



Enhancing Consumer Awareness of Privacy and the Internet of Things



Enhancing Consumer Awareness of Privacy and the Internet of Things

Ian Warren
Monique Mann
Diarmaid Harkin

August 2021



Enhancing Consumer Awareness of Privacy and the Internet of Things

Authored by **Ian Warren, Monique Mann and Diarmaid Harkin**

Published in **2021**

This project was funded by a grant from the Australian Communications Consumer Action Network (ACCAN).

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

Deakin University

Website: www.deakin.edu.au

Email: ian.warren@deakin.edu.au

Telephone: 03 5227 2434

Australian Communications Consumer Action Network

Website: www.accan.org.au

Email: grants@accan.org.au

Telephone: 02 9288 4000

If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: <https://www.communications.gov.au/what-we-do/phone/services-people-disability/accesshub/national-relay-service/service-features/national-relay-service-call-numbers>

ISBN: **978-1-921974-68-7**

Cover image: Design by **Richard Van Der Male** with images from Shutterstock



This work is copyright, licensed under the Creative Commons Attribution 4.0 International Licence. You are free to cite, copy, communicate and adapt this work, so long as you attribute the authors and “Deakin University, supported by a grant from the Australian Communications Consumer Action Network”. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>

This work can be cited as: Warren, I. Mann, M. & Harkin, D. 2021, *Enhancing Consumer Awareness of Privacy and the Internet of Things*, Australian Communications Consumer Action Network, Sydney.

Table of Contents

List of Tables	iv
List of Figures	v
Acknowledgements.....	1
Executive Summary.....	2
Main findings	2
The role of icons.....	4
Recommendations	5
Chapter 1. Introduction	7
Aims and rationale for this project	7
Policy context.....	7
Project overview	8
Chapter 2. Consumer Internet of Things in the home	9
What are CloTs?	9
The Internet of Toys.....	9
CloTs and sensors.....	10
Risks of CloTs.....	12
Regulation of CloTs	13
Security and Privacy by Design	14
Privacy law and technology companies	15
Notice and consent	17
Unfair contract terms.....	19
Previous studies on CloTs and privacy	20
Potential solutions	21
Icons and their design	21
Conclusion.....	25
Chapter 3. Methodology.....	27
Icon design	27
Privacy policy statements	27
Survey design, administration and sample demographics	28
Key stakeholder interview sample and procedure	30

Conclusion.....	31
Chapter 4. Privacy Policy Statements and Terms of Service.....	32
Content of PPS	33
Justifications for collecting personal information	33
Data anonymisation and aggregation.....	34
Consent	34
Information sharing	35
Information access and deletion.....	36
Privacy by design and disabling CloT functions	37
PPS updates.....	37
Public knowledge and awareness of PPS.....	38
Perceived utility of PPS	39
Perspectives of notification and consent.....	40
Conclusion.....	41
Chapter 5. Patterns and Perspectives of CloTs	43
Consumer purchasing patterns.....	43
Benefits of IoTs	44
Concerns about IoTs	45
Information and security risks of IoTs.....	47
Privacy concerns	48
Responsibility	51
Children and IoTs	52
CloTs and accessibility.....	55
Conclusion.....	56
Chapter 6. Privacy and Regulation	57
Problems with privacy law, regulation and enforcement.....	57
The role of consumer law	59
Regulatory responsiveness: self-, co- and ‘smart’ regulatory approaches.....	60
Improved security, product standards and enforcement.....	63
Conclusion.....	65
Chapter 7. Icons	66
Icon design	66
Icon prototypes.....	68

Utility of icons	71
Limits of icons	72
Icons and community education.....	73
Conclusion.....	75
Conclusions	76
Recommendations	78
Recommendation 1.....	78
Recommendation 2.....	78
Recommendation 3.....	78
Recommendation 4.....	78
Recommendation 5.....	79
Recommendation 6.....	79
Recommendation 7.....	79
Recommendation 8.....	79
Authors.....	80
Appendix 1 Consumer Privacy and the Internet of Things: Survey Tool	81
Appendix 2 Consumer Privacy and the Internet of Things: Interview Schedule	106
References	112

List of Tables

Table 1 Types of CloT sensor devices.....	11
Table 2 Best practice for privacy notice design	23
Table 3 Codes and descriptors for visual privacy.....	25
Table 4 IoT device purchases in the previous 12 months.....	28
Table 5 Survey respondents according to gender identity.....	29
Table 6 Survey respondents according to geographic location.....	30
Table 7 Key stakeholders and their fields of expertise	31
Table 8 Proportion of respondents who do and do not read PPS	38
Table 9 Reasons why respondents decide to read PPS	38
Table 10 Reasons why respondents decide not to read PPS	39
Table 11 Perceived utility of PPS.....	39
Table 12 IoT devices purchased by respondents in the previous 12 months.....	43
Table 13 Perceived value of functions and characteristics of IoT devices.....	45
Table 14 Perceived concern about different types of data collection by IoT devices	46
Table 15 Responses to items measuring privacy concern	50
Table 16 Perceived responsibilities of individual consumers	51
Table 17 Perceptions of organisational responsibility for raising consumer awareness of IoTs.....	51
Table 18 Summary of perceptions of children’s privacy.....	54
Table 19 Icon recognition task: Complete results.....	71
Table 20 Distribution of perceived utility of piloted consumer icons	71
Table 21 Reasons why consumer icons are perceived as useful	72
Table 22 Reasons why consumer icons are not considered useful	73

List of Figures

Figure 1 Privacy law and the problem of consent	3
Figure 2 Icons illustrating sensors and other technological functions	12
Figure 3 Privacy Commissioner of New Zealand Trustmark – Te Mana Matapono Matatapu.....	67
Figure 4 Californian IoT Privacy Icon.....	68
Figure 5 Icon prototype: Offline.....	68
Figure 6 Icon prototype: Overseas data sharing.....	69
Figure 7 Icon prototype: Privacy safeguards	69
Figure 8 Icon prototype: Child safety controls.....	70
Figure 9 Icon prototype: Environmentally conscious	70
Figure 10 Consumer privacy educational flyer: facing side	74
Figure 11 Consumer privacy educational flyer: rear side (8 key consumer information issues).....	74

Acknowledgements

We gratefully acknowledge the input and assistance of the following people.

Michael Wilson, Chloe Boyd, Sally Kennedy and Kat Scanlon for providing dedicated research assistance.

Kathrin Kohl for producing the icon prototypes.

Lauren Solomon, Andrew Thomsen and Brigid Richmond, who provided vital insights into consumer law and policy.

Kayleen Manwaring and Lee Bygrave who provided important feedback on different iterations of the literature review and survey.

Luca Treccani, working on behalf of the Online Research Unit, who was extremely helpful in reviewing several drafts of the CPIoT survey pilot, organising the pilot and ensuring rapid administration of the final survey and consolidation of raw data.

All key stakeholders for providing us with their time and insights in the extended interviews, all of which provided valuable data and important learning experiences.

U3A Geelong and the Centre for Cyber Security Research and Innovation at Deakin University for providing opportunities to present early iterations of the literature review and findings from this research.

Tanya Karliychuk, Catherine Wyburn and Stephanie Whitelock for ongoing guidance, support and flexibility during the various interruptions to this project at the height of the COVID-19 pandemic. Your constant support and encouragement were highly valued.

The CPIoT survey and key stakeholder interviews were conducted with ethics approval from the Faculty of Arts and Education Human Ethics Advisory Group at Deakin University (HAE 20-012).

Executive Summary

This report presents empirical data about the purchasing patterns, common uses and knowledge Australians have of the privacy impacts of consumer Internet of Things (CloTs) devices. This data is supplemented by interviews concerning the security, privacy and regulatory risks of CloTs with 32 key stakeholders from the fields of information security, regulation and academia. These perspectives provide new understandings of the role of CloTs in contemporary Australian life and demonstrate the policy and regulatory challenges that emerge from their rapidly expanding use. Graphic icons were also considered as a potential mechanism for raising consumer awareness of privacy issues associated with CloTs, but survey and interview findings indicate that substantial law reform and greater industry engagement are required before icons can have meaningful impact in addressing the privacy issues relating to CloTs.

Main findings

The literature on IoTs, CloTs and devices targeting specific groups of consumers, such as children and their parents, illustrates a range of privacy and consumer protection issues that are inherent in the commercial expansion and popular appeal of these technologies. As Chapter 4. Privacy Policy Statements and Terms of Service indicates, there is some commercial incentive, but limited regulatory incentive, for technology companies to simplify the communication of privacy policies to consumers. These approaches are sanctioned by the Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth) and are tied to problems with the notice and consent model of privacy, which requires technology companies to inform consumers of privacy risks in a way that provides a limited ‘take-it-or-leave-it choice: give up your privacy or go elsewhere’ (Schaub et al., 2018, pp. 674-675). A fundamental problem with the regulation of CloT devices is the current regime under the *Privacy Act*, the APPs and case law was developed in a pre-digital era. The inadequacy of this regime means there is very limited legal protection for consumers who use CloT devices, which places much responsibility for safety and security issues onto the consumer. Device manufacturers are also largely unaccountable for any privacy or security breaches (Posadas, 2017). Their only requirement is to request and obtain consent from consumers before using the CloT device. This approach significantly limits the opportunity for consumers to provide meaningful consent to commercial privacy policy statements (PPS) (Solove, 2013, Kim, 2019). The “notice and consent model of privacy” is one element of the privacy regulatory framework that requires reconsideration and reform due to the unique functions of CloTs.

Power disparities between manufacturers and consumers undermine the capacity of the “notice and consent model” to produce genuine consent from consumers. People are forced into accepting the terms and conditions if they want to use IoT devices. If consent is not provided, they won’t be able to use the device. The power disparities that underpin these arrangements are also acknowledged to produce privacy fatigue and digital resignation amongst consumers (Draper and Turow, 2019). This means consumers tend to uncritically accept the terms and conditions without reading them in detail because they want access to the device or can only gain access if they consent to the collection and use of their personal data. These problems warrant reconsidering and strengthening both under Australian privacy and consumer protection requirements for both IoTs and other online services (ACCC, 2019; Manwaring, 2017b). The following flowchart outlines how consumer choice about providing personal data is compromised by the current Australian privacy regime.

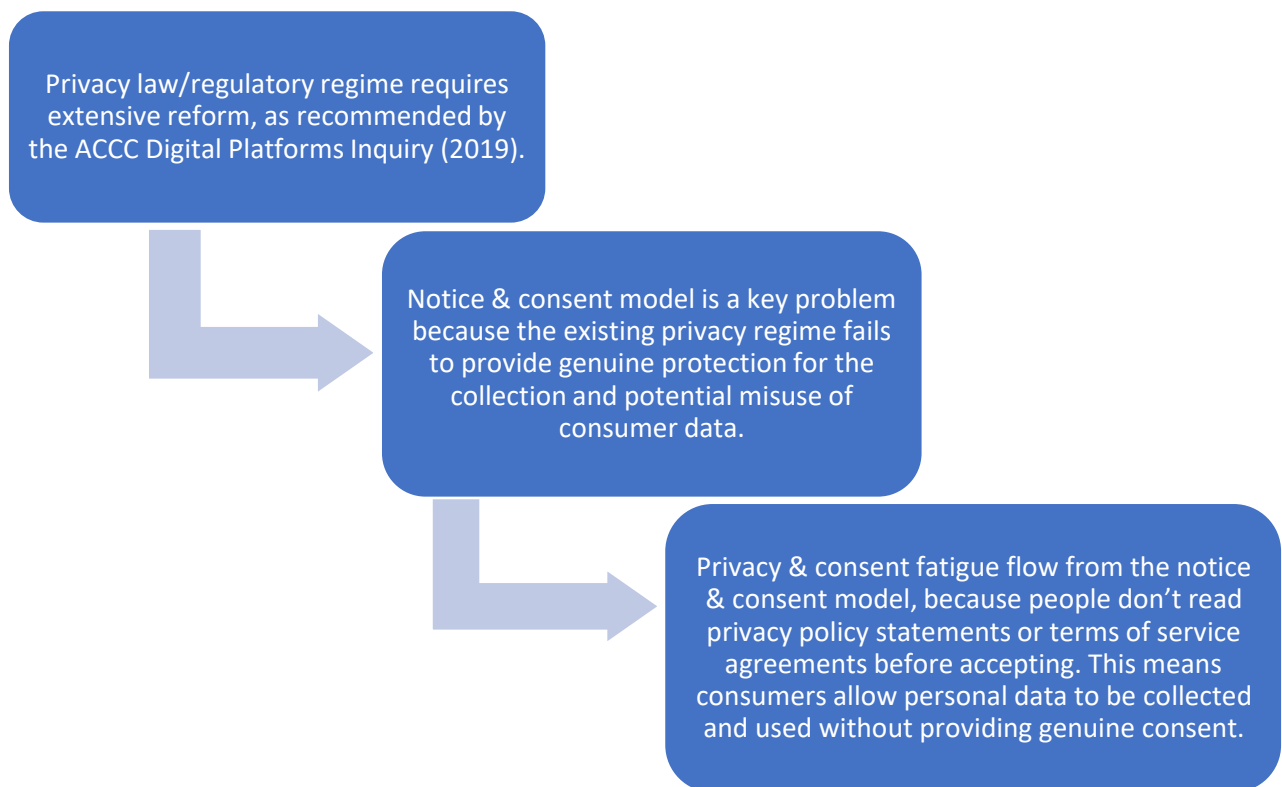


Figure 1 Privacy law and the problem of consent

There also is a contradiction between these issues and the data from a national Consumer Privacy and the Internet of Things (CPIoT) survey administered for this study. In a sample of 1052 Australian respondents, which comprised 844 IoT consumers, it was reported the convenience provided by these devices largely outweighed concern about their privacy impacts. The survey indicates consumers want to control their data yet remain willing to provide personal information to access the

benefits of CloTs. In line with other Australian research (Richardson et al., 2017), CPlOT survey respondents were also concerned about the ability of CloTs to collect certain forms of personal data, such as credit card information, phone conversations and photographs. However, this concern does not extend to the data associated with personal or family habits that stem from ongoing interactions with CloT devices.

When combined with concerns expressed by key stakeholders about the lack of general data security standards for CloT devices, even with Australia's IoT security code of practice (Manwaring and Clarke, 2021), consumers appear to believe technology companies have limited accountability for their data collection practices. However, they feel they can do little about this problem if they want the benefits of CloTs. Lack of enforced accountability for data security breaches is also an issue with the current consumer protection regime.

Of particular concern amongst key stakeholders interviewed for this project is the lack of appropriate regulatory oversight of CloT development, security and marketing. Lack of regulatory oversight is an issue with both the current privacy and consumer protection regimes. Although opinion is divided on the optimum approach for regulating CloTs, it is recommended a 'smart' approach to the regulation of 'smart' technologies is required. This could involve incentivised compliance and self-regulation as a starting point, with stronger external enforcement of penalties for breaches of privacy and consumer protection laws by organisations such as the Office of the Australian Information Commissioner (OAIC) or Australian Competition and Consumer Commission (ACCC) to enhance CloT product standards and consumer protection.

The role of icons

Recommendations Recommendation 5 and Recommendation 6 indicate that any icon system must be situated within a stronger privacy and consumer protection framework that is supported by adequate enforcement mechanisms and potentially supplemented by direct involvement of the CloT industry. While there were mixed views about the value of the icon prototypes produced for this study, survey and interview findings lead to the conclusion that icons may have an important role to play in enhancing consumer awareness of privacy issues associated with CloTs. This could lead to consumers altering their purchasing behaviour or potentially forcing much needed regulatory change associated with CloT technologies.

Survey and key stakeholder interview findings indicated that icons alone would not remedy many of the issues related to CloTs that relate to a lack of adequate regulatory oversight. There are also hidden costs associated with their development and use. For example, several key-stakeholders indicated

that the global nature of the CloT industry demanded a global standard for its regulation, which icon development should reflect. Moreover, the range of design considerations intended to simplify the process of icon recognition (Consumers International, 2019; Genaro Motti and Caine, 2016) can also unduly complicate the process for consumers. Ultimately, icons can place more demands on consumers to protect their own rights and interests when making CloT purchasing choices. In other words, while many survey respondents and key stakeholders favoured icons as one way of potentially simplifying the content of PPS, they may place additional burdens on consumers that do nothing to address fundamental gaps in regulatory oversight. It is unlikely privacy icons will have significant impact in addressing privacy issues that arise from CloTs in the absence of substantive legislative reform, enforcement oversight, and industry engagement.

This study provides empirical evidence highlighting the need for regulatory reform to enhance the transparency of CloT data collection practices. The optimal form of such regulation is less clear. CPIoT survey and interview data suggest that consumers and key stakeholders like the idea of icons to simplify the content of PPS, but also recognise that icons will be insufficient to address many of the concerns associated with CloTs. Therefore, in absence of holistic reform to privacy and consumer laws and their related enforcement processes, the value of icons to educate consumers about the risks of CloTs is likely to be limited. In other words, icons should not serve as a substitute for regulatory reform but can have an important supplementary role in any reform process.

Recommendations

The recommendations from this study are:

1. Prevailing sentiment amongst key stakeholders interviewed for this research strongly indicated that Australia does not currently have adequate protections for consumers for the many privacy, security and safety concerns presented by CloTs. It is recommended that additional regulatory and enforcement efforts are pursued to address these deficiencies, particularly in light of the expanding presence and penetration of CloTs into the community.
2. Several key stakeholders identified compelling arguments that specific groups such as children, the elderly, and those living with a physical or intellectual disability, face specific problems with CloTs and other digital technologies. This includes the inability to provide direct consent if other individuals are setting-up devices. It is recommended any future regulatory efforts are cognisant of, and responsive to, the privacy impacts of CloTs on specific populations where consent cannot be assured.

3. Several key stakeholders criticised the current model of notice and consent. This has led to long and complex terms of service and PPS that are assumed to reflect an adequate level of consumer understanding and informed consent. Of our survey respondents, 47% reported that they did not read PPS. It is recommended efforts are taken to simplify, enhance and reconsider obligations and approaches to informing consumers about the privacy implications of CloTs.
4. Key stakeholders were often critical of the lack of transparency and clear information about CloT data collection and handling practices. In addition, 54% of survey respondents hold technology companies responsible for raising awareness of the privacy impacts of CloTs. It is recommended further pressure is placed on CloT manufacturers and vendors to be more transparent about the data collection practices associated with these technologies.
5. Key stakeholders provided notional support for an icon system to enhance consumer awareness of the privacy implications of CloTs, while 74% of survey respondents indicated icons would assist them to make purchasing decisions about IoT devices. It is recommended that an icon-based system following the New Zealand or Californian model is considered in Australia, supported by adequate regulatory oversight, to address many of the current deficiencies of communicating privacy impacts of CloTs.
6. Many key stakeholders indicated that any icon system would need to be situated within a robust regulatory framework involving the stronger enforcement and protection of the privacy and consumer rights of Australians. It is recommended an icon-system be incorporated into a broader process of reform to current privacy and consumer protection laws, which includes enhanced enforcement and placing increased obligations on the CloT industry to participate in these processes.
7. The commencement of a public campaign to educate consumers about the types of data collected by CloTs relating to personal and family behaviours or habits, and how this type of information differs from conventional transactional data such as name, address and credit card details, which appear to generate the most privacy concern.
8. Future research into the counterintuitive nature of privacy attitudes and behaviours, as many CPlOT respondents appear willing to sacrifice their privacy for the convenience of device functionality.

Chapter 1. Introduction

This chapter provides an overview of the aims, rationale, and importance of this project, which examines consumer awareness of the privacy issues associated with Consumer Internet of Things (CloT) devices. It provides a brief outline of the policy context for this report and the four key methodological approaches used to examine these issues.

