed 24 April 2018.

[107] Information Commissioner's Office, 'Actions We've Taken' https://ico.org.uk/action-weve-taken/enforcement/ accessed 24 April 2018.

[108] For example, Allie Coyne, 'Starved of Funding, Resources, OAIC is Left to Shrivel' (*IT News*, 17 July 2015) www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273; Denham Sadler, 'Privacy Office at Breaking Point' (*InnovationAus,* 26 March 2018) www.innovationaus.com/2018/03/Privacy-office-at-breaking-point; Ben Grubb, 'Australia's Privacy Watchdog is "Woefully" and "Criminally" Underfunded' (*Crikey*, 16 July 2018) www.crikey.com.au/2018/07/16/australias-privacy-watchdog-is-woefully-and-criminally-underfunded/?ft=SGxCKzkvcXRVNWk0eU1tcjdPcGlNQT09.

[109] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report 108, May 2008) 674–83.

[110] For example, Privacy Act 1988 (Cth) sch 1, Australian Privacy Principle 7, which regulates direct marketing.

[111] Joel R Reidenberg and others, 'Ambiguity in Privacy Policies and the Impact of Regulation' (2016) 45 The Journal of Legal Studies S163; Rachelle Bosua and others, 'Privacy in a World of the Internet of Things: A Legal and Regulatory Perspective' (2017) Networked Society Institute Research Paper 6, 10; Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 24) 76–80.

[112] Nguyen and Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* Table 4, 59.

[113] This analysis of the weaknesses of the Privacy Act 1988 (Cth) was published by the lead author of this report in the article Manwaring, 'Will emerging information technologies outpace customer protection law? — The case of digital consumer manipulation' (n 66) 175–77, which was published online on 3 December 2018. A week later, on 10 December 2018, the ACCC released its preliminary report as part of the Digital Platforms Inquiry, which contained similar criticisms. ACCC, *Digital Platforms Inquiry: Preliminary Report* (n 98) 223.

[114] Ibid 456-496.

[115] ACCC, *Digital Platforms Inquiry: Final Report* (n 40) 498-501.

[116] Recommendation 18, ACCC, *Digital Platforms Inquiry: Final Report* (n 40) 498.

[117] BA LLB (Sydney) LLM (UNSW) Grad Dip Communications (UTS) PhD dissertation (UNSW) submitted for examination.

[118] B Media, Research Assistant, UNSW School of Taxation & Business Law.