Aims and rationale for this project

This project seeks to raise awareness about the scale and extent of personal information collected from IoT technologies, and, specifically, CloTs in the home. The objective was to develop a series of icons to educate and inform consumers about privacy issues associated with CloTs. For reasons explained throughout the report, the development of privacy icons was more difficult than originally anticipated. However, this research has demonstrated that icons may have a significant role to play in helping to reform consumer protection and privacy regulation, by improving public awareness and, with time, simplifying personal data collection standards.

Policy context

Current policies for the collection and use of personal information from CloTs include requirements under the 13 Australian Privacy Principles (APPs) contained within the Australian *Privacy Act 1988* (Cth) (OAIC, 2014). These involve ensuring appropriate standards for the collection, storage and use of personal information. These procedures and practices must be communicated to consumers of CloTs and related online services.

The *Competition and Consumer Act 2010* deals with unfair contract terms, consumer product guarantees, national product safety requirements and various types of prohibited corporate conduct (see generally Carter and Chan, 2019). However, there are concerns that Australian and international consumer protection standards do not adequately address the technical functions of CloTs (ACCC, 2019; Manwaring, 2017a; 2017b; 2018). Given this, icons offer a potential method of raising privacy awareness to protect consumers.

There is also a need for the simplification of privacy policy statements (PPS) more generally. This is now mandated under the European Union's (EU) General Data Protection Regulation (GDPR) (Rossi and Palmirani, 2019), and the Californian Consumer Privacy Act (CCPA) (Rossner and Kennealy, 2018). Privacy icons might help to simplify corporate notification and data collection practices for the benefit

of consumers. However, substantial reform to the notice and consent model associated with information privacy in Australia is also necessary, as corporate practices generally aim to maximise personal data collection and CloTs collect very sensitive data about families and their habits or activities.

Project overview

In light of these issues, this project involved four methodological components:

1. A systematic review of the literature on CloTs, including an examination of their functions, risks, and the legal frameworks governing privacy and consumer protection;
2. A review of CloT privacy policies, focusing on a range of devices including 'smart' speakers, connectable toys, security cameras and pet accessories;
3. A survey examining consumer knowledge and behaviours associated with CloTs, privacy and perspectives on a suite of icons developed for the project; and
4. Extended interviews with 32 key stakeholders with backgrounds in privacy compliance, regulation, security and accessibility, to examine key privacy issues associated with CloTs and providing expert views on the roles of icons as a consumer protection measure.

Chapter 2. Consumer Internet of Things in the home

What are CloTs?

IoT, also known as ‘smart devices’,¹ connect to the internet and each other, to form a digital ecosystem in many contemporary homes (ACOLA, 2020, p. 24). Newer homes are likely to have a range of CloT devices pre-installed, while a large proportion of the CloT market involves stand-alone devices connected to a common hub or router. All CloTs have a unique MAC (Media Access Control) identification number and an allocated internet protocol (IP) address. They ‘communicate’ with other internet-enabled devices through either satellite, cellular, Wi-Fi, or Bluetooth connections (Greengard, 2015, p. 20).

This project defines CloTs as ***any device that can transmit or receive signals and commands via the internet or another internet-connected device, which enables remote, interconnected or automated functionality in the home.*** The primary focus of attention in this project is *consumer* products that are commonly sold in popular commercial technology stores, or are pre-installed in newer homes, and are available to general consumers. CloT devices include:

- Hubs which enable the connection of multiple devices that can be remotely controlled using direct voice commands or via a mobile phone or tablet app;
- Individual ‘smart’ devices installed or fixed in the home, including thermostats, television sets, light globes, doorbells and other goods that operate with a Wi-Fi connection to a domestic router or to another device using Bluetooth. These CloTs can also be connected to and controlled via a hub, mobile phone or tablet app or another connected device;
- Any mobile device that is commonly used or synced in the home, such as a watch or wearable device.

The Internet of Toys

An important subset of devices includes the Internet of Toys (IoToys) (Haber, 2020; Holloway, 2019; Albuquerque et al., 2020). Child monitoring technologies have been defined as ‘caregiver-focused IoT

¹ We avoid using the term ‘smart’ as it has misleading connotations about the privacy and consumer protection issues associated with CloTs (Sadowski, 2020).

devices' (Haber, 2020, p. 1218), and include prenatal testing devices, baby monitors, nanny cams, RFID-enabled clothing, and GPS trackers (e.g., Mascheroni, 2018, p. 517). There are heightened concerns that data collected from CloTs and IoToys can have profound impacts on a child's education, wellbeing, privacy, and freedom of expression (Electronic Privacy Information Centre, 2018; McRae, Ellis and Kent, 2018; Forbrukerrådet, 2017; Forbrukerrådet, 2016). There are also limited controls over the retention and use of CloT and IoToy data once it is collected (OECD 2021, p. 16). While it is increasingly difficult for children 'to avoid surveillance and datafication' (Haber, 2020, p. 1211), the direct impacts of CloTs on child privacy (Stoliova, Livingstone and Nandagiri, 2020; Stoliova, Nandagiri and Livingstone, 2020; van der Hof, 2017) also extend to other members of a household or any non-resident guests.

CloTs and sensors

The types of sensors installed into household and consumer goods determine the nature of the data that CloTs can collect and transmit *and* the privacy risks they generate. Sensors enable CloTs to automatically send and receive data to and from other devices, apps, computer programs or an electronic communications service or network (ACOLA, 2020, p. 24; Council of the European Union, 2021, p. 11). Sensors give CloTs their functionality, and can measure sound through in-built microphones, temperature, humidity, air pressure and quality, fluid levels, acceleration, heartbeat, images, geo-location and device motion (see generally Peppet, 2014; Andrejevic and Burdon, 2015; Caron et al., 2016; Manwaring and Clarke, 2015). CloT hubs communicate to the sensors installed in devices such as refrigerators or smart speakers and enable the execution of device functions through direct voice commands or remote control using a mobile phone or tablet application. Electronic sensors enable device users or external providers to direct the device or monitor things such as home temperature to activate heating thermostats, for example. The main types of CloT devices and sensors are outlined in Table 1.

Table 1 Types of CloT sensor devices

(derived from Peppet, 2014, pp. 98-117)

Sensor Type	Location	Examples
Health and Fitness	Countertop	Wi-Fi scales, kettles, blood pressure monitor, pill bottles, Hapifork
	Wearable	Fitbit, bio-tracking chips in armbands or clothing; iTbras that can detect heat abnormality as signs of breast cancer
	Intimate contact sensors	Epidermal electronics embedded in bandages, medical tape, patches, tattoos, peel and stick thermometers, biostamp Band-Aids that transmits heart rate, brain activity, body temperature, hydration and UV exposure
	Ingestible or implantable sensors	Smart pills that monitor inside the body, or contain 'pill cam', embedded sensors in medicines to monitor prescription compliance, dental devices that transmit information to a dentist
Home and Electricity	The 'smart' home	Google Nest and related hubs; stand-alone devices, including ovens reporting temperature control, the 'smart grid' that remotely monitors home energy use, plant watering sensors, locks, alarms, vibration sensors, motion sensors monitoring sleep, fitness, medication, water use, home temperature
	Toys and Televisions	Toys for children or pets as well as connected 'smart' televisions
Smartphone		Compass, accelerometer, ambient light monitors, proximity sensors, gyroscope, GPS, sensitive microphone, multiple cameras

Figure 2, taken from Genaro Motti and Caine (2016, p.4), provides a series of icons that depict the functionality of sensors. These visual representations can convey the common forms of data collection, transmission, storage, sharing, and the types of data obtained from a particular source or device based on the sensors that are installed. These images provide visual cues that reflect the functions of specific CloT technologies and can be matched with various rules or principles for data collection.









Collection	Transmission	Storage	Sharing
Sensors 	Network 	Physical Object 	Users' Groups 
Data 	Connector 	Virtual Metaphor 	Visibility 

Figure 2 Icons illustrating sensors and other technological functions

(Genaro Motti and Caine, 2016, p. 4)

Risks of CloTs

CloTs generate many potential consumer and household risks (OECD, 2018). Four key harms identified in previous studies are:

1. Limitations of consumer privacy policies, including notice and consent models (see for example Koops, 2014; Solove, 2013), with CloTs potentially generating and collecting data without the knowledge of other home users or non-consenting people, such as children or guests (Peppet, 2014, pp. 117-166; Weber, 2015). Specific concerns also apply to landlord and tenant arrangements (Burns and Hood, 2017);
2. The vulnerability of CloTs to information security breaches. This issue was investigated for ACCAN by Sivaraman, Gharakheili and Fernandes (2017, pp. 6-10), who identified many IoT devices have limited capacity to ensure confidentiality, data integrity and authorised access control, among other concerns;
3. The challenges of de-identifying or anonymising personal data collected from CloTs (OVic, 2021, p. 6); and
4. The analysis of IoT data via machine learning, or AI, which will lead to sensitive inferences being developed about people in potentially unacceptable and discriminatory ways (see for

example Mann and Matzner, 2019; Friedman and Nissenbaum, 1996; Wachter and Mittelstadt, 2019; Kryla-Cudna, 2018; Noble, 2018; Sandvig et al., 2016; O’Neil, 2016; Hildebrandt, 2015; Leese, 2014).

Consumers should have knowledge of these risks *before* a CloT device is sold. It is also important for consumers to be aware of how CloT manufacturers can affect future consumer rights by changing the functionality of devices or withdrawing long-term support for software upgrades. In general, the risks of CloTs are extensive but, as suggested by many of our key stakeholders, poorly understood and regulated under current privacy and consumer protection laws in Australia.

Regulation of CloTs

The development of CloTs, and the administration of data they collect, is mainly done by *private companies* through *private legal agreements*. This structure has been characterised as enabling corporate access into the private home through contract law (Bygrave, 2015) via Terms of Service (ToS) agreements, End User License Agreements (EULAs) (Belli and Venturini, 2016) or corporate Privacy Policy Statements (PPS).

These policies operate through principles of notice and consent. The complexity of these contractual and quasi-contractual arrangements means they are limited in protecting consumer rights and privacy (see Solove, 2013). This is because they presume the methods of communicating privacy requirements in PPS are understood by consumers and enable them to provide free consent for corporate access to their personal information. The focus of regulation depends on which organisations collect the data from the device, how and with whom that data is shared, and whether or how these factors impact consumer choice. Depending on the device, CloTs could also be simultaneously regulated through network infrastructure, equipment standards and consumer safety standards (ACMA, 2020, pp. 10-16).

Manwaring (2017a) identifies six key aspects of CloTs that require enhanced consumer awareness. These are:

1. IoT devices collect data on consumers (and their children);
2. Many IoT devices have information security risks (see also Sivaraman, Gharakheili and Fernandes, 2017);
3. IoT devices are never really owned, even after they are paid for. This is because the software for their use requires accepting the company’s ToS, EULAs and PPS;

4. IoT devices collect a lot of personal and sensitive information about consumers and other people who visit their homes;
5. It is difficult to understand the implications for using CloTs or how long they will last, because the contractual agreements are highly complex or opaque;
6. The law may not adequately protect consumers or their personal information.

These problems are magnified because the data collected from CloTs is highly granular and encompasses details about the habits and interactions people have with these devices or each other while the devices are dormant (Peppet, 2014; OVIC, 2021). In addition, many CloTs are designed by small start-up companies that either fail to gain formal regulatory approval or are exempt from the same privacy controls that attach to large multinational corporations. Thus, much personal information collected through CloTs may not be protected by Australian privacy law.

Security and Privacy by Design

In November 2019 the Australian government announced an enhanced voluntary industry-based security code for IoTs (Tonkin, 2019). The initial draft sought to encourage ‘device manufacturers, IoT service providers and app developers’ to ensure improved information security standards are incorporated into the development of IoTs. The 13 draft principles were finalised by the Australian federal government as a *Code of Practice for Securing the Internet of Things for Consumers* (Australian Government, 2020; see Manwaring and Clarke, 2021). These mirror those adopted in the UK (Department for Digital, Culture, Media and Sport, 2018; 2019a) and build on other models that have been established internationally by governments or the private sector (ENISA, 2018a; 2018b; 2018c; IoTSF, 2018; Lloyds, 2018; Malaysian Communications and Multimedia Commission, 2018; Bosua et al., 2017b; Brass et al., 2017; IoTAA, 2017; Childon and Ben-Sahar, 2016; Federal Trade Commission, 2015). Some key elements of the Australian Code include obligations to implement vulnerability disclosure policies, to keep software regularly and securely updated, to minimise exposed attack surfaces and to ensure IoT systems are resilient to outages.

The Australian Office of the e-Safety Commissioner (2019) also issued a series of requirements directed at service providers to improve the empowerment and autonomy of IoT device users and foster greater accountability and transparency for the provision of online services more generally. These principles include placing increased responsibility on service providers for policy creation and implementation to deal with consumer safety, including the enforcement of community standards and ToS agreements, and clear lines of communication to help assist and protect all consumers,

including children. The e-Safety Commissioner also recommends the provision of technical measures to ensure users can better manage their own safety, while device manufacturers must configure the most secure privacy and safety levels as default settings. Where possible, technical measures should minimise consumer harms and maximise safety, with regular evaluation procedures of these security-by-design and privacy-by-design (PbD) measures and the introduction of clear processes for lodging and resolving consumer complaints. Finally, it is recommended that technology companies consult widely on the development of appropriate safety standards and regularly report on their effectiveness.

Privacy law and technology companies

The Australian *Privacy Act 1988* (Cth) governs the collection and use of personal information by requiring businesses with an annual turnover of more than AU\$3 million to comply with the 13 Australian Privacy Principles (APPs). The APP framework has been criticised for providing limited regulation of questionable corporate data collection practices through highly technical ‘clickwrap’ ToS and EULAs that appear in lengthy fine print when a consumer is asked to accept the conditions of use for a device or application (Obar and Oeldorf-Hirsch, 2018). Many of these standardised corporate privacy policies also have uncertain status under contract, property and consumer protection laws (Fairfield, 2017; Perzanowski and Schultz, 2016; Radin, 2013; Clapperton and Sorones, 2007).

CloTs are manufactured and marketed to enhance convenience, but also expand corporate surveillance into private homes (Zomet and Urbach, 2016; Zuboff, 2019; Andrejevic and Burdon, 2015). Koops et al. (2017) capture how the use of personal information can vary from the point of its initial access to its ultimate control by the corporate sector or government (see also Nissenbaum, 2010; Cohen, 2017). These issues span both the physical and non-physical or informational aspects of privacy in five key sites that provide the basis for different forms of regulation.

CloTs bridge the private and public divide once information from the private home is conveyed to corporate providers, even if this is done through secure networks (ACMA, 2020). For example, the granular nature of data collected by CloTs, even when they are dormant or in ‘sleep’ mode, can significantly compromise elements of ‘solitude’, ‘intimacy’ and ‘secrecy’ associated with domestic life (Koops et al., 2017). This raises extensive concerns about how to control, correct and delete such personal information captured by these devices. The communication of personal behaviours and habits recorded by CloTs ultimately creates a ‘variability of privacy expectations’ which ‘is not an abstract nor absolute right or static good to be traded off against other possible goods’, but a ‘structural condition and a related entitlement’ (Cohen, 2017, p. 1055) the law should protect.

When information from different devices is integrated and aggregated, it can draw very detailed, sensitive and personalised inferences about a person's or family's activities (see Wachter and Mittelstadt 2019; Mann and Matzner, 2019; Lupton, 2016). Such technically complex data management relationships (Manwaring, 2017b; Noto la Diega and Walden, 2016; Manwaring and Clarke, 2015) raise several issues about information privacy, as well as the accuracy, ownership and accessibility of personal data held by technology companies or governments (Logsdon Smith, 2018; Rosner and Kenneally, 2018; Caron et al 2016).

Fair information principles require the provision of adequate information about data collection and storage practices to ensure consumers can exercise informed decisions to provide personal information and personally identifiable information (PII). Notice and consent requirements also extend to the ability to *access* information and correct inaccuracies, the right to information about *security* measures aimed at preventing unauthorised access, and the development of appropriate *enforcement* mechanisms applicable to the rules for collecting, storing and sharing personal information or PII (Quirk and Rothchild, 2010, pp. 355-361). Most of these issues are incorporated into the APPs.

There are several problems with this *self-management approach to information privacy* based on notice, consent and 'opt-out' principles, because it places the primary responsibility on individuals to decide whether to accept or use digital services according to the terms provided by technology companies. The Australian *Privacy Act 1988*, and the APPs, reflect this self-management approach. The APPs, which were modified in 2012, apply to all Commonwealth Government entities, as well as private corporations with an annual turnover of at least AU\$3 million. However, this restriction means many small start-up companies are automatically exempt. APP corporations with an annual turnover higher than AU\$3 million must inform consumers of their practices for collecting, storing and correcting 'personal information'. If these disclosures are made, a user is deemed to consent to handing over their personal information when they agree to a PPS, even if there is no way of monitoring whether consumers have understood the data collection, storage or correction policies.

Personal information is viewed as a 'technologically neutral' term designed 'to ensure sufficient flexibility to encompass changes in information-handling practices over time' (OAIC, 2017, p. 4). Personal information 'conveys something about' the person even if the connection is vague (OAIC, 2017, p. 7). This is because 'information can have different degrees of connection with an individual and still be personal' (OAIC, 2017, p. 7), and result in a person's actual or potential identification. Reasonable identification occurs if it is likely a person's identity can be discovered based on the nature and quantity of the information, the individuals or organisations in possession of the information, and

any additional information that could be used for identification purposes. If there is no likelihood of identifying a person, the information will not be personal and can be readily collected without reliance on the APPs (OAIC 2017, p. 8). Under the *Privacy Act 1988* (Cth), the following types of personal information are specifically mentioned:

- ‘Sensitive information’, including ‘information or opinion about an individual’s race, ethnic origins, political opinion, religious beliefs, sexual orientation or criminal record’ that relates to an identified individual or someone who is ‘reasonably identifiable’;
- Health information, which is also classed as sensitive information, and can include genetic and some biometric information;
- Credit, employee record and tax file number information.

Some information regarding CloT users, such as credit information, will be collected at the point of sale. However, sensitive information can also be collected through the routine uses of CloTs. Under the *Privacy Act 1988* (Cth), determinations about whether a person is identified or reasonably identifiable from the information are made on a case-by-case basis² (OAIC, 2017, p. 6).

De-identified information is not considered personal information, so is exempt from the 13 APPs. A major difficulty with this exception is ‘robust anonymisation of Internet of Things data is extremely difficult to achieve, or, put differently, that re-identification is far easier than expected’ (Peppet, 2014, p. 130; see also OVIC, 2021). This is because many IoT and CloT devices collect information that is highly personalised and individualised (Kryla-Cudna, 2018), including detailed information about a person’s or family’s habits and interactions with and near these devices. The range of biographical, biological, physical or biometric, and geographic location data collected by CloTs and stored by technology companies is almost impossible to de-personalise, de-identify or, when re-aggregated, provides extensive insight into a person’s or family’s activities and habits.

Notice and consent

Four main factors undermine the ability of technology consumers to provide meaningful consent for the collection of their personal information. First, ToS, EULAs and PPS commonly use confusing and convoluted language. Second, information is usually provided to consumers after the purchase has

² Digital metadata is not considered personal information under the *Privacy Act* but is classified in this way under legislation governing the interception of and access to telecommunications information (OAIC, 2017, pp. 4-5).

been made, or during product registration, rather than at the point of sale. Third, there is a lack of true choice with current notice and consent arrangements, because failure to provide consent usually means the service will not work or access is denied (Schaub et al., 2018). Finally, there is a large degree of digital resignation amongst consumers, which is commonly attributed to the normalisation of these unbalanced corporate communication arrangements (Draper and Turow, 2019).

Technology companies have a significant role in determining how consumer rights are shaped through ToS, EULAs and PPS. These private clickwrap agreements can potentially undermine regulatory oversight (Belli and Venturini, 2016; Bygrave, 2015) and there is currently no clear legal requirement for companies to simplify privacy disclosure warnings for consumers either at the point of sale or during device set-up.

In addition, as some CloTs do not have screens, information about their use must be conveyed on device packaging, in instructions or during product registration processes, which commonly involves using another internet connected device to access the manufacturer's website or an app. These processes have the potential to hamper the ability of consumers to make reasoned purchasing choices that consider privacy issues, because ToS, EULAs and PPS all involve high degrees of 'contract distancing' at the time a CloT is purchased. This means specific privacy terms are not presented to the consumer until the device is set-up and are not necessarily conveyed to the consumer at the time of sale (Manwaring, 2017b; Peppet, 2014). There is no requirement for CloT packaging in Australia to disclose information about the types of data these devices collect or the privacy approaches adopted by the companies with access to this data.

While the individualised self-management privacy model is compliance based (Solove, 2013; Schaub et al., 2018), and consumers receive an opportunity to consent to the terms and conditions specified in the agreement through an opt-out notice, there is often no choice but to accept the terms and conditions presented by the manufacturer. This means it is often questionable whether true consent is ever established under the notice and consent model (see Koops, 2014). If the consumer declines to accept the terms and conditions, the online goods and services will remain inaccessible or will not function as intended.

The complexity of ToS agreements for online services can also confuse consumers, leading to ‘digital resignation’ (Draper and Turow, 2019), which is a symptom of unfairness (Kennedy, Elgesem and Miguel, 2017). Digital resignation stems from a process that has enabled technology companies to:

... engage in obfuscatory strategies and tactics that cultivate the perception that efforts at control are pointless. The result is to encourage feelings of resignation [amongst consumers] by conveying a sense of normalcy around consumer surveillance practices and discouraging collective action (Draper and Turow, 2019, p. 1830).

PPS offer minimal ‘clarity around a website’s data collection and handling practices’ (Draper and Turow, 2019, p. 1831). This occurs by using complex language that consumers tend to avoid. Such complexity is considered to further undermine the notice and consent model that is the foundation of Australian privacy law.

Unfair contract terms

Although there are some protections for household consumers under Australian law, it is unclear how these relate to CloTs. The *Competition and Consumer Act 2010* contains limited protection against unfair terms in consumer contracts (Carter and Chan, 2019). The value of these provisions for CloTs in Australia is uncertain (see Clapperton and Sorones, 2007; Manwaring, 2018), as there needs to be a contract in existence for any terms relating to information privacy to be considered unfair (Clifford and Paterson, 2020, p. 750). There are also complexities about how product software, which commonly operates through a licence, relates to ownership of the physical device. The separation of hardware and software is yet to be reconciled under current property, contract or consumer requirements governing CloTs in Australia (Manwaring, 2017b; 2018; Fairfield, 2017). Further, CloTs are part of a ‘product-service package’ where responsibility for the object, its software and data storage can involve different entities (Manwaring, 2017, p. 273). As such, while there are numerous sites where personal information can be obtained or shared amongst corporate entities within a digital ecosystem, Australian consumer law provides minimal guidance on how consumers rights can be protected within these ecosystems.

The 2019 Australian Competition and Consumer Commission (ACCC) inquiry into digital platforms recommended a suite of reforms that included strengthening protections for consumers under the *Privacy Act 1988* (Cth) (ACCC, 2019, Chapter 7). This would result in stronger prohibitions against unfair contract terms, greater transparency in ToS, EULAs and PPS (Clifford and Paterson, 2020), and more rigorous standards to deal with unfair or anti-competitive trading practices (ACCC 2019, p. 26; 34-37). The ACCC considered several potential impacts of IoT and voice-activated devices that contribute to the increased ‘collection, analysis and distribution of user data’, with various potential

risks to ‘user rights, privacy, autonomy and data security’ (ACCC, 2019, p. 510). It also recommended that consumers receive advance notice of the relationships between manufacturers and partner organisations that affect information privacy, even if this information is commonly incorporated in ToS, EULAs and PPS for CloTs.

Previous studies on CloTs and privacy

While some research documents consumer engagement with privacy policies for digital services and CloTs in Australia, three studies deserve specific attention for identifying consumer willingness to use IoT devices despite extensive concerns about their privacy impacts. One Australian study examined ‘the importance and value of privacy, concerns about the ability of IoT users to control access to their personal information as well as use of their personal information once collected’ (Richardson et al., 2017, p. 4). This study found privacy was highly valued amongst this small sample of IoT users. However, respondents also expressed concerns over the lack of control and transparency for the collection, use and storage of IoT data. This included expressing the desire to ‘restrict what businesses can do [with my data]’ and criticism of the lack of ‘transparency around [who is protecting your data]’ (Richardson et al., 2017, p. 5). Interestingly, despite these concerns, there still appears a willingness to use CloTs. This is consistent with research into the ‘anxieties of control’ relating to data about people’s spatial movements (Leszczynski, 2015), and highlights a lack of confidence in the ability of IoT PPS to sufficiently inform consumers of their rights. These concerns were compounded by a general lack of awareness about possible protective measures under Australian law. This study recommended a graded system of responsive regulation involving minimum PbD or data protection-by-design standards, along with an improved consumer and data protection regime, and more rigorous enforcement of Australian privacy laws (see Richardson et al., 2017, pp. 8-9).

A UK study, Williams, Nurse and Creese (2017) surveyed 170 IoT users and interviewed 40 respondents about their knowledge of privacy risks. This study reinforced the ‘privacy paradox’, where consumers express concern about privacy risks but generally ignore these problems when purchasing an IoT device. It found CloT users ‘do less to protect their data’ than users of conventional computer devices, primarily due to the preoccupation with device functionality and lack of awareness of privacy issues (Williams, Nurse and Creese, 2017, p. 6). Only 9% of respondents considered privacy is a barrier to purchasing these devices (Williams, Nurse and Creese, 2017, p. 4). Increased convenience was considered a legitimate trade off to justify replacing a password protected device with a more insecure wearable CloT (see also McMahon, 2018). Only 13% of respondents studied their CloT PPS in detail, leading to the conclusion that ‘a large number of consumers are held to terms of which they have no knowledge’ (Williams, Nurse and Creese, 2017, p. 8).

Potential solutions

While there is a general awareness of privacy risks associated with CloTs, it appears consumers are more concerned about setting up or configuring the device so that it is operating. One potential remedy would involve developing ‘awareness campaigns’ to enhance consumer knowledge of privacy and security issues associated with CloTs (Williams, Nurse and Creese, 2017, p. 9). Simplifying data collection and use practices, embedding ‘privacy options ... in the installation process’, and developing icons were also considered important methods of helping to raise consumer awareness about the privacy risks of CloTs (Williams, Nurse and Creese, 2017, p. 9).

A UK study involving 24 semi-structured interviews and a survey of 200 people examining CloT security and privacy labels supports these findings (Emami-Naeni et al., 2019). This study found most respondents purchased CloT hubs primarily due to curiosity, with few respondents considering their privacy or security risks (Emami-Naeni et al., 2019, p. 6). This is despite most respondents expressing post-purchase concerns with the listening functions of intelligent personal assistants, hubs and televisions. Most participants indicated their preferences for online and in-store CloT device information were:

... to have the label in the online store’s device description, as one of the images, or after the features and before the consumer reviews. For in-store shopping, about half of the participants wanted the label to be on the package of the device so that they could refer to it later. The other half wanted the label to be on the shelf to compare devices easily, even though some participants noted the possibility of devices being placed incorrectly in the store (Emami-Naeni et al., 2019, p. 8).

A layered approach to label design involving a ‘static version’ or ‘top layer’ conveying ‘the most critical information’ about security and privacy issues was favoured, ‘as it is likely that most consumers will glance over labels without interacting with them’ (Emami-Naeni et al. 2019, p. 9). A star rating consumer protection system was also recommended. The mistrust of device manufacturers suggests clear enforcement and oversight of the marketing and sale of CloTs is needed, backed by recognisable trust marks and notifications to enhance consumer awareness of the intricacies of CloT operability, privacy and security (DCMS, 2019b; Harris Interactive, 2019; Rossi and Palmirani, 2019; Things/Mozilla Open IoT Studio, 2017).

Icons and their design

Voluntary or mandatory icons are an attempt to simplify the disclosure of corporate data collection, use and storage practices for the benefit of consumers. While numerous studies into CloTs indicate the value of icons, there are limits to the disclosure of information aimed at protecting consumers engaging with complex industries or products. Privacy icons can play an important role in enhancing

corporate transparency (Schaub et al., 2018, p. 670) and consumer awareness about the risks of CloTs, but they do not solve all problems inherent in the notice and consent model of information privacy. Indeed, icons may reinforce privacy habituation or fatigue, while providing a false sense of security that the consumer controls the use of their personal data. These problems are explored throughout this section and in the remainder of this report.

According to a report by the Australian Securities and Investments Commission (ASIC) and the Dutch Authority for the Financial Markets (AFM) (2019, p. 3), disclosure involves '[material] information the law mandates must be provided to consumers by firms' in 'hard-copy document form or electronically' through emails and websites. Such information can be presented at the time of sale or during the lifecycle of the product. Disclosure requirements often compete with other routine forms of corporate messaging, such as advertising and promotional material. Regulators are aware mandated '(w)arnings are not a cure-all for problems in financial services markets' and greater evaluation of their effectiveness in protecting consumers from certain features of a product or policy is required (ASIC, 2019, p. 46). This is because:

...we can ignore, overlook, misunderstand or misremember warnings. They can have no impact on our behaviour, or even backfire ... 'warning fatigue' may be a relevant factor given our finite attention, and the over-proliferation of warnings in relation to so many of the risks we encounter in our day-to-day lives (ASIC/AFM, 2019, p. 46).

Developing user-friendly visual representations of privacy concepts is complex. It requires consideration of icon design, the mode of delivery, the level of visual literacy the design assumes and the messages it aims to convey to consumers (Holtz, Nocun and Hansen, 2011; Holtz, Zwingelberg and Hansen; 2011; Consumers International, 2019; DCMS, 2019b). As the ACCC has indicated, a layered approach is preferred due to the lack of 'a standard vocabulary for describing privacy notice options' (Schaub et al., 2018, p. 672; Cohen, 2017; Genaro Motti and Caine, 2016). This means the icon acts as a signpost for more detailed privacy policies that can be accessed through a digital platform via a weblink, QR code, app or some other prompt.

Schaub et al. (2018) offer a best practice model for developing privacy icons that is summarised in Table 2. This requires flexible, easy-to-understand and multi-layered content that can facilitate informed consumer choice. Privacy notices can be device and context-dependent, involve ambient and haptic notifications (Hildebrandt and Koops, 2010; Gilmore, 2017) and be standardised in various ways to enhance consumer awareness (Cranor, 2012). These multi-layered options provide important clues on how privacy warnings can be presented in different formats at different times during the device lifespan, to maximise consumer understanding and choice about their privacy options.

Table 2 Best practice for privacy notice design

(Schaub et al., 2018, pp. 685-701)

Key Factors	Options	Benefits and Problems
Timing	At setup before purchase or first use	Habituation and icon fatigue
	Just in time when information is collected, used or shared; can replace setup notices; good for sensitive data	Users more receptive at the time data is taken to help with informed consent
	Context-dependent when location changes, or new users visit smart homes;	Activates with proximity to sensors; problems of automation and error
	Periodic when data is taken or any other time; notice and consent varies with the device; informs when policies change	Awareness of privacy-sensitive information occurs when a reminder is given; could be too frequent (combined for multiple data forms)
	Persistent when information is continuously collected	Only viable for critical data collection practices
	On demand - web based	Dashboards
Channel or location	<p>Primary within the system</p> <p>Secondary useful for CIoT through apps or centralized cloud or control centres; device in proximity; point of sale, just-in-time, context-dependent or periodic notices via text or email; links to policy or relevant icons;</p> <p>Public for smart cities</p>	
Modality – context-based warnings	Visual – images, icons or a combination with colours and distinctive fonts; must have impact (with conversion to audibility)	Text, user-testing and evaluation; tables; ranking systems; standardized by industry or law; personalized; needs universal language or narration
	Auditory – spoken words or tones	Requires learning
	Haptic – sensory or smell	Links to formal policy needed
	Machine-readable – phones or QR codes	
Control options for users	Blocking – notice blocks access until user agrees (opt-in or opt-out)	Needs layered choices; drag and drop data sharing to compel interaction
	Non-Blocking – simple warnings	Easy to ignore
	Decoupled – dashboards to update or alter options at user discretion	Potential automation and adaptability with other devices

Genaro Motti and Caine (2016) investigated different ways of visualising privacy using various combinations of text, images and icons. They identify four key considerations for icon development that are elaborated in Table 3.

1. **Who** are people, institutions or organisations involved in discussing, providing or threatening user privacy;
2. **How** objects, actions, behaviours, attitudes and mechanisms enable privacy control;
3. **Why** users want to obtain privacy and the feelings, intents or emotions involved;
4. **Where** are the places, locations and real-world scenarios users perceive privacy is required.

This study developed seven codes that can be further divided into 15 sets of descriptive terms to describe IoT device functions. Table 3 summarises relevant descriptors that can help in the development of privacy icons. Each code represents a potential action, object, organisation, individual, abstract concept or location that can generate feelings or attitudes about privacy. Each code is then linked to a range of possible descriptors to inform the design of images that reflect specific privacy behaviours or themes.

Table 3 Codes and descriptors for visual privacy

(Genaro Motti and Caine, 2016, p. 3)

Codes and descriptors	Descriptors
Action - what users do to ensure privacy, common attitudes and behaviours in real world or information systems	Analysing, authenticating, blindfolding, blocking, blurring, covering, connecting, closing, dimming, disclosing, erasing, forwarding, hiding, localizing, locking/unlocking, looking, observing/being observed, packing, protecting, protesting, revealing, sharing, shredding, spying, surveilling, synchronizing, uploading, uncovering
Objects and mechanisms to manage information collection, storage and distribution, or potential blockers to prevent access	<p>Blockers: Blinds, curtains, diary, door, fence, gate, key, message, padlock, wall, windows</p> <p>Control: Semaphore, ToS, privacy policies, privacy settings, browser add ons</p> <p>Sensors: Camera, camcorder, microphone</p> <p>Storage: Memory card, cloud</p>
Organisations that promote or threaten privacy	<p>Regulatory: NSA, AFP</p> <p>Social Media: Ashley Madison, Bitcoin, Facebook, Google</p> <p>IT: Instagram, Pinterest, RSS, Twitter, Whatsapp</p>
People	<p>Politicians: Legislators, Individuals</p> <p>Public Persons: Snowden, Orwell</p> <p>Circles: Group, Individual</p>
Abstract concepts	Betrayal, confidentiality, creepiness, exclusivity, fear, intimacy, isolation, loneliness, public v. private, safety, secrecy, shame
Places where users seek for and find privacy	Home, bedroom, bathroom, garden, desert island

These criteria offer important guidance on factors to consider when designing and implementing an icon system for CloTs. However, it is important to note icons will not resolve structural inadequacies in the regulation of privacy or consumer protection law.

Conclusion

This chapter demonstrates a variety of privacy and consumer protection issues associated with CloTs. While these devices have growing consumer appeal, there are minimal regulatory or commercial

incentives to communicate privacy risks through simplified processes, such as an icon system. However, an icon system can fulfil an educative or warning function to raise consumer awareness about actual or potential privacy risks. Based on research examined for this study and the various technical risks posed by CloTs, the optimum value of icons is only likely to be realised in conjunction with other significant reforms to privacy and consumer protection regulations and their enforcement in Australia.

Chapter 3. Methodology

This chapter details the methodology for this project. It commences with a brief statement outlining the process of designing the icon prototypes that were tested through the Consumer Privacy and the Internet of Things (CPIoT) survey and key stakeholder interviews. It then describes the process for reviewing IoT privacy policies, followed by an outline of the design, procedure for administering the national CPIoT survey and demographic characteristics of respondents who completed survey. The chapter concludes with a description of the approach for identifying and interviewing key stakeholders with expertise in the information privacy, regulatory and academic fields to gain an in-depth understanding of the consumer privacy risks associated with IoTs.

Icon design

A graphic artist was commissioned to design several monochrome icons that reflected key themes in the 13 APPs. The initial designs were incorporated into the CPIoT survey to test consumer perceptions and understanding of the icons. In depth interviews also focused on key stakeholder perceptions of these designs. Data from the CPIoT survey and key stakeholder interviews provided an invaluable framework to further develop and refine the piloted icons.

Privacy policy statements

A key element of this study involved reviewing Privacy Policy Statements (PPS) for 203 IoTs. These related to products manufactured or distributed by over 100 separate corporations, comprising a mix of large multinational businesses and small start-up companies. The policies depict how key aspects of information collection are conveyed to consumers in line with the APPs, with many policies for larger corporations consolidating instructions for different devices. The PPS included:

- 35 'smart' speakers and hubs by 33 manufacturers;
- 36 IoTs by 27 different manufacturers, consisting of board games, educational aids, trucks, robots, drones and musical devices marketed specifically for children;
- 20 television sets by 20 manufacturers, many of which also produce 'smart' hubs and other home appliances;
- 12 gaming consoles, with 5 manufacturers that did not produce any other IoTs;
- 47 home appliances, with 22 manufacturers that did not produce other IoTs. These policies applied to washing machines, ovens, refrigerators, coffee machines, heaters and coolers, lightbulbs, home security systems with cameras, locks and doorbells, and several single

devices including a dishwasher, a kettle, a set of bathroom scales, an alarm clock, an air quality monitor and a digital photo frame;

- 51 pet accessories with 35 unique manufacturers that included interactive cameras, food dispensers, GPS and health trackers, toys and related accessories.

Chapter 4. Privacy Policy Statements and Terms of Service presents results from this review, which shows the core information conveyed through PPS as required by Australia’s APPs. This review was important in framing the questions examined in the consumer survey and interviews with key stakeholders.

Survey design, administration and sample demographics

The CPIoT Survey was developed over a 10-month period between January and October 2020, with an initial pilot of 130 respondents conducted between 28 to 31 August 2020. The aim of this survey was to examine community attitudes towards IoTs, related privacy policies and our icon prototypes. After preliminary analysis of the pilot data, minor adjustments to survey items were made, with the final version administered online from 7 to 13 October 2020. The survey was administered by the Online Research Unit (ORU), which obtained a total sample of 1052 responses, comprising a non-probabilistic sub-sample of 844 IoT consumers and a corresponding sub-sample of 208 non-consumers for comparison purposes. Table 4 outlines the proportion of respondents who indicated they had purchased an IoT device in the 12 months prior to October 2020. The survey instrument is reproduced in Appendix 1 Consumer Privacy and the Internet of Things: Survey Tool.

Table 4 IoT device purchases in the previous 12 months

IoT Ownership	N	%
Consumers	844	80.2%
Non-Consumers	208	19.8%
TOTAL	1052	100.0%

The average age of the 1052 respondents was 46.6 years (SD=15.28). The final sample included a small over-representation of male respondents (n=564, 53.6%) compared with female respondents (n=486, 46.2%), with two (n=2) respondents opting not to disclose their gender identities (these participants

were excluded from any inferential analyses examining gender identity as an independent variable). Reported gender identity is represented in Table 5.

Table 5 Survey respondents according to gender identity

Gender Identity	N	%
Male	564	53.6%
Female	486	46.2%
Other	0	0%
Prefer not to say	2	0.2%
TOTAL	1052	100.0%

Respondents from metropolitan regions as classified by the ABS remoteness index are overrepresented, with 87% (n=917) of CPIoT survey respondents reporting that they lived in a major capital city (Table 6). ORU’s sampling process sought to reflect the broader population demographic in Australia that is concentrated in the eastern states. This means findings regarding education, income and proficiency with information technology are more likely to reflect patterns in urban Australia.

Table 6 Survey respondents according to geographic location

(against ABS remoteness index)

ABS Remoteness Index	N	%
Major Cities of Australia	913	86.8%
Inner Regional Australia	99	9.4%
Outer Regional Australia	32	3%
Remote Australia	5	0.5%
Very Remote Australia	1	0.1%
Not classified	2	0.2%
TOTAL	1052	100.0%

Key stakeholder interview sample and procedure

Following administration of the survey and preliminary examination of the survey results, 30 in-depth interviews with 32 key stakeholders were conducted. Our aim was to draw on the expertise of these respondents in assessing their views of the risks, benefits and regulatory issues associated with ClOTs in Australia and internationally. A semi-structured interview schedule, which is reproduced in Appendix 2 Consumer Privacy and the Internet of Things: Interview Schedule, was adapted to accommodate the expertise of each key stakeholder, while drawing on key themes from the literature review, the examination of ClOT privacy policies and preliminary CPlOT survey findings. All interviews were conducted between November 2020 and March 2021, and were audio recorded and selectively transcribed. Many key stakeholders had held various roles in technical, regulatory, policy and academic fields throughout their careers. Table 7 provides an overview of the sample and the fields of expertise of the key stakeholders interviewed for this project.

Table 7 Key stakeholders and their fields of expertise

Field of Expertise	Number
Technical and Security	11
Privacy (including regulation, compliance)	14 (12 interviews)
Advocacy (including representatives for children and people with disability)	4
University research/academic	3
TOTAL	32 (30 interviews)

Conclusion

The multi-method approach for this study used general patterns associated with PPS and ToS agreements as the basis for developing the survey to produce data about consumer uses, concerns, and privacy behaviours associated with CloTs. This body of work was supplemented by in-depth interviews with 32 leading experts in the fields of digital security, regulation, advocacy, and privacy. Each component of the methodology supplements data obtained from each preceding research stage to provide a detailed and critical understanding of consumer activity relating to data privacy and CloTs in contemporary Australia, while critically examining the value and limits of icons in communicating the privacy issues associated with these devices.

Chapter 4. Privacy Policy Statements and Terms of Service

There are significant concerns about the ability of Privacy Policy Statements (PPS) and Terms of Service (ToS) agreements to foster genuine informed consent about personal data collection. The current notice and consent approach requires consumers to opt-out, which involves a ‘take-it-or-leave-it choice: give up your privacy or go elsewhere’ (Schaub et al. 2018, pp. 674-675). As Kim (2019, p. 131) indicates ‘(c)onsent to participate in an activity where the participant lacks knowledge about what the activity entails *cannot* be valid consent’. This system does not accommodate most users of technology and is particularly problematic for the aged or people with disability. There is also no mechanism to ensure consumers understand PPS, ToS and end user licence agreements (EULAs).

In absence of holistic legal and regulatory reform to information privacy law (Australian Law Reform Commission, 2014), there is a need to foster improved communication of PPS that explains the specific types of information collected from all digital technologies. This can potentially assist in raising consumer knowledge of privacy issues to enable more informed choices when purchasing CloT devices. Substantial legal reform would also serve the broader purpose of offering more consumer protection by placing greater responsibility for privacy protection on CloT device manufacturers and their corporate partners, rather than technology consumers.

This chapter provides a summary of key elements of PPS covering a wide range of devices, including loToys, household appliances and pet accessories. Instructions on websites, downloadable and printed material, product packaging and accompanying mobile applications were consulted. PPS and ToS agreements are complex documents written in technical, legalistic language, with no standardised content or terminology. Some policies for smart speakers vary between 2,400 and over 7,000 words in length and make no mention of consent, or refer to consent by use, usually with the statement ‘*by using this website you consent to our privacy policy*’. It is often unclear whether a consumer is providing consent to accept the privacy policies associated with a CloT they have purchased, or are consenting to additional terms and conditions associated with accessing services on the manufacturer’s websites, such as product registration services, or accompanying apps that are often developed and administered by other companies (see Peppet, 2014).

This chapter is conscious not to name specific devices or companies associated with PPS. Rather, the purpose is to identify general trends about how PPS are structured, including their basic content and focus. PPS are mandated elements of Australian privacy law under APP 5, which requires companies

to disclose the purposes for collecting personal information. The objective here is to demonstrate how the current notice and consent process generates unduly complicated PPS and ToS arrangements that validate the collection, use and storage of various forms of highly intrusive data. These practices affect all consumers of digital products, including CloTs.

Content of PPS

This section outlines key reasons cited in PPS for collecting the personal information of consumers. Frequently, a range of personal information is collected, although this is seldom connected to specific types of sensors installed in a CloT. Rather, the emphasis is on corporate legal rights and potential consumer benefits stemming from the information collection process. In many cases, PPS contain general statements that say very little about the types of personal information collected. In others, a range of personal information actively provided by or accessible about consumers, including a username and password during account set up, a photograph or other avatar, credit card details, billing address, social media accounts, or other information that is already accessible online through open-source data mining technologies, are expressly mentioned. The key problem is the extensive variation in these practices that are reflected in PPS and related agreements with CloT companies and their corporate ecosystems.

Justifications for collecting personal information

Improving the consumer experience and future product development are two leading justifications for collecting personal information. Most CloT policies examined contain their justifications either in a paragraph or itemised list. One technology manufacturer refers to 22 listed purposes for using personal information from a range of devices. Many of these requirements are framed as corporate responsibilities to act on a customer's request, or to improve the company's services for consumers. Other justifications include defending corporate legal rights, regulatory compliance, product marketing and internal record keeping.

One online PPS indicates the collection of various forms of personal information helps to *'personalise and continually improve your ... experience'*. The online platform where this PPS is located identifies information that is directly provided by the consumer, as well as 'automatic information' collected by the company through 'mobile', 'email communications' and 'other sources'. This range of information is considered necessary to assist the company in building customer profiles for targeted advertising and providing consumers with special offers. Details about these information collection processes are contained in active web links on the company's website. Consumers are advised that they *'will have an opportunity to choose not to share the information'*.

Notice provisions commonly document the kinds of personal information likely to be collected about people from other online sources. This includes ‘*information about individuals who are, or are employed by, our suppliers (including service and content providers), contractors, dealers, related companies, agents, advisors, corporate customers and business partners*’. Such information is considered necessary to ‘*(u)nderstand the way you use the Services so that we can improve your experience*’. This information can also be shared with ‘*trusted companies that may provide information about products and services you might like*’. It is also common to find statements outlining how personal information might be shared with law enforcement, although specific organisations or locations of relevant agencies are not usually mentioned.

Data anonymisation and aggregation

It is common for IoT policies to have an anonymisation clause that describes how personal information is de-identified once collected. One manufacturer of smart hubs uses the following anonymisation clause:

We may anonymize your Personal Information so that it can no longer identify you. We may also aggregate data in a way that prevents it from personally identifying you. We do not link personally identifiable information with aggregated user data.

Similarly, the manufacturer of a Wi-Fi connected dog toy indicates it retains anonymised data ‘*for any purpose and [will] disclose anonymous data to third parties in its sole discretion*’. Other companies reserve the right to combine personal and non-personal information and ‘*the combined information will be treated as personal information for as long as it remains combined*’. This aims to ensure personal information about consumers remains ‘protected information’ under Australian privacy law.

Consent

Consent is a precondition for accessing the interconnected functions of IoT devices. One company that manufactures several IoTs provides the following statement documenting the implications of *not* agreeing to its PPS and the location of information storage:

By using the services you consent to the collection, use, and transfer of your information as described in this privacy policy. If you do not agree with any part of this privacy policy, then please do not use the services.

Another company that sells smart home technologies indicates consent is provided when a consumer enters personal information into the company’s website ‘*to complete a transaction, verify your credit card, place an order, arrange for a delivery or return a purchase*’. These forms of data exchange become active once the IoT product is registered. Only data collected for secondary reasons, such as

marketing, require express consent from the consumer. There is also an instruction for withdrawing consent via the company's email address.

One PPS with contains a consent agreement that provides users with limited choice regarding the preferred location for data storage. The following quote appears on this company's website in capital letters:

Please be aware that all associated services and systems may be housed on servers in the United States. If you are located outside of the United States, information we collect (including cookies) are processed and stored in the United States, which may not offer the same level of privacy protection as the country where you reside or are a citizen. By using the services and providing information to us, you consent to the transfer to and processing of the information in the United States.

Larger multinational companies often have references to information transfer requirements under regional economic agreements. These include regulations specific to the European Economic Area or the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules that aim to 'ensure protection of personal information transferred among participating APEC economies'.

Information sharing

Large multinational companies appear conscious of indicating that '*(i)information about our customers is an important part of our business, and we are not in the business of selling it to others*'. However, information will be shared with affiliated businesses to enhance co-selling and this practice is communicated to consumers in PPS. Access can also be given to third party service providers, but is likely to be confined to specific tasks that could involve:

...fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analysing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service.

Exchanging personal information with other organisations is often considered necessary '*for fraud protection and credit risk reduction*'. However, many companies are cautious to note '*this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes.*'

Smaller companies are likely to have general statements about the collection and sharing of information with other companies. These provisions will explain how companies and their affiliates '*collect, use, share and protect information in relation to our mobile services, website, and any software*'. This includes providing data for fraud checks managed by '*a 3rd party service that builds*

[an] Artificial Intelligence database, and your records will have to stay there even after you stop using our services. One company that manufactures voice-controlled speakers reserves the right to share information amongst:

- Vendors providing support services to the company;
- Partners, including *'car manufacturers or electronic consumer device manufacturers, to integrate components ... into their own devices and software'*;
- Owned and affiliated companies;
- Providers of legal services; and
- Organisations involved in corporate transactions such as mergers, acquisitions or the sale of business assets.

Consumers might be able to control their personal data through specific device settings or their online accounts with the service provider. This includes the ability to *'(a)ccess, modify, or delete your Personal Data; Opt out of marketing communications'* and manage *'cookies and other data collection technologies, which includes opting out of ads on social media ... or by adjusting personal settings on mobile devices'*. Many of these information sharing requirements are considered by the primary company or corporate affiliates to improve IoT devices, consumer services and the development of AI technologies. Some companies indicate that once data enters their systems, it is retained permanently, which raises important issues about the appropriate durations for data retention.

Information access and deletion

The ability to access, scrutinise, correct, and request the deletion of personal information are central obligations under APP 12 and APP 13. However, PPS often include these requirements with a qualifier that a consumer *'can always choose not to provide information, even though it might be needed to make a purchase'* or is at liberty to take advantage of another online service. If an alteration to personal information is sought, a company will *'usually keep a copy of the prior version for our records'*.

PPS place much of the obligation for information provision, access, and correction onto the consumer. This includes instructing consumers to alter default settings via web portals to control advertising preferences. These provisions generally confine data access to very narrow classes of personal information that are likely to be readily accessible in most personal accounts or through online tools that can be used for *'access, deactivation/restriction, correction or deletion'*. Direct requests for personal data could readily be declined if they are considered to be:

Frivolous/vexatious, jeopardise the privacy of others, are extremely impractical, or for which access is not otherwise required by local law. We may also decline aspects of deletion or access requests if we believe doing so would undermine our legitimate use of data for anti-fraud and security purposes.

Another example illustrates the practices of qualified data deletion, where copies of original personal data files are generally retained for archival purposes:

You may request deletion of your Personal Data by us, but please note that we may be required to keep this information and not delete it (or to keep this information for a certain time, in which case we will comply with your deletion request only after we have fulfilled such requirements). When we delete any information, it will be deleted from the active database, but may remain in our archives.

Full deletion of the data will only occur if a formal complaint about a company's data collection practices is lodged. This reinforces the view that the consumer is considered to bear the primary responsibility for any personal information transferred to technology companies, including the correction or removal of any corresponding data under the requirements of APP 12 and APP 13.

Privacy by design and disabling IoT functions

Privacy by design (PbD) is rarely mentioned in privacy policies or ToS. Some IoTs, however, are designed to enhance privacy choices with functions that prevent sharing household data with a centralised company or cloud server, which ensures any data remains stored on the device itself or within a private network. Through this process, *'the whole system and data is managed on your device without being sent to an alien cloud server'*, with the only data collected involving *'personal information to complete a purchase, verify a credit card, create an account or to arrange delivery, return an item or use any of the company's online services'*. Such an approach is certified via European Union privacy, payment, and data security standards, but is extremely rare amongst the policies examined for this study.

Other IoTs allow certain device functions to be disabled. For example, some smart hub systems are advertised as being *'designed around your privacy – Turn off the microphone and camera with the press of a button. Slide the built-in shutter to cover the camera'*. However, many other products can only be fully disabled by keeping them disconnected or turned off.

PPS updates

It is common for companies to use email or text messages to notify consumers of relevant PPS updates or revisions. It is also common for previous PPS and their updates to be maintained for open public access. However, some companies warn consumers of their responsibility to visit their websites to find updates. This is despite rules that require APP entities to take reasonable steps to inform users of any significant changes in their data collection policies.

Public knowledge and awareness of PPS

This section documents results from the CPIoT survey dealing with respondents' awareness of PPS. Almost 53% (n=554) of respondents, reported that they read PPS.

Table 8 Proportion of respondents who do and do not read PPS

PPS Engagement	N	%
Do read PPS	554	52.7
Do not read PPS	498	47.3
TOTAL	1052	100.0

The most common reason respondents recorded for reading PPS was because they are interested to know how their personal information would be used (n =290, 52.4%). This was followed by the view that PPS can inform purchasing decisions (n=109, 19.7%) or can help determine which technology company's products or services to purchase (n=90, 16.2%). Additionally, 10.8% (n=60) of respondents indicated they based the sincerity of the information they choose to disclose on the contents of a PPS. Table 9 summarises these findings.

Table 9 Reasons why respondents decide to read PPS

Why Respondents Read PPS	N	%
I am interested to know how my personal information will be used by the device or service I intend to purchase	290	52.4
I like to compare privacy policy statements when determining which technology company's devices and/or services to purchase	90	16.2
The contents of a privacy policy statement will influence whether I decide to purchase that specific device and/or service	109	19.7
The contents of a privacy policy statement will influence the accuracy of any information I disclose when registering a device and/or service	60	10.8
Other	5	0.9
TOTAL	554	100.0

The most common reasons for *not* reading a PPS is that respondents find them too difficult to read (n=151, 31.5%), they do not have the time to read them (n=132, 27.6%), they do not believe technology companies are honest with their contents (n=118, 24.6%), they want immediate access to

the product or service (n= 66, 13.8%), or they do not know where to find the PPS for the product or service they are using (n=12, 2.5%). These findings are summarised in Table 10.

Table 10 Reasons why respondents decide not to read PPS

Why Respondents Do Not Read PPS	N	%
They are too difficult to read	151	31.5
I do not have the time to read them	132	27.6
Companies will do whatever they want with my information anyway	118	24.6
I do not know where to find privacy policy statements	12	2.5
I just want to immediately access the product or service	66	13.8
TOTAL	479	100.0

Perceived utility of PPS

Survey respondents were asked their perceptions of the value of PPS. Table 11 reveals that 70% (n=746) of respondents indicated they felt PPS were of no value to some value, with the remaining 30% (n=306) indicating they were a lot of value or completely valuable.

Table 11 Perceived utility of PPS

Perceived Utility of PPS	N	%
Not at all	151	14.4
A little bit	188	17.9
Somewhat	407	38.7
A lot	237	22.5
Completely	69	6.5

Many key stakeholders expressed concern about the complexity of PPS that was also evident in CPIoT survey responses. One stakeholder with legal training indicated ‘*I have drafted privacy policies and some of the policies I am reading I don’t understand*’ (Research/Academic, RA3). There was also a belief that PPS are ‘*not meaningful*’ or genuine statements that elicit consumer trust (TS10, Technical and Security Expert). This helps to explain why people do not engage with PPS:

Nobody reads them and ... I don’t really trust that they’re actually enforceable in any meaningful way and that they’re pretty much just full of weasel words. Going on the years of evidence we have - although google

and amazon say they don't store or record conversations - they do.

TS 10, Technical and Security Expert

Additional concern was expressed over the inability to agree with the terms of a PPS. As one key stakeholder indicated: *'a policy tells you something, it's not optional'* (PP1, Privacy Professional). Further, it is unlikely people will read PPS because they simply want to install and use the technology. Finally, given time constraints faced by most people with *'work and children'*, it is often *'impossible'* for a consumer to devote the time to reading privacy policies. However, this view was tempered by another key stakeholder who suggested that despite their limitations, it is possible to envisage reforming PPS to convey useful information for consumers.

I think there are plenty of people who have pointed out the length of these agreements that people have to accept and I think we all know, have any of us read through one? That doesn't mean they're not useful but there are probably improvements that can be made in that area to the way consumers are informed about privacy issues.

PP8, Privacy Professional

There were specific concerns that IoT devices cannot provide adequate privacy notifications as they do not have screens to convey detailed information to consumers. One key stakeholder indicated this was a significant problem because it forces consumers to go to another source to find out important information about privacy. This is considered to place an unreasonable burden on consumers because they should not *'be expected to go and read the privacy policy or statement, particularly when the product now ships in a box that doesn't include the privacy statement'* (TS11, Technical and Security Expert).

Perspectives of notification and consent

Key stakeholders also expressed considerable doubt about the viability of the notice and consent model. Even if consumers fail to understand a company's PPS or ToS, they are still bound to its terms. One key stakeholder indicated that *'consent is probably one of the biggest core privacy principles that are [sic] challenged by IoT'* (PP12, Privacy Professional). This is because of the general view that *'consent ... [is] not working the way consent was intended to work'* (PP1, Privacy Professional), and it *'all boils down to this one time I click, I agree and then that's just it'* (RA1, Research/Academic).

The flaws with notice and consent magnify problems of vulnerability in relation to IoTs. This was evident in the following quote from a regulator, who highlighted two key issues regarding capacity and voluntariness of consent:

One of them is around the capacity to consent ... This is a particular issue I think when children are involved, when young people are using devices, being of such a young age

they don't necessarily have the capacity to understand what these devices are doing with their information and how it is being used. So can consent be meaningful if a small child who's using a particular device doesn't have that capacity to understand. Other issues [are] around consent being voluntary, so if somebody doesn't have a real choice but to use a particular device and to have their information collected or used in a particular way then that's not meaningful consent because a person essentially is being forced to provide consent or agree with terms and conditions.

PP12, Privacy Professional

This issue is reinforced by the highly technical and complex nature of terminology used in most PPS. Some key stakeholders considered this to be a deliberate ploy by technology companies to overwhelm and confuse consumers to justify collecting the data they want (see Draper and Turow, 2019):

When you put your ... analytical law professor's hat on and say 'what is this document telling me ... weasel words'. Things that are very aspirational but probably unenforceable ... of course they do that, would anyone suggest otherwise?

RA2, Research/Academic

Several key stakeholders expressed cynical views about current notice and consent requirements under Australian law. One suggested the self-regulatory nature of these requirements justified introducing 'a superimposed requirement of fairness and reasonableness in relation to all consumer privacy applications' (TS11, Technical and Security Expert). This is because:

... some providers choose to think that they can say whatever they want to say in a notice or in a click through 'I agree consent' and that that somehow trumps normal consumer expectations around how data about them is used.

TS11, Technical and Security Expert

The idea of consent is also questionable in the specific context of CIoT. This is because PPS and other ToS arrangements are considered 'a term of entry, a term of use. That's not asking for my permission. It is telling me what is happening' (PP1, Privacy Professional). In fact, many key stakeholders viewed PPS as a 'fiction that technology companies have created around consent through their use of online terms and conditions' (PP1, Privacy Professional). Or, as another key stakeholder suggested:

I don't think that any organisation seeks consent. They see it more as an enabler to pursue their goals rather than a source of reassurance to the consumer.

PP6, Privacy Professional

Conclusion

Clearly, many PPS have complex terms that relate directly to the APPs. Both CPlOT survey respondents and key stakeholders indicated technology companies need to do more to promote greater consumer awareness of data collection and use practices. This requires technology companies or regulators to

take more proactive measures to educate the public about the types of personal information collected through CloTs and other digital technologies. However, the CPIoT survey findings also suggest many respondents either do not look at or do not recall when they might have been exposed to a PPS. These findings affirm many criticisms about the notice and consent model expressed in the literature (Solove, 2013; Schaub et al., 2018; Kim, 2019) and by key stakeholders who indicated technology companies do not go to sufficient lengths to disclose their information collection practices in a clear, accessible and simplified manner. The problem lies in the complexity, technicality and obfuscation associated with PPS (Draper and Turow, 2019). Therefore, icons are one possible way of simplifying communication about the practices associated with the collection, use and retention of personal information, while helping to educate the public about key issues relating to privacy and CloTs.

Chapter 5. Patterns and Perspectives of CloTs

This chapter reports several general observations from the CPlOT survey and interview data that outline key purchasing patterns and the perceived benefits of CloTs, including their value for those with disabilities and for monitoring home energy-use and security. It also documents several concerns raised by survey respondents and key stakeholders about the types of data collected by CloTs, the accompanying security standards of many devices, and the privacy implications of how technology companies collect and use data. The chapter ends by indicating consumers believe they have joint responsibility with technology companies for the privacy ramifications of CloTs.

Consumer purchasing patterns

Table 12 summarises the CloT devices purchased by respondents in the preceding 12 months. It indicates the most common devices were smart watches, Wi-Fi speakers and smart home assistants or hubs (n=187), while the least common devices purchased were child monitoring devices (n=30), irrigation systems (n=24) and automatic pet feeders (n=23).

Table 12 IoT devices purchased by respondents in the previous 12 months

(In order of popularity; n=844)

IoT Device	N
Smart watch	280
Wi-Fi speakers	246
Smart home assistance (e.g., Alexa)	187
Home security system	128
Household whitegoods	119
Other household device that connects to the Internet	109
Exercise equipment	108
Smoke detector	102
Espresso machine	87
Smart doorbell	80
Automatic garage door	74
Household lighting system	74
Smart fridge	71
Smart clock	70
Heart rate monitor	57
Sleep tracker	53
Smart heater/cooler	51
Smart energy monitor	50
Smart batteries	49
Digital thermostat	42
Smart home lock	40
Smart Toy	38
Child monitoring device	30
Irrigation system	24
Automatic pet feeder	23
TOTAL	2192

Benefits of IoTs

Many key stakeholders highlighted the ability of CloTs to improve access to various day-to-day functions for people with disabilities. One key stakeholder indicated how mobile and remote CloTs allow people with vision or hearing impairments to have a greater degree of independence:

Mobile phones changed their entire lives because it was a device that they could wear and own and completely control themselves, whereas prior to that, a PC was a remote machine that someone else sort of managed for them.

A3, Advocate

Table 13 outlines the perceived value of CloT device functions. Some functions considered most valuable include the ability to monitor energy or water use (3.61), remotely access home security systems (3.58) and connect devices from multiple manufacturers (3.56). In contrast, respondents showed lower comparative value for relinquishing control over decision-making to the CloT device

(2.81) or sharing data with third parties (2.63). CloTs such as smart doorbells were seen to have some beneficial ‘security features - to protect your home and family’ (TS 11, Technical and Security Expert).

Table 13 Perceived value of functions and characteristics of IoT devices

(As an average across the sample; 1 = ‘not at all valuable’ to 5 = ‘completely valuable’)

Item	Mean	SD
The need to install regular security updates	3.64	1.08
Monitoring energy/ water use	3.61	1.10
Remotely accessing home security systems	3.58	1.14
The ability to connect devices from multiple manufacturers	3.56	1.12
The ability to connect with and operate multiple devices	3.56	1.06
Setting an alarm	3.50	1.15
Greater interconnectedness between devices	3.46	1.06
Storage of data within the cloud	3.42	1.13
Voice/ hands-free activation	3.32	1.15
Environmental impacts of always-on devices	3.32	1.16
Automatic traffic notifications	3.30	1.12
Scheduling daily tasks	3.28	1.11
Making daily tasks easier (such as reminders from Siri)	3.27	1.18
A need for ongoing device maintenance	3.24	1.10
Increasing automation of daily life	3.16	1.11
Voice-activated internet searches	3.10	1.20
Controlling your household lighting	3.03	1.20
Remotely controlling room temperature	3.03	1.20
Growing dependence on the Internet for basic household functions	2.89	1.18
Relinquishing control over decision-making (e.g., whether to change temperature)	2.81	1.18
Remotely feeding pet(s)	2.67	1.28
Sharing of data with third parties	2.63	1.23

Concerns about IoTs

Concerns over the data collection functions of CloTs were found in both the consumer survey and interviews with key stakeholders. The multifaceted nature of the data collected was raised by one IoT security expert as a significant concern:

... if all of a sudden your location, your activities or if there’s someone else in the room suddenly are detectable even at relatively low levels of information... You’re suddenly starting to reveal much more about yourself, your preferences, your relationships, when you’re at home, when you’re not at home and what you’re doing at home or in fact any place that is being monitored in ways we have never considered before.

TS2, Technical and Security Expert

These issues raise the prospect of unauthorised access or data breaches. This is considered a major problem given the lack of stringent regulation of CloT security:

if companies don't have an obligation to make sure that they are selling things that are secure then obviously that's going to be the focus for attempts to ... unlawfully access networks.
PP9, Privacy Professional

Table 14 ranks the perceived concerns about the types of data collected by IoTs amongst survey respondents (5 = most concerned and 1 = least concerned). Respondents were most concerned about the collection of data relating to their credit card details (4.36), phone conversations (4.20), and photographs (4.19). By contrast, respondents were less concerned about the collection of data about their music and media preferences (3.08), the contents of their refrigerator (3.12) or their proximity to others to prevent the spread of illness (3.25).

Table 14 Perceived concern about different types of data collection by IoT devices

(1 = 'not at all concerned' to 5 = 'very concerned')

Item	Mean	SD
Your credit card details	4.36	0.96
Phone conversations	4.20	1.05
Personal photographs	4.19	1.01
Access to documents stored in the cloud	4.17	1.00
A list of your contacts	4.15	1.01
Details about your family relationships	4.08	1.06
Your home address	4.05	1.07
A recording of your voice	4.04	1.07
Your medical history	4.03	1.11
Security camera recordings	4.02	1.13
Details about your sex life	4.02	1.20
When and where your family holidays	3.99	1.12
Data about your location	3.95	1.06
Your daily schedule	3.87	1.15
Your internet search history	3.82	1.11
Details about your workplace/ employer	3.74	1.19
Your name	3.63	1.19
Sleep patterns	3.44	1.29
Records of your heart rate	3.40	1.30
Your body temperature	3.32	1.31
When/ how much electricity you use	3.29	1.21
Your proximity to others to prevent the spread of illness	3.25	1.29
The contents of your refrigerator	3.12	1.37
Music and media preferences	3.08	1.28

Concerns were also raised in key stakeholder interviews over the practice of ‘bricking’, where access to device functions is remotely denied by the service provider, often because software licenses have expired or have been bought and sold through corporate activities that are beyond a consumer’s control (see Tusikov, 2019). The lack of forewarning associated with bricking is of particular concern to consumers: ‘you ... expect your device to work and its stopped working for no discernible reason’ (TS1, Technical and Security Expert). In addition, key stakeholders reflected that CloTs have clear environmental impacts stemming from their manufacture and disposal:

Use of rare scarce resources to possibly very limited positive effects just feeding excess consumption essentially for many of these more frivolous devices.
TS1, Technical and Security Expert

Information and security risks of IoTs

Several experts in IT security expressed concerns about the design of many CloTs. Security issues were considered a particular problem that has not been adequately factored into the product design-stages:

Security is not there ... The way that IoT is designed, is created, it is inherently insecure because the architecture, the purpose of the architecture, is to allow data to flow from the collecting environment into some sort of central or intermediate point depending on how far the data is taken. And the device is low power by definition. They’re low power devices, which means they lack the capacity to support their energy. Their energy signature is insufficient to support the requirements of strong cryptography, that’s not to say that that’s the way that it has to be but that is the result of a number of choices we have made.
TS3, Technical and Security Expert

An Australian cybersecurity expert pointed to the lack of security features and disposability as two major problems with CloTs:

It’s amazing how much bad code there is ... When you combine that with relatively cheap devices that are thrown together in a hurry and put onto the market at scale with the idea that what we lose on each transaction we’ll make up in volume you end up with this interesting, well horrendous, financial incentive to throw out what in other contexts would be called unsafe products. And they’re then thrown out onto the market and tend to become abandonware, so they are not maintained.
TS4, Technical and Security Expert

According to several key stakeholders, there are various reasons for the lack of a clear in-built security structure for CloTs. One key stakeholder indicated that the ‘main goal is to just increase profit at any cost’ and expanded on this view in the following quote:

Security is something that's kind of annoying for these companies ... 'just put it out and if there's an issue we will just patch it up later, let's just get it out as soon as possible'.

RA1, Research/Academic

Another key stakeholder attributed this issue to the business model that drives the IoT Industry:

Nobody in the start-up world does security by design or privacy by design. They're all just building stuff to ship stuff as fast as they can. We've got a whole lot of people building stuff that have got no consideration for privacy and don't really have the resources to consider it.

TS5, Technical and Security Expert

Others suggested that CloTs are particularly 'vulnerable to hacking' (RA3, Research/Academic).

Weaknesses in encryption were also highlighted as a specific problem:

A lot of them [CloTs] don't really have much sort of encryption or anything else on a lot of their traffic or they don't really design that as part of the components, that's really not what they're focussed on when they're designing them.

TS8, Technical and Security Expert

The purported technical insecurity of CloTs raises additional concerns about the longevity and environmental legacies of these devices.

Privacy concerns

Privacy risks were considered to mainly stem from the lack of adequate information disclosure by CloT manufacturers. This impacts consumer understanding of the scope and scale of data being collected.

This was described by one technical and security expert in the following way:

... connected fridges ... I think they're collecting and sharing a lot of information that people probably don't understand that's getting collected and getting used and shared.

TS8, Technical and Security Expert

One key stakeholder in the regulatory sphere indicated:

I would like to see transparency around what is being collected, and where it is going and for how long it is stored and to what end it is used and also the ability to understand a device when it is given to you.

TS10, Technical and Privacy Expert

Privacy issues have significant impacts on individuals who do not purchase and set up CloT devices yet are directly affected by their routine collection of personal data. This has specific impacts on children, people who are aged or living with disabilities, and people who rent properties where CloTs have been pre-installed. In each case, people depend on others to set these devices up or monitor their ongoing operation on their behalf:

In the case of ... an older adult who has their devices set up for them by a younger relative they never even had any type of way of knowing that there are privacy risks.
RA1, Research/Academic

These risks were also recognised as a particular concern in cases of family violence (see Dragiewicz et al., 2019):

There's also the risk of someone who has or had legitimate access who shouldn't anymore. So we hear a lot of stories ... unfortunately of relationship breakdowns where usually the man, the male partner is the one who has installed all these devices because technology is male dominated so they know all the passwords and then they break up and their wife or girlfriend has these devices in their house but the partner who has now left still has access to them and can use them to harass them.
TS 4, Technical and Security Expert

CPIoT survey respondents indicated varying degrees of concern about these privacy issues. Table 15 outlines the responses to eleven items developed to measure privacy concern. Consumers expressed a clear preference for having 'control over how our personal information is collected, used, and shared by technology companies' (approx. 79% agreement), being 'aware of how my personal information is used by a technology company' (approx. 78% agreement), and considered technology companies 'should not use my personal information for any purpose unless I have authorised it' (approx. 80% agreement). Milder concerns were expressed about other issues, with only approximately 60% of respondents 'troubled by requests to disclose personal information when setting up a device', 60% expressing direct concern that 'personal information could be stored overseas', and 64% concerned that technology companies should 'not be allowed to share consumer data, without obtaining their consent, to assist with product development'. These findings emphasise that while a large majority of consumers want control of their data and to be aware of how it is used, a smaller majority is concerned about specific instances of companies sharing their data or transferring it overseas.

Table 15 Responses to items measuring privacy concern

(n=1052)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
It bothers me when a technology company asks me to provide personal information in exchange for using their service	40 (3.8%)	185 (17.6%)	331 (31.5%)	276 (26.2%)	220 (20.9%)
I am troubled by requests to disclose personal information when setting up a device that connects to the internet	22 (2.1%)	89 (8.5%)	302 (28.7%)	403 (38.3%)	236 (22.4%)
It concerns me that my personal information could be stored overseas	45 (4.4%)	150 (14.4%)	214 (20.4%)	246 (23%)	397 (37.8%)
I believe consumers should have control over how our personal information is collected, used, and shared by technology companies	14 (1.3%)	34 (3.2%)	170 (16.2%)	348 (33.1%)	486 (46.2%)
If I want to connect a device to the internet, it is unreasonable to give some control over my personal information to a technology company	90 (8.6%)	298 (28.3%)	337 (32.0%)	186 (17.7%)	141 (13.4%)
I think technology companies should not be allowed to share consumer data, without obtaining their consent, to assist with product development	36 (3.4%)	131 (12.5%)	192 (18.3%)	266 (25.3%)	427 (40.5%)
It is important I am aware of how my personal information is used by a technology company	11 (1.0%)	37 (3.5%)	176 (16.7%)	367 (34.9%)	461 (43.9%)
I believe technology companies should not use my personal information for any purpose unless I have authorised it	19 (1.8%)	25 (2.4%)	153 (14.5%)	303 (28.8%)	552 (52.5%)
I think it is unreasonable that technology companies are required to obtain consent from customers before sharing their personal information with another company	103 (9.8%)	162 (15.4%)	193 (18.4%)	193 (18.3%)	401 (38.1%)
I think technology companies should be responsible for preventing unauthorised access to their customers' personal information	103 (9.8%)	154 (14.6%)	190 (18.1%)	206 (19.6%)	399 (37.9%)
I think databases containing personal information should be protected from unauthorised access, no matter the financial cost	15 (1.4%)	30 (2.8%)	165 (15.7%)	331 (31.5%)	511 (48.6%)

Responsibility

The CPIoT survey measured respondent beliefs about the level of responsibility consumers currently have for the protection of their privacy. Respondents indicated they thought consumers have ‘quite a bit’ or ‘a lot’ of responsibility for educating themselves about the functions and issues associated with CloT devices, with a comparative minority viewing consumers as having ‘all’ or ‘none’ of these responsibilities. These results are depicted below.

Table 16 Perceived responsibilities of individual consumers

Consumer Responsibility	N	%
None	26	2.5%
A little bit	179	17.0%
Quite a bit	417	39.6%
A Lot	361	34.3%
All	69	6.6%

Table 17 outlines respondent views about which organisations are responsible for raising consumer awareness about the privacy impacts of CloTs. Most respondents ascribed responsibility to technology companies (n=570, 54%), followed by almost a third of respondents (n=300, 29%) holding government agencies responsible.

Table 17 Perceptions of organisational responsibility for raising consumer awareness of IoTs

Organisational Responsibility	N	%
Government agencies	300	28.5%
Technology companies	570	54.2%
Retailers	148	14.1%
Other	34	3.2%
TOTAL	1052	100.00%

Many key stakeholders indicated there should be greater emphasis on protecting consumers. A common theme in interviews was to avoid placing ‘*excessive reliance upon consumers to self-manage safety and privacy settings in respect of their IoT devices*’ (TS11, Technical and Security Expert). Another key stakeholder expressed this issue as an expectation that PbD or security-by-design should be default settings for CloTs:

I shouldn't have to ... look inside the box or go searching on the web to find out that the privacy settings are privacy by design and security by design at default. That should be a reasonable assumption that I can make as a buyer of a IoT device and if the setting is other than that, well there should be prominence in the warnings to me ... that the settings are other than privacy and security by design as default.

TS11, Technical and Security Expert

However, one key stakeholder indicated the responsibility is with the consumer to 'balance up what other services you actually need and those that you don't need ... that is an individual choice' (PP4, Privacy Professional). The difficulty with this reasoning, as another key stakeholder suggested, is:

A lot of the stuff in this space is so nuanced and so sophisticated that the average person does not have the background to be able to make an informed decision on it.

PP7, Privacy Professional

It was considered that more corporate responsibility was necessary on this issue. This was stated in the following way by a respondent in an advocacy role:

Why is the onus not on the company to also say ok well, it's my corporate social responsibility to make sure that by selling this product I am not actually going to be putting people in harm's way?

A2, Advocacy

Children and IoTs

While vulnerability cuts across many dimensions, both the survey and interview data identified children, people from culturally and linguistically diverse (CALD) backgrounds, and people with vision and/or hearing impairments as having specific needs with respect to CloTs.

Children were considered by many key stakeholders to be particularly vulnerable when it comes to CloTs and IoToys. One key stakeholder indicated the central problems were:

... vulnerability and need for protection combined with parents' uncertainty often about how to protect their children. There's a need for parents to have more information with how these things [CloTs] work and what role they can play ... [and] there's a danger that parents will be less vigilant when it comes to IoT's.

RA2, Research/Academic

This is seen by some to be a key problem with contemporary surveillance technologies and the inability of children to consent to data collection practices. For example, one key stakeholder described this problem as stemming from the inability of:

... a child to consent to being tracked for the information that is on their device that their parents bought them for Christmas, I don't know if they bought a step tracker or something, and that is sending information off to a US based

surveillance company. A 9-year-old can't give consent at law ...
TS4, Technical and Security Expert

The CPIoT survey also measured parents' and guardians' (n=475) perceptions of children's privacy. It is clear respondents held agreed concerns about their child(ren)'s privacy. Table 18 summarises these responses. Over 75% of respondents indicated they were 'concerned about technology companies collecting and storing personal information about my child[ren]' and technology companies should be 'legally compelled to delete any personal information they obtain about children'. Over 70% of parents and guardians also indicated they avoid posting personal information about their children on the internet. Similarly, over 60% of parents and guardians reported that they consider the impacts of CIoTs on their child's privacy before making a purchasing decision. Finally, a smaller majority of slightly over 50% supported the rights of children to determine what personal information about themselves is published online.

Table 18 Summary of perceptions of children's privacy*(n=475)*

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Before deciding to purchase an internet-connected device, I consider how it will impact the privacy of my child[ren]	2 (0.4%)	24 (5.1%)	111 (23.4%)	209 (44%)	129 (27.1%)
I avoid posting personal information about my child[ren] on the Internet	3 (0.6%)	18 (3.8%)	100 (21.1%)	161 (33.9%)	193 (40.6%)
I think children should be able to decide what information about them is published on the internet [e.g. photographs, birthdate]	57 (12%)	56 (11.8%)	112 (23.6%)	158 (33.2%)	92 (19.4%)
I am concerned about technology companies collecting and storing personal information about my child[ren]	5 (1.1%)	13 (2.7%)	93 (19.6%)	179 (37.7%)	185 (38.9%)
I think devices that connect to the internet, such as a smart watch, are useful for monitoring the safety of my child[ren]	14 (3.0%)	29 (6.1%)	191 (40.2%)	181 (38.1%)	60 (12.6%)
I believe technology companies should be legally compelled to delete any personal information they obtain about children	5 (1.1%)	14 (3.0%)	93 (19.5%)	163 (34.3%)	200 (42.1%)

The examination of PPS clearly showed many companies communicate that they *'respect the privacy of children'*, with a number of CIoT and related services *'not designed to attract an audience younger than 16'* or by informing consumers that *'we do not knowingly collect personal data from children under 16.'* This is in line with tighter restrictions on obtaining information about children and the surveillance issues associated with IoT (see for example Electronic Privacy Information Centre, 2018; McRae, Ellis and Kent, 2018; Forbrukerrådet, 2017; Mascheroni, 2018; Forbrukerrådet, 2016). Despite these clear disclosures, CPlOT survey data showed an overall perception that greater measures are required to protect the privacy of children.

CloTs and accessibility

CloTs have enormous potential to enhance day-to-day living for people with vision or hearing impairments. Indeed, specific references to the need for recognised accessibility standards in recommendations 24-38 of the Australian Human Rights Commission Inquiry into Technology and Human Rights (2021), aim to ensure new digital technologies are easily accessible to people with various levels of ability. However, there was concern amongst key stakeholders that technology companies had ignored these populations when designing and developing CloTs. This comes with certain risks, as one key stakeholder explained:

There is a real danger that ... if there is not a shift either culturally or legislatively or both towards greater focus on accessibility we could end up with a situation where people who are blind or have low vision are more excluded than they are now.

A1, Advocate

The general view was technology companies and governments have failed to ensure people with vision and/or hearing impairments are accommodated when new technologies are designed, developed and sold. For people with vision impairments in particular:

... there is a greater need for protection [because] ... we are more likely to have to provide data that other people don't have to provide and again because most of these apps are developed by companies that are not based in Australia the opportunity to access data is very limited.

A1, Advocate

People with disabilities are more reliant on carers and other people, which reshapes their views of privacy. One key stakeholder indicated this is not a concern amongst most of the population:

I think we are quite used to having our privacy sort of violated, usually with our consent but not always ... [but] I don't think that it is something that [other] people are going to get hugely concerned about.

A2, Advocate

However, the question of accessibility creates a bind for many people because the technology has the potential to significantly enhance their independence. The privacy issues stemming from the 'risk and reward' nature of CloTs are aptly captured in the following quote:

I can control my heating and air conditioning ... [remotely]. For anybody else, that's nice to have. For me, that's the difference between my air conditioning system being accessible or inaccessible. If it's a toss-up between giving away some of my privacy and gaining some accessibility, I am always going to choose gaining accessibility.

VA2, Vulnerability Advocate

Lack of accessibility is magnified because around 4.4 million, or 1 in 6, Australians has some form of disability (AIHW, 2020). However, it is considered this population is not a sufficiently *'large cohort who are [sic] going to drive [commercial] demand'* in the technology sector (A3, Advocate). This can lead to vulnerable people becoming reluctant to engage with technology because of the perception that it is unsafe, which can deprive them of the benefits of CloTs. This reluctance primarily stems from the exclusion of people with varying disabilities from the design process, and partly because *'they just never opt in because no one will ever tell them it's safe enough'* (A3, Advocate). The lack of inclusion on political, regulatory and design issues associated with CloTs, which includes broader questions regarding digital accessibility and privacy, means that people with disability *'never understand if they actually have influence ... [or] what the outcome of their contribution will be'* (A4, Advocate).

Conclusion

The CPIoT survey data shows CloT consumers have less concern for privacy issues when compared with non-CIoT consumers, and those who own CloT devices emphasise their benefits over their risks. CloT device users have strong concerns about the ability of CloTs to collect data such as credit card information, details of phone conversations and personal photographs. Similarly, several key stakeholders with expertise in IT security expressed strong reservations about general standards of data security and the transparency of information about data collection by CloTs, particularly in circumstances where individuals have not necessarily played a role in the set up processes, such as children, people with disabilities, the elderly, those in family violence situations or renters. Consumers demonstrate a clear desire to control their personal data and have some degree of authority over the types of information shared by technology companies but have softer positions on whether they are willing to provide personal information to technology companies, or whether their personal information should be stored overseas. Key stakeholders often expressed the firm belief that technology companies need to do more to protect consumer privacy, whilst CPIoT survey respondents emphasised that consumers also have a significant level of responsibility for managing their own privacy exposure.

Chapter 6. Privacy and Regulation

Interviews with key stakeholders working in the fields of information security, privacy and regulation revealed extensive concerns about the types of data collected, analysed and stored remotely through the routine use of CloTs. Likewise, the effectiveness of current regulatory frameworks, including Australian privacy and consumer laws, was also a concern. This chapter details these views and reflects upon the role of consumer law as an alternate or complementary field of law that could be strengthened to deal with the privacy issues presented by CloTs. Drawing on established regulatory theory, including responsive and ‘smart’ regulation (see e.g., Ayres and Braithwaite, 1992; Braithwaite, 2017; Gunningham and Sinclair, 2017; Richardson et al., 2017), this chapter identifies potential avenues for future reform. The chapter also includes a discussion about how security and product standards for CloTs can be enhanced by combining technical and enforcement approaches to the ‘smart’ regulation of ‘smart’ things.

Problems with privacy law, regulation and enforcement

One problem identified with ‘*regulation and legislation is [that] you have to know what you’re regulating and legislating and ... it’s an ever-moving target*’ (TS7, Technical and Security Expert). Indeed, it is hard to ensure CloT devices are appropriately regulated in the face of new technological developments. It is often stated that the law lags behind new technology:

The rate of IT development and progress and expansion and intrusion is much much faster than the rate of government regulation or monitoring. It’s a runaway train.

PP6, Privacy Professional

There is also concern amongst key stakeholders that the privacy legal and regulatory framework in Australia is insufficient to deal with digital technologies. This concern has prompted two ongoing reviews: one by the Australian Competition and Consumer Commission (ACCC, 2020) into digital platform services (2020-2025) and the other a federal government review into the *Privacy Act 1988* (Cth) (see OAIC, 2020). One key stakeholder remarked that there is an incoherent legal and regulatory system governing digital technologies in Australia:

It is now pages of laws that are mutually inconsistent and very patchily enforced. There is no need for more law yet because we don’t know if the current laws work.

PP3, Privacy Professional

This key stakeholder also remarked that there is no real substance to defining or protecting privacy under existing law:

If you have a look at the Privacy Act, there is no definition of privacy in there. Like all data protection and privacy laws the meat is in a set of principles and those principles are only process requirements [that determine] if you collect information you've got to tell people you're collecting it. Nobody has ever demonstrated the linkage between those process requirements and an undefined concept of privacy.

PP3, Privacy Professional

There are several broader issues regarding the lack of a collective or group right to privacy (see for example Mann and Matzner, 2019; Loi and Christen, 2019). This was expressed by a leading technical and security expert:

Insofar as we are able to arrange privacy to comply with legislation and indeed individual preferences, whatever they may be, I don't believe we have any mechanisms for applying those requirements to a group. In the simplest example you have a device placed in a home, a smart TV for example. It is going to apply equally to all members of that family but somebody in the family is going to be the person who sets its settings and if somebody else in that family has different preferences, well when they all sit in the same room together it cannot possibly observe a mixture of preferences all simultaneously and this to me is a major challenge which I don't think we have any way of approaching at the moment.

TS1, Technical and Security Expert

This challenge is exacerbated by CloTs that often collect data from anyone within their vicinity, not just the person who sets up the device. As indicated by an expert in privacy regulation:

That means anyone can ask it questions, it's not just ... [the person] authorising it. That's a problem ... obviously getting the right people to monitor these things, that's difficult.

PP4, Privacy Professional

It was also suggested the APPs are largely irrelevant to organisations that are 'driving the development of technology' (A3, Advocate). This problem is magnified because there is a view within the global IoT industry that 'if you're developing something you will only do the barest minimum that you're required to do' (TS7, Technical and Security Expert).

There are important questions regarding the value of the *Australian Privacy Act 1988* (Cth) and the 13 APPs in adequately covering the functionality of CloTs. According to one key stakeholder, part of the problem is the existence of 'a lot of laws and regulation with very little enforcement' (PP13, Privacy Professional). One major concern about privacy regulation in the Australian context is financial, with many key stakeholders indicating budget limitations restrict the capacity of the Office of the Australian Information Commissioner (OAIC) to adequately undertake its regulatory functions. Further, the APPs do not apply to corporate entities with an annual turnover of less than AU\$3 million, which was viewed

by one key stakeholder as an outdated exemption that does nothing to ensure ‘privacy is going to be embedded into culture [or] corporate culture’ (A1, Advocate). As a result:

What if the companies deploying the IoT's are start-ups or small businesses ... and those companies have hybridised ... with plug-ins from various different other companies, including the data giants? Then what you have is a part of the sector that is not even captured by privacy law deploying IoT's to homes and all of that data is sitting in this unregulated space.

PP1, Privacy Professional

This key stakeholder also suggested privacy regulation is fragmented and largely confined to government departments rather than the private sector:

There isn't that additional layer of protection for individuals. So what governments do with your personal information is regulated by the privacy laws here in Australia ... and the government has to use it in accordance with that law. When we are talking about IoT's that are deployed in the domestic sense - who is regulating that? What happens to that data? There is so much fragmentation the world over.

PP1, Privacy Professional

The role of consumer law

Several key stakeholders discussed whether consumer protection law can help foster minimum standards for CloT product quality and safety. For example, one respondent suggested that minimum standards could provide a guide for law reform in the privacy realm:

The time is well past due that we have a national conversation about how much privacy everyone should be able to enjoy as a minimum standard. And we should be defining minimum standards in the same way that we do for other areas where it's a minimum acceptable product quality. Individuals choosing to purchase products that are of a higher quality level. I don't think it's possible to do that because the quality level isn't there in the [IoT] market. It would arrive quicker if we had something like the equivalent of safety belts, minimum quality standards.

TS4, Technical and Security Expert

Clear standards offer one possible response to the lack of consumer knowledge of how CloTs operate. However, the ability of current consumer law to address many of the technical issues associated with the operation of CloTs appears limited:

I don't think they [regulators] take cognisance adequately of the nature of the risk that IoT devices bring into a consumer's world, and it's because of the nature of firmware ... [consumers] when they buy their IoT devices they don't have the level of technical knowledge that they need to know to make sure they are safe and I don't think consumer law takes cognisance of that.

TS5, Technical and Security Expert

Several key stakeholders indicated consumer law offers several benefits for enforcing compliance *‘because it starts from the concept that an organisation, a supplier, should not be misleading or deceptive’* (TS11, Technical and Security Expert). This emphasis can offer some protection because corporations *‘must show that you have taken adequate steps to seek consent where it is required’* (PP1, Privacy Professional). One key stakeholder suggested consumer law could integrate provisions relating to *‘warranties about what’s happening to your information’* that might improve or extend notions of consent that are viewed as *‘not sufficient for operating services’* (PP4, Privacy Professional).

A strategic use of privacy and consumer law in conjunction may offer an avenue for the improved governance and regulation of CloTs. However, there is always the problem of effective enforcement: while consumer law might add a further dimension to the regulation of privacy and CloTs, the underlying issue that *‘consumers have very little access, real access of [sic] justice related to this’* (RA3, Research/Academic) remains.

Regulatory responsiveness: self-, co- and ‘smart’ regulatory approaches

Ayres and Braithwaite’s (1992) model of responsive regulation and the accompanying enforcement pyramid could serve as a template to regulate CloTs (see also Richardson et al, 2017). This model aims to be *‘responsive to the regulatory environment and to the conduct of the regulated in deciding whether a more or less interventionist response is needed’* (Braithwaite 2017, p. 117; see also Parker, 2013). A responsive regulatory approach involves graded and escalating levels of enforcement, along with the imposition of sanctions, that start with incentivising compliance and move towards more stringent responses. As Richardson et al. (2017, p. 8) point out, this could commence with self-regulation through PbD *‘as a first and fairly minimal’* response to the regulation of CloTs. This could then escalate to enforced self-regulation, then command regulation with punishment for repeated non-compliance. Direct consumer and data protection standards for CloTs could then escalate to privacy-based doctrines enforced through litigation (Richardson et al., 2017, p. 9), or co-regulatory approaches where design and enforcement are shared between a regulator and those being regulated (see Levi-Faur, 2011a; 2011b). Finally, *‘smart regulation’* can entail multiple responsive regulatory strategies and parties (see Gunningham & Sinclair, 2017). This could involve, for example, a combination of approaches aimed at improving the technical design of CloTs to ensure privacy and consumer rights are protected, enhancing consumer awareness through icons and developing enforceable privacy standards in collaboration with industry.

Certainly, many key stakeholders indicated regulatory reform was necessary to deal with the combination of technical, privacy and consumer protection issues associated with CloTs. There was also widespread agreement that existing regulatory models dealing with information privacy are outdated and unable to meet the technological challenges of CloTs. One key stakeholder explained there are few mandated or minimum requirements for technology companies to follow or be 'compliant' with, which undermines the capacity for self-regulation or industry-based standards to protect consumers and their rights:

A lot of these laws were developed either before the world wide web or just shortly after the world wide web was becoming popular and haven't gotten a chance to really catch up to what we see going on today with the new level of data collection and retention ... if there's no regulatory mandate to ... have privacy by design in your devices the companies won't.

RA1, Research/Academic

The need for minimum or mandated standards for improved information security was considered particularly important amongst technical and security experts. For example, it was suggested manufacturers should be required to adopt 'at least encryption of some sort' (TS8, Technical and Security Expert), even if this might increase the prices of CloTs. One key stakeholder expressed concerns about the Australian IoT Code of Practice for providing minimal regulatory guidance or enforceable standards to improve the design and marketing of CloTs:

when I looked at the IoT code ... [the aim] is to identify something that everybody in the community would look at and say ... this industry should not be doing this thing, so they will put it in the code and say we're 'not going to do this thing'. But the fact is they [the technology industry] never wanted to do this thing. They're actually creating rules against things that nobody ever wanted to do, which just raises the suggestion this [the code of practice] is all window dressing, this is just PR ... and when it comes to things they do want to do there's a lot of weasel words and a lot of loose language.

RA2, Research/Academic

However, one key stakeholder suggested that stronger standards or enhanced regulation could also be considered as 'regulation for regulation's sake' (TS7, Technical and Security Expert). In addition to the perception that codes of practice are regulating the wrong things, there is concern that a compliance-based model is insufficient because of a lack of appropriate enforcement. Many key stakeholders indicated there needs to be a move away from a 'goodwill kind of voluntary principles-based approach to a more legislative approach' with stronger and more coercive enforcement (A1, Advocate). This view is considered appealing due to the widespread perception that voluntary codes of practice or self-regulation results in 'no enforcement at all' (TS9, Technical and Security Expert).

Consideration was also raised about the need for different standards to protect ‘sensitive data subjects’ (TS2, Technical and Security Expert). This recognises that certain groups, such as children or people from CALD communities, can be exposed to quite particular types of harm. One key stakeholder described the need for regulation to protect sensitive data subjects in the following way:

All around the world groups like the Australian Bureau of Statistics will talk about sensitive data subjects so children, minorities, data about religious or sexual orientation are all areas where ... The data subject is one of the dimensions of sensitivity that you need to think about and therefore different levels of data governance need to be applied.

TS2, Technical and Security Expert

This means the type of data subject should inform the nature and degree of regulation applicable in any given situation.

Another strong theme from the key stakeholder interviews was the perceived need for governments and technology companies to develop better methods to ensure individual privacy is protected. This was expressed as an important governmental responsibility by one key stakeholder:

The onus is on governments to ensure that even if you don't read the documents that your rights, your privacy and data is going to be protected because there are sufficient requirements on companies to ensure that. I don't think we should be putting consumers in a position where they have to accept all of the risks or not have access to a product. I think we have got to find a way as a society to ensure those risks are borne by the developers. Some kind of regulation, whether its legislation ... [or] stricter principles, better promotion, better or more public attention given to privacy issues I really think is essential.

A1, Advocate

Finally, several key stakeholders indicated that increased funding was needed to ensure the OAIC has adequate resources for conducting investigations. This sentiment was captured in the following quote:

They've actually been reducing the budget of the OAIC and the staff there over the last 3-4 years. So, from our view, it doesn't make sense that you're strengthening the regulations but you're reducing the capability of the regulator to actually do something ... because it is a manual process. You've got to investigate these things. You've got to find out whether the company, corporation ... was negligent and to do that you need resources.

TS9, Technical and Security Expert

Importantly, the OAIC has received increased funding relating to its mandates regarding the Consumer Data Right and My Health Record (OAIC, 2021).

Improved security, product standards and enforcement

A complementary avenue of regulation could involve requiring stronger uniform minimum standards for CIoT product development. This was expressed by one technical and security expert in the following way:

There should only be one standard, or there should be a small number of standards. It is the assurance frameworks and where you put those thresholds in those assurance frameworks which I think are more important.

TS2, Technical and Security Expert

One key stakeholder suggested the United Kingdom's (UK) IoT Security Foundation (IoTSF) offers a viable model that could be emulated in Australia:

IoTSF ... they are quite strongly UK based and orientated, in fact it is an industry voluntary body of some relatively enlightened people from a number of firms involved in the area who realised ... that IoT security was a major problem.

TS1, Technical and Security Expert

The UK has also introduced an IoT Toys certification scheme, administered by IoT Scheme Limited, which is funded through the Department of Digital, Media, Culture and Sport. The Internet Toys Certification Scheme website at https://iotoys.org.uk/about_us, allows consumers, manufacturers, reviewers and conformity assessment bodies to examine the security and age-appropriate design components of various devices that are directly marketed to and for children in line with European product standards. In providing 'guidance on the level of connected functionality', this process aims to reduce 'the risk of vulnerabilities in children's connected toys' while 'providing parents with that much needed peace of mind'.

Organisations such as the IoT Alliance Australia (IoTAA) could potentially assist with an equivalent CIoT certification process. One key stakeholder considered this could be helpful in implementing 'meaningful standards' (TS10, Technical and Security Expert) that ensure manufacturers or producers represent their products accurately. A certification procedure could equally assist in raising standards for consumer protection and privacy through an industry-based or industry-led system, supplemented by industry-endorsed icons. Another key stakeholder suggested an incentive-based regulatory process, with positive rewards for the proactive design of CIoTs to promote privacy, could be developed at the lower levels of the responsive regulation pyramid:

At the moment everything is about disincentives, but the problem is ... these organisations ... do risk assessments to determine [that if they] ... don't really align to the spirit of ... [the] law ... [then] what's the actual likelihood that we get fined. If we do get fined, how much is it going to [cost]? What if there was a positive, like an incentive. Let's

Speak the language of corporations. Let's make it a monetary incentive for corporations to demonstrate that they have done this stuff- up front, proactively by design.

TS6, Technical and Security Expert

One academic stakeholder suggested an icon system could work through gold, silver and bronze medal rankings to denote proactive PbD or regulatory compliance (RA1 Research/Academic). This could be administered either by an industry organisation or government department.

There was, however, significant concern amongst key stakeholders about the efficacy of self-regulation in the technology industry, with one indicating this approach *'has never ever worked'* (TS3, Technical and Security Expert). Specifically, there are discernible limits with self-regulation if there are no incentives to motivate commercial industries to achieve compliance:

Self-regulation and voluntary codes work only so far as there is strong internal regulation ... I don't think the financial incentives, which are the ones that actually matter in this market, I don't think the [current] financial incentives are aligned with a voluntary code of conduct [for CloTs].

TS4, Technical and Security Expert

A major difficulty is designing effective regulation, given that it is relatively easy to identify and criticise regulatory regimes. One option could involve a multi-faceted approach towards CloT regulation, or the 'smart' regulation of 'smart' devices (as per Gunningham & Sinclair, 2017). This was proposed by one key stakeholder in the following way:

The answer is probably a regulator backed by standards, backed by conformity assessment and backed by principles in law which understand the world differently from the way that more law has been drafted to date. To acknowledge that, that gap between the principles of law ... and the bits that are moving at gigahertz speeds ... so that you don't have to stop everything you need to do every single time ... To decide, 'yes that bit can go forward' ... A sophisticated regulator and a rethink next level down in some of the principles of law.

TS2, Technical and Security Expert

Improved enforcement of existing regulations was preferred by several respondents, through *'visible enforcement, not just the threat of enforcement'* (PP3, Privacy Professional). One possibility could involve expanding the ACCC's power to impose fines:

ACCC should actually audit. If you don't have a policeman ... out with a speed gun in the street ... you'll drive faster ... And then when you do see that they catch people, the fine is 1% of the real cost.

PP14, Privacy Professional

Several key stakeholders indicated the regulation of CloT advertising for specific populations, such as children, was also necessary. One also identified a need to regulate the predictive analytics and

profiling associated with the data created by CloTs. This could be akin to the approach taken under Article 22 of the European Union General Data Protection Regulation (GDPR) that grants a right not to be subject to automated decisions or profiling³ (see also Mann and Matzner, 2019). Finally, in relation to the stronger protections in the EU with its enforceable human rights framework under the European Convention of Human Rights, one key stakeholder indicated the only way to ensure appropriate legal and regulatory reform in Australia is through constitutional changes that integrate enhanced human rights protection:

There should be a fundamental right to privacy encoded in the constitution. We need to have a Bill of Rights, so there should be a backstop of minimum standards for every Australian to enjoy, and it shouldn't then matter what happens with funding and regulators whether regulators do their job or not. We are then able to rely on those core protections and can take action through the judiciary ourselves, up to the high court and higher.

TS4, Technical and Security Expert

Conclusion

As detailed throughout this chapter, key stakeholders described many issues with privacy laws, regulation and enforcement in Australia. However, opinion remains divided on the best approach when looking to the future of regulating CloTs. Based on expert stakeholder views, and established regulatory theory, it is recommended a combination of approaches to incentivise compliance and self-regulation by industry is necessary in the first instance. However, this must be backed with stronger external enforcement via a better resourced OAIC or ACCC to assist with enhancing security and product standards for CloTs. Together these approaches may offer the best starting point for the 'smart' regulation of 'smart' technologies.

³ Article 22 of the GDPR states: The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Chapter 7. Icons

A series of icons was developed that could potentially enhance consumer awareness of privacy issues associated with CloTs. These were tested in both the CPlOT survey and during interviews with key stakeholders. This chapter reviews the broader process of icon development and the perspectives of their value amongst survey respondents and key stakeholders.

Icon design

The design of icons to promote privacy awareness for CloTs is a complex issue that benefits from a strong evidence base (Cranor, 2021). Most key stakeholders gave notional approval to the idea of using icons, but also recognised that *‘part of the challenge becomes how can you make them widely understood and known?’* (PP3, Privacy Professional) The major problem key stakeholders identified is how to communicate complex information through basic visual imagery. This could favour the use of *‘symbols that don’t have meaning completely abstracted from context’* (PP3, Privacy Professional). It is also important to ensure clear interpretation with *‘easy English translations’* or the use of images, designs and concepts *‘that we know to be universally accepted’* (A4, Advocate). These issues require sensitivity to the visual design of icons themselves and the surrounding educational materials that give them meaning. There is also the issue of who has responsibility for the development, use, and placement of icons, which is arguably more important than what icons depict.

Several benefits of icons were identified by key stakeholders. These include the innovative development of simplified methods for conveying privacy issues at retail outlets, by enabling consumers to:

... take their iPhone and hover over that icon and, much the way a QR code takes you to a website, you could do that with an icon like this and get a very simple explanation of what that means.

PP1, Privacy Professional

Privacy icons could also assist with securing CloTs, or be built into the technology, much like a Wi-Fi signifier, to convey when personal data is being transmitted through device sensors. One key stakeholder suggested building icons into technology design might assist with understanding device functionality. For example:

In the consumer space, I go back to my experience trying to update firmware, my router, to make it more secure, change the DNS (Domain Name System) settings, to give consumers a quick and easy visual that shows them, makes them stop to think that privacy might be built in or they’ve considered privacy or its been verified by a

third party that they adhere to a certain standard, I think that's all a positive.

TS10, Technical and Security Expert

Likewise, icons may offset the time and complexity associated with reading privacy policies, provided there is *'some standardisation about what icons mean'* (PP1, Privacy Professional). One key stakeholder indicated that designing icons independently could be *'a more useful approach than waiting and waiting for effective regulation'* (TS11, Technical and Security Expert).

Several key stakeholders pointed to overseas examples of icons to illustrate their potential value. One key stakeholder described the New Zealand trust mark system, which is granted to businesses and manufacturers subject to formal endorsement by the Privacy Commission (see Figure 3):

The New Zealand Privacy Commissioner has a trust mark. It is a great idea for a Privacy Commissioner to be able to do but if you are going to put something like that in place you actually have to be able to ensure that the product is trustworthy.

PP8, Privacy Professional



Figure 3 Privacy Commissioner of New Zealand Trustmark – Te Mana Matapono Matatapu

California has introduced a mandatory icon to be placed on all approved products as part of a series of reforms aimed at promoting enhanced IoT security. This icon, depicted in Figure 4, was developed by an independent research team that tested various designs through several consumer evaluation trials (Cranor, 2021). The successful design was then incorporated into the California legislature's CloT regulatory framework.



Figure 4 Californian IoT Privacy Icon

(See Cranor, 2021)

Icon prototypes

The 13 APPs in the Australian *Privacy Act 1988* provided a guide for the icons developed for this project, although several designs also related to CloT functionality. Figure 5 depicts the prototype of an ‘offline icon’ that is designed to signify ‘the right to disconnect’, or that a device can function as intended without being connected to the internet.



Figure 5 Icon prototype: Offline

Figure 6 signifies that data from a device will be stored offshore. Australian consumers should be informed of this practice under APP 8.



Figure 6 Icon prototype: Overseas data sharing

Figure 7 depicts an icon, signifying that the device contains certain undetermined in-built privacy safeguards.



Figure 7 Icon prototype: Privacy safeguards

Figure 8 signifies that the CloT has child safety controls. While this icon is not matched to any of the APPs, it is considered important due to concerns regarding CloTs that are designed to entertain or monitor children.



Figure 8 Icon prototype: Child safety controls

Finally, Figure 9 shows an icon prototype that signifies a device's construction is environmentally conscious (see also Consumers International, 2019, p. 5). This design is also not based on the APPs but is considered important to promote awareness of eco-friendly design and disposal practices. The design is signified by a leaf with a white tick in the foreground that implies some additional regulatory structure to ensure compliance with relevant standards, which currently does not exist for CIoTs in Australia.



Figure 9 Icon prototype: Environmentally conscious

Table 19 documents intuitive consumer recognition of the meaning of these icon prototypes. Respondents were given multiple-choice options for each response, with no additional prompts regarding their meaning. This data indicates the child safety (70.6%), environmentally conscious (63.4%) and the privacy safeguards (62.0%) icons had the highest degree of accurate recognition amongst CPIoT survey respondents.

Table 19 Icon recognition task: Complete results

(Ordered by proportion of respondents who identified the prototype icons)

Icon	Accurately Identified	Inaccurately Identified	Unsure
Child Safety	743 (70.6%)	114 (10.8%)	195 (18.6%)
Environmentally conscious	667 (63.4%)	98 (9.3%)	287 (27.3%)
Privacy safeguards	648 (62.0%)	246 (23.4%)	158 (14.6%)
Overseas data sharing	566 (53.8%)	138 (13.1%)	348 (33.1%)
Offline	287 (27.3%)	292 (27.9%)	473 (44.8%)

Finally, survey respondents rated the usefulness of the proposed consumer icon system developed for this study. Table 20 demonstrates there was moderate support for the utility of the piloted consumer icons.

Table 20 Distribution of perceived utility of piloted consumer icons

Perceived Utility of Icons	N	%
Not at all	241	22.9%
Slightly	237	22.5%
Somewhat	336	31.9%
Quite a bit	187	17.8%
Completely	51	4.9%
TOTAL	1052	100.00%

Utility of icons

Almost three quarters of CPlOT survey respondents (74%, n=778) indicated the prototype icons would assist them when deciding to purchase a ClOT device. Among those who found some utility in an icon system (n=778), just over a third (37.3%, n=290) thought that icons would help them to better understand the data collection and sharing practices of technology companies (see Table 21).

Table 21 Reasons why consumer icons are perceived as useful

Reasons	N	%
I think a standard set of privacy-related symbols would help me better understand what information is being collected and shared by a technology company	290	37.3%
I would like to be able to compare privacy-related symbols when deciding which digital device to purchase	274	35.2%
I think other people would obtain useful information from privacy-related symbols that would inform their purchasing decisions	107	13.6%
I think this would be useful as current approaches to informing consumers about privacy rights are not working	100	12.9%
Other	7	1.0%
TOTAL	778	100.00%

Limits of icons

The limitations of icons were also considered in key stakeholder interviews. The following comment sums up these concerns: *‘If that was on the box would it mean this is safe for me to install in my home? That’s a big call.’* (TS5, Technical and Security Expert). In absence of clear regulatory or industry backing, icons could be misleading and potentially expose an authorised certifier, if one existed, to legal liability:

[What if] you make something which is explicit and it’s [actually] misleading or deceptive. If you put something on a product that says “safe” or “secure” or “certified”. There’s a chance that somebody who suffers some misadventure using the product based on it being hacked or some other weakness will sue you for allowing that mark to be applied indicating something which wasn’t achieved’.

PP5, Privacy Professional

One key stakeholder suggested *‘most people will assume that if you have a privacy tick equivalent then if they plonk it on their home network they will be safe’* (TS5, Technical and Security Expert). This suggests that icons could provide a false sense of security while not necessarily addressing the problems of poor or insecure CloT design or network configuration. Another key stakeholder was *‘a little bit nervous of icon schemes that put me as a consumer under more obligations to understand an icon and the degree of reliance I can place upon that icon’* (TS9, Technical and Security Expert). Perhaps the most significant barrier to the effectiveness of icons or a consumer ratings system involves the

question of ‘*how much cooperation will you get from service providers if their rating is really poor?*’ (PP4, Privacy Professional)

Survey respondents raised similar concerns that are outlined in Table 22. Among those who did *not* think privacy-related icons would be useful (n=274, 35.2%), over 40% (41.6%, n=114) reported they did not think consumers will understand the prototypes tested in this study and just under a third (28.9%, n=79) reported that consumers would not bother using the symbols when deciding to purchase a CloT device. A small number of respondents (n=26 or 9.5%) opposed the use of icons to regulate product packaging.

Table 22 Reasons why consumer icons are not considered useful

Reason	N	%
I do not think consumers will understand privacy-related symbols on products sold either in-store or online	114	41.6%
I do not think consumers will bother looking at privacy-related symbols on products sold either in-store or online	79	28.9%
I think consumers have a personal responsibility to do background research and engage with written privacy policy statements	48	17.5
I do not think product packaging should be regulated in this manner	26	9.5
Other	7	2.5

Icons and community education

The following educational flyer was developed as one method for improving consumer understanding of the risks to consider when purchasing a CloT device. In absence of clear regulatory oversight or acceptance of an icon system by industry, an educational flyer such as this may have some value in raising consumer awareness of the privacy risks of CloTs.



Figure 10 Consumer privacy educational flyer: facing side

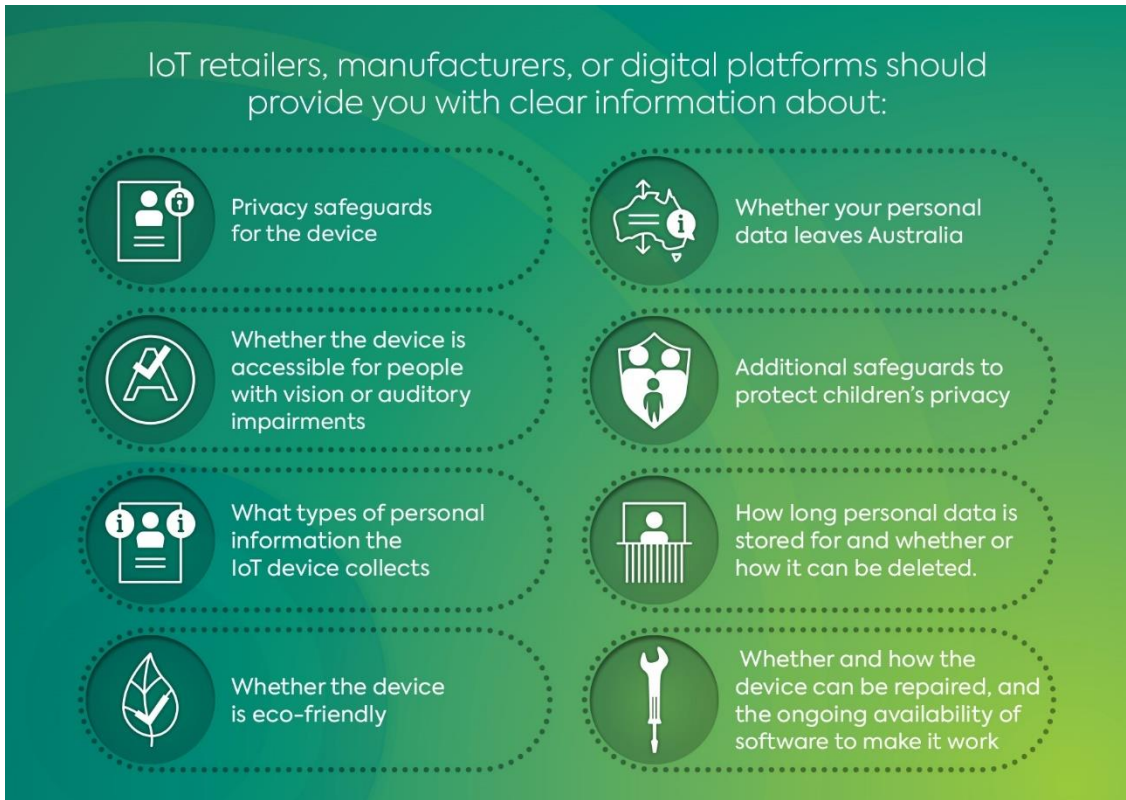


Figure 11 Consumer privacy educational flyer: rear side (8 key consumer information issues)

Conclusion

Survey findings and interviews produced mixed views about the value of icons in enhancing consumer awareness of the privacy issues relating to CloTs. While a majority of surveyed CloT consumers thought icons would be useful, it was also recognised they would not remedy many of the deficiencies that affect consumer privacy. Ultimately, the principal challenges in creating a strong and effective icon system for CloTs are (a) the lack of clear regulatory ‘back-stop’ protection for consumer privacy or safety for CloTs in Australia, (b) the lack of a clear enforcement agent to achieve this objective, and (c) an uncertain level of industry ‘buy in’ for endorsing a comprehensive icon system.

Conclusions

This research reinforces the findings of several Australian (Richardson et al, 2017; ACCC, 2020; Clifford and Paterson, 2020) and international studies (Solove, 2013, Peppet, 2014; Schaub et al, 2018; Draper and Turow, 2019) that suggest regulatory reform to privacy and consumer protection law is needed to address the various privacy, security and safety implications of CloTs. Interviews with 32 key stakeholders suggested the current regulatory regime does not provide adequate protection for Australian technology consumers. Key stakeholder interviews suggested consumers currently face several risks to their personal privacy, safety and information security due to CloTs, and this was a particular concern for specific groups, such as children. With rapid growth in the uptake of CloTs, these risks will persist and perhaps compound if not addressed by additional regulatory efforts. Several key stakeholders also expressed significant concerns about the information security standards of CloTs, and many felt CloT manufacturers were not doing enough to inform consumers about their data collection, storage and use practices. While key stakeholders raised various issues about the profound growth in use of CloTs in Australia, no clear consensus emerged about the specific regulatory solutions that are needed.

Icons were considered a potentially important method for addressing the problem of CloT manufacturers and vendors providing inadequate information to Australian consumers. Whilst survey respondents and key stakeholders viewed the idea of icons favourably, any icon system was only considered to be effective if it was integrated into a stronger regulatory environment. Icons alone may have some educational value to encourage consumer reflection on privacy concerns when making purchasing decisions. Without additional legal and enforcement reforms, they are not considered adequate to address the many regulatory issues associated with CloTs identified by key stakeholders.

The icons piloted in this project were designed around core elements of the 13 APPs. Developing icons based on these privacy principles proved challenging and raised several contradictions. Many stakeholders criticised the notice and consent model the APPs are based on for its inability to adequately protect consumers. It was also identified that an icon system presents several risks including 'warning fatigue' (ASIC/AFM, 2019, p. 3), while their purpose could be misconstrued by consumers as a statement from government or technology industries that CloT devices are privacy compliant.

Any icon system should ideally be one component of an integrated regulatory approach targeting the specific privacy and consumer protection issues associated with CloTs. Possible options include ensuring that improved methods of privacy and accessibility are incorporated into CloT design;

fostering the development and enforcement of appropriate standards through a consumer-driven product certification process, such as the UK approach to dealing with the Internet of Toys; a public certification process such as the NZ model; a mandatory labelling system, such as the Californian model; and combining any of these measures with stronger powers for industry, state or federal oversight bodies to incentivise compliance and impose graded penalties for non-compliance. This latter option will help to foster a 'smart' approach to the regulation of 'smart' technologies.

This project provides a starting point for using icons as a supplement to written descriptions of privacy policies associated with CloTs. In future, icons might be considered part of an integrated approach to legal or regulatory reform, so they alleviate the burden of privacy awareness that is currently placed on Australian consumers, while ensuring technology companies bear greater responsibility for ensuring data collection, use and storage practices are communicated clearly and transparently. Without appropriate and responsive regulatory backing, icons may serve some educational function, but are likely to have limited impact in improving consumer protection.

Perhaps the most significant findings the CPlOT data and key stakeholder interviews involved the privacy paradox. This relates to the counterintuitive concerns about privacy, which contradict consumer purchasing habits. This finding could provide some clues about why notice and consent models are not considered to protect consumers. Industry-based or mandated privacy disclosure requirements at retail outlets, or other modes of standardising and simplifying PPS in product instructions or on technology company websites, could help to protect consumers and enhance the overall appeal of CloTs. Greater insight into the paradoxical relationship between the high level of consumer concern about privacy and contradictory nature of consumer behaviour regarding CloT use will greatly assist with the refinement of the icons developed and evaluated in this study, or other variants that might emerge in the future.

Recommendations

Eight recommendations emerge from the combination of the literature review, the review of PPS, and the results of the CPlOT survey and key stakeholder interviews for this study. These are:

Recommendation 1

Prevailing sentiment amongst key stakeholders interviewed for this research strongly indicated that Australia does not currently have adequate protections for consumers for the many privacy, security and safety concerns presented by CloTs. It is recommended that additional regulatory and enforcement efforts are pursued to address these deficiencies, particularly in light of the expanding presence and penetration of CloTs into the community.

Recommendation 2

Several key stakeholders identified compelling arguments that specific groups, such as children, the elderly, and those living with a physical or intellectual disability, face specific problems with CloTs and other digital technologies. This includes the inability to directly provide their consent if other individuals are setting-up devices. It is recommended any future regulatory efforts are cognisant of, and responsive to, the privacy impacts of CloTs on specific populations where consent cannot be assured.

Recommendation 3

Several key stakeholders criticised the current model of notice and consent. This has led to long and complex ToS and PPS that are assumed to reflect an adequate level of consumer understanding and informed consent. Of our survey respondents, 47% reported they did not read PPS. It is recommended efforts are taken to simplify, enhance and reconsider the obligations and approaches to informing consumers about the privacy implications of CloTs.

Recommendation 4

Key stakeholders were often critical of the lack of transparency and clear information about CloT data collection and handling practices. In addition, 54% of survey respondents hold technology companies responsible for raising awareness of the privacy impacts of CloTs. It is recommended further pressure is placed on CloT manufacturers and vendors to be more transparent about the data collection practices associated with these technologies.

Recommendation 5

Key stakeholders provided notional support for an icon system to enhance consumer awareness of the privacy implications of CloTs, while 74% of survey respondents indicated icons would assist them to make purchasing decisions about these devices. It is recommended an icon-based system following the New Zealand or Californian model is considered in Australia, supported by adequate regulatory oversight, to address many of the current deficiencies of communicating privacy impacts of CloTs.

Recommendation 6

Many key stakeholders indicated that an icon system would need to be situated within a robust regulatory framework involving the stronger enforcement and protection of the privacy and consumer rights of Australians. It is recommended an icon-system be incorporated into a broader process of reform to current privacy and consumer protection laws, which includes enhanced enforcement and placing increased obligations on the CloT industry to participate in these processes.

Recommendation 7

The commencement of a public campaign to educate consumers about the types of data collected by CloTs relating to personal and family behaviours or habits, and how this type of information differs from conventional transactional data such as name, address and credit card details, which appear to generate the most privacy concerns.

Recommendation 8

Future research into the counterintuitive nature of privacy attitudes and behaviours, as many CPlOT respondents appear willing to sacrifice their privacy for the convenience of device functionality.

Authors

Ian Warren is a Senior Lecturer in criminology and a member of the Alfred Deakin Institute for Citizenship and Globalisation at Deakin University. Amongst several socio-legal projects, his previous research has examined privacy issues and the role of technology in policing and criminal justice administration both in Australia and comparatively.

Monique Mann is a Senior Lecturer in criminology and a member of the Alfred Deakin Institute for Citizenship and Globalisation at Deakin University. Her research expertise involves three main interrelated areas: (1) new technology for policing and surveillance, (2) human rights and social justice, and (3) governance and regulation.

Diarmaid Harkin is a Senior Lecturer in criminology and a member of the Alfred Deakin Institute for Citizenship and Globalisation at Deakin University. He has recently published a book on *Private Security and Domestic Violence: The Risks and Benefits of Private Security Companies working with Victims of Domestic Violence* (Routledge 2020) and has conducted research into technology-facilitated forms of intimate partner abuse, including the use of consumer IoT.

Appendix 1 Consumer Privacy and the Internet of Things: Survey Tool



DEAKIN
UNIVERSITY AUSTRALIA

accan



**Consumer
Policy Research
Centre**

Consumer Privacy and the Internet of Things (IoT) Survey

Section 1: Socio-Demographic Information

In this section of the survey, we are going to ask you some questions about yourself and whether you are an owner of an *internet-connected device*.

[Internet-Connected Device] – Any device that you can remotely access and control using a computing device (e.g. a smartphone, tablet, or computer) through Wi-Fi or Bluetooth. We are interested in your experience with these devices that do not include regular computers, smartphones, or tablets. For example, an internet-connected device includes a smart watch, home security system, a Wi-Fi pet feeder, or similar device.

Q1.1 What is your current age?

(Allowable responses must be restricted to 18 and over)

Q1.2 Which best describes your gender?

- Male
- Female
- Transgender, Intersex, or Non-Binary
- Prefer not to say

Q1.3 What is your postcode?

Q1.4 What is your highest level of completed education?

- Primary School
- Secondary or High School
- TAFE or Vocational Qualification
- University Undergraduate Degree
- University Postgraduate Qualification
- Other Tertiary Qualification

Q1.5 Have you purchased any of the following **internet-connected devices** during the previous 12 months? (Please select all that apply)

- | | |
|-----------------------------------|-----------------------|
| Smart Toy | <input type="radio"/> |
| Smart home assistant (e.g. Alexa) | <input type="radio"/> |
| Smart energy monitor | <input type="radio"/> |
| Home security system | <input type="radio"/> |
| Exercise equipment | <input type="radio"/> |
| Child monitoring device | <input type="radio"/> |
| Smart clock | <input type="radio"/> |
| Digital thermostat | <input type="radio"/> |
| Smoke detector | <input type="radio"/> |

- Irrigation system
- Household whitegoods
- Wi-Fi speakers
- Smart watch
- Smart batteries
- Automatic garage door
- Sleep tracker
- Heart rate monitor
- Automatic pet feeder
- Smart home lock
- Household lighting system
- Espresso machine
- Smart fridge
- Smart heater/ cooler
- Smart doorbell

If (yes) to any option, then (proceed to Q1.6)

If (none selected) then (end survey)

Q1.6 How many hours do you spend using **internet-connected devices** (not including a computer, smartphone, or tablet) on an average day?

Q1.6a How many hours do you spend using a computer, smartphone, or tablet on an average day?

Q1.7 How would you describe your level of internet and computer proficiency?

Limited proficiency	Average proficiency	High proficiency	Very high proficiency
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q1.8 Which best describes your current living situation?

- I have ownership of my primary place of residence
- I pay rent at my primary place of residence
- I do not contribute to housing costs at my primary place of residence

Q1.9 What is your annual level of personal pre-tax income?

- Less than \$15,599 p.a.
- \$15,600 - \$31,199 p.a.
- \$31,200 - \$51,999 p.a.
- \$52,000 - \$77,999 p.a.
- \$78,000 - \$103,999 p.a.
- More than \$104,000 p.a.
- Prefer not to say

Q1.10 Do you currently live with any children at your primary place of residence (as either a full or part-time carer)?

Yes (A)

No (B)

If (A) then (include Section 7) else (exclude Section 7)

Q1.11 Would you rent a house with preinstalled **internet-connected devices** that you cannot disconnect or control?

Yes

No

Why/ not?

(please specify)

Section 2: Privacy Icon Comprehension

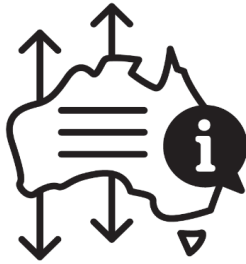
Please examine the following icons. For each icon, please indicate which of the following phrases best describe what they depict:

Q2.1



- Child Safety Controls
- Overseas Data Sharing
- Low Energy Consumption
- Ability to Use Offline
- Privacy Safeguards

Q2.2



- Child Safety Controls
- Privacy Safeguards
- Low Energy Consumption
- Ability to Use Offline
- Overseas Data Sharing

Q2.3



- Low Energy Consumption
- Overseas Data Sharing
- Privacy Safeguards
- Ability to Use Offline
- Child Safety Controls

Q2.4



- Low Energy Consumption
- Child Safety Controls
- Overseas Data Sharing
- Ability to Use Offline
- Privacy Safeguards

Q2.5



- Privacy Safeguards
- Overseas Data Sharing
- Ability to Use Offline
- Low Energy Consumption
- Child Safety Controls

Randomised order of icons/ responses

Q2.6 If any of these icons were included on product packaging at the point-of-purchase, how would you rate the likelihood they would inform your purchasing decision?

Not at all	Slightly	Somewhat	Quite a bit	Completely
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q2.7 How much individual responsibility do you think consumers have for educating themselves about the functions of **internet-connected devices**?

None	A little bit	Quite a bit	A Lot	All
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q2.8 Which organisation do you think should be responsible for making consumers aware of issues with **internet-connected devices**? (please select the most appropriate response)

- Government agencies
- Technology companies
- Retailers
- Other (please specify)

Q2.9 Do you have any feedback you would like to provide concerning the proposal to include icons on **internet-connected device** packaging?

Section 3: Privacy Literacy

In this section of the survey, we are going to ask you some questions about the internet, technology, and consumer and privacy rights in Australia.
You do not need to research your answers.

Please choose a number between 1 and 5, where **1** represents having '**no knowledge**' and **5** represents having '**complete knowledge**' of the term:

Q3.1 Please indicate how familiar you are with each of the following terms?

	1	2	3	4	5
Browser	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Server	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ISP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
HTML	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Crawler	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firewall	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Filtibly (A)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MP3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Proximity operators	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Proxypod (B)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cookies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
P3P	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Click-through	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
JFW (C)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Shareware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Torrent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Slushware (D)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagging	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PDF	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please randomise the order terms are presented.

(A, B, C, D) are nonsense terms to test respondent sincerity; (A) has no relation to other items on the scale; (C) is similar to acronyms (i.e. RSS, PDF); (B and D) share semantic similarity to other items (i.e. proxy, ware).

Predicted order of familiarity is B/D → C → A.

Please read the following statements carefully and indicate whether you believe the statements are **True** or **False**.

Q3.2 Companies have the ability to use targeted online advertisements based on your past web-browsing activities

Q3.3 A company cannot tell whether you have opened an email if you do not respond to the email

Q3.4 When you visit a website, it can only collect information about you if you register an account

Q3.5 Popular search engine sites, such as Google, track the websites you come from and go to

Q3.6 E-commerce sites, such as Amazon or Netflix, may exchange your personal information with law enforcement agencies

Q3.7 Australian privacy law places a time limit on how long websites can keep personal information they gather about you

Q3.8 Australian-based websites are legally allowed to share information about you with affiliated organisations

Q3.9 Under Australian law, telephone and internet companies are required to give you access to *any* information they collect about you

Q3.10 Australian law enforcement agencies can collect information about your online activity without your knowledge and consent

Q3.11 Australian law enforcement agencies can access data about you that is stored overseas without your knowledge and consent

Section 4: Privacy Concern

In this section of the survey, we are going to ask about your opinions concerning the collection, use, and disclosure of your **personal information** by **technology companies**.

Please indicate to what extent you **agree** or **disagree** with the following statements

[Personal Information] – This can include any data that may be used alone, or in combination with other information, to identify you. For example: your name, age, gender, place of residence, occupation, and internet-browsing history.

[Technology Company] – A company that manufactures electronic goods and/or provides services related to internet-based technology (such as apps).

Q4.1 It does not bother me when a **technology company** asks me to provide **personal information** in exchange for using their service

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4.2 I am troubled by requests to disclose **personal information** when setting up a device that connects to the internet

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4.3 It does not concerns me that my **personal information** could be stored overseas

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4.4 I believe consumers should have control over how our **personal information** is collected, used, and shared by **technology companies**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4.5 If I want to connect a device to the internet, it is reasonable to give some control over my **personal information** to a **technology company**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4.6 I think **technology companies** should be allowed to share consumer data, without obtaining their consent, to assist with product development

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4.7 It is important that I am aware of how my **personal information** is used by a **technology company**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q4.8 I believe **technology companies** should not use my **personal information** for any purpose unless I have authorised it

Strongly Disagree Disagree Neutral Agree Strongly Agree

Q4.9 I think it is unreasonable that **technology companies** are required to obtain consent from customers before sharing their personal information with another company

Strongly Disagree Disagree Neutral Agree Strongly Agree

Q4.10 I think **technology companies** should not be responsible for preventing **unauthorised access** to their customers' personal information

Strongly Disagree Disagree Neutral Agree Strongly Agree

Q4.11 I think databases containing **personal information** should be protected from **unauthorised access**, no matter the financial cost

Strongly Disagree Disagree Neutral Agree Strongly Agree

[Unauthorised Access] – When an individual or organisation without authorisation gains access to personal information.

Section 5: Privacy Attitudes

Q5.1 How favourably do you consider each of the following characteristics or functions of **internet-connected devices**?

Please choose a number between 1 and 5 for each of the following items, where **1** represents being '**not favourable**' and **5** represents being '**very favourable**':

	1	2	3	4	5
Scheduling daily tasks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Controlling your household lighting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Voice/ hands-free activation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Making daily tasks easier (such as reminders from Siri)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
The ability to connect with and operate multiple devices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Remotely controlling room temperature	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Remotely feeding pet(s)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Remotely accessing home security systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Voice-activated internet searches	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Automatic traffic notifications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Monitoring energy/ water use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					
Setting an alarm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<hr/>					

Storage of data within the cloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Increasing automation of daily life	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Growing dependence on the Internet for basic household functions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Environmental impacts of always-on devices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A need to connect devices from multiple manufacturers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ongoing device maintenance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Install regular security updates	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Relinquishing control over decision-making (e.g. whether to change temperature)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sharing of data with third-parties	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Greater interconnectedness between devices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Order of items presented in Q5.1 to be randomised.

Q5.2 How concerned are you about a **technology company** collecting and storing the following **personal information** about you?

Please indicate your responses on the below scale, where **1** represents being '**not concerned at all**' and **5** represents being '**very concerned**'

	1	2	3	4	5
Your name	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
_____ Your home address	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Your credit card details	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sleep patterns	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Personal photographs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phone conversations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data about your location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A recording of your voice	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Details about your workplace/ employer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When/ how much electricity you use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The contents of your refrigerator	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Details about your sex life	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Music and media preferences	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your internet search history	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A list of your contacts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Records of your heartrate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Details about your family relationships	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Access to documents stored in the cloud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your daily schedule	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security camera recordings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When and where your family holidays	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your medical history	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your bodily temperature	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your proximity to others, to prevent the spread of illness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Section 6: Privacy Behaviours

In this section of the survey, we are going to ask about you some questions about how you manage your **personal information**.

Among the following, please only select statements that accurately reflect how you manage your personal information.

Q6.1 I actively control the information my digital devices collect by changing privacy settings

Q6.2 I regularly clear my web browser history and/or remove cookies from my web browser

Q6.3 I use a pop-up window blocker

Q6.4 I control who can send me private messages on social media platforms

Q6.5 My computer is protected against viruses and malware

Q6.6 I have entered inaccurate personal information (e.g. my birthdate, a pseudonym) when registering for a website

Q6.7 I use a Virtual Private Network (VPN) on a computer or mobile phone

Q6.8 I turn off or disconnect computers and other **internet-connected devices** when not using them

Q6.9 I have removed a mobile phone or internet-connected device from a room to avoid a conversation being overheard

Q6.10 I strictly control what information about myself is published online

Q6.11 I avoid visiting specific websites that monitor my internet browsing

Section 7: Perceptions of Child Privacy

In this section of the survey, we are going to ask you about how you manage your child(s) personal information.

Q7.1 Before deciding to purchase an **internet-connected device**, I consider how it will impact the privacy of my child(ren)

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q7.2 I avoid posting **personal information** about my child(ren) on the Internet

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q7.3 I think children should be able to decide what information about them is published on the internet (e.g. photographs, birthdate)

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q7.4 I am concerned about **technology companies** collecting and storing **personal information** about my child(ren)

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q7.5 I think devices that connect to the internet, such as a smart watch, are useful for monitoring the safety of my child(ren)

Strongly Disagree Disagree Neutral Agree Strongly Agree

Q7.6 I believe **technology companies** should be legally compelled to delete any **personal information** they obtain about children

Strongly Disagree Disagree Neutral Agree Strongly Agree

Section 8: Privacy Policy Salience

In this section we are going to ask some questions about privacy policy statements and the **internet-connected devices** you own.

[Privacy Policy Statement] – means a statement of some or all of the ways an organisation gathers, uses, discloses, and manages a customer or client's data.

Q8.1 When deciding whether to purchase any device that connects to the internet, how much does the technology company's **privacy policy statement** impact your decision?

Not at all A little bit Somewhat A lot Completely

Q8.2 I tend to read the **privacy policy statement** when setting-up or accessing a product that requires me to disclose personal information

- True (A)
- False (B)

If (A) then (include Q8.2d) and (skip Q8.2e)

If (B) then (include Q8.2e) and (skip Q8.2d)

Q8.2a When you purchased and/or set-up an **internet-connected device** in your house, do you recall being directed to read a **privacy policy statement**?

- Yes (A)
- No (B)
- Maybe (C)

If (A or C) then (include Q8.2b and Q8.2c)

Q8.2b At what point do you initially recall being presented with the **privacy policy statement**?

- At time-of-purchase
- When I initially set-up the device
- When I registered the device online
- When I downloaded the accompanying app
- I was not notified about a privacy policy
- I do not recall being notified about a privacy policy

Q8.2c How well do you think you understood their **privacy policy statement**?

No understanding	Some understanding	Average understanding	Good understanding	Complete understanding
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q8.2d Which of the following best describes why you tend to read **privacy policy statements**?

(Please select the most appropriate option)

- I am interested to know how my **personal information** will be used by the device or service I intend to purchase
- I like to compare **privacy policy statements** when determining which **technology company's** devices and/or services to purchase
- The contents of a **privacy policy statement** will influence whether I decide to purchase that specific device and/or service

- The contents of a **privacy policy statement** will influence the accuracy of any information I disclose when registering a device and/or service

Other:
(Please specify)

Q8.2e Which of the following best describes why you tend **not** to read **privacy policy statements**?

(Please select the most appropriate option)

- They are too difficult to read
- I do not have the time to read them
- Companies will do whatever they want with my information anyway
- I do not know where to find privacy policy statements
- I just want to immediately access the product or service

Other:
(Please specify)

Q8.3 If you discovered that an **internet-connected device** you purchased was collecting and using your **personal information** in a way that makes you feel uncomfortable, what would you do? (Please select the most appropriate option)

- Continue using the device
- Stop using the device without returning it to the retailer
- Attempt to return the device to the retailer
- Write a negative review and post it on the manufacturer or retailer's website
- Write a negative review and post it to an independent consumer website
- File a report with the Privacy Commissioner
- Avoid purchasing another device from the manufacturer or retailer

Other:
(Please specify)

Q8.4 When you last purchased an **internet-connected device**, when do you initially recall being notified about the following privacy-related information?

	At Purchase	During Set-up	Registering Online	Via the App	I was not notified	I do not recall
What data they would be collecting about me	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
How long they would retain data collected about me	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
How they would use my personal information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Who they would share my personal information with	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My rights to request access to my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My rights to request the deletion of my data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

My rights to withhold personal information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Who I can contact to discuss the use of my personal information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Their duty to notify me if there is a data breach	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[Privacy-Related Icons] – These are icons that would indicate information to consumers such as: 1) what types of information a product or service collects; 2) where the device manufacturer will store and manage this information; and 3) how this information will be used by the company.

Q8.5 Do you think a standard set of **privacy-related icons** – that indicate to consumers what types of information a product or service collects, where and how it is stored, and how it is used – on a product’s packaging at the point-of-purchase (in-store or online), for example similar to an energy rating system for appliances, would assist you to make purchasing decisions about internet connected devices?

Yes (A)

No (B)

If (A) then (proceed to Q8.5a) and (skip Q8.5b)

If (B) then (proceed to Q8.5b) and (skip Q8.5a)

Q8.3a Which of the following best explains why you think **privacy-related symbols** on product packaging might be useful at the point-of-purchase for a digital device?

(Please select the most appropriate option)

I would like to be able to compare privacy-related symbols when deciding which digital device to purchase

- I think other people would obtain useful information from privacy-related symbols that would inform their purchasing decisions
- I think a standard set of privacy-related symbols would help me better understand what information is being collected and shared by a **technology company**
- I think this would be useful as current approaches to informing consumers about privacy rights are not working

Other:
(Please specify)

Q8.3b Which of the following best explains why you do **not** think **privacy-related symbols** would be useful at the point-of-purchase for a digital device?
(Please select the most appropriate option)

- I do not think consumers will bother looking at privacy-related symbols on products sold either in-store or online
- I do not think consumers will understand privacy-related symbols on products sold either in-store or online
- I think consumers have a personal responsibility to do background research and engage with written privacy policy statements
- I do not think product packaging should be regulated in this manner

Other:
(Please specify)

Appendix 2 Consumer Privacy and the Internet of Things: Interview Schedule

Section 1: Participant Experience and Expertise

Q1.1 What is your background and experience in the field of privacy, consumer protection and the Internet of Things (IoT)?

Q1.2 What is your current role and how does it inform your expertise in this area?

Q1.3 What is the role of your employing organisation/institution in the field of privacy, consumer protection and the Internet of Things?

Section 2: Internet of Things and Risk

Q2.1 How do you think IoT connected devices differ from other technologies?

Q2.2 What do you perceive to be the main technological benefits/advantages of IoT devices?

2.2.1 Can you please elaborate on these benefits?

2.2.2. Are there any other technological or social benefits you can think of for IoT devices?

Consider health applications, for example, or other forms of positive automation.

Q2.3 What do you perceive to be the main challenges/risk of IoT devices?

Q2.4 What security risks are associated with IoT devices?

Q2.4.1 Are these risks offset by the benefits of IoT?

Q2.4.2 Are these risks uniform or do specific devices carry higher or lower risks than others?

Q2.4.3 Are those risks magnified with multiple devices?

Q2.4.4. Based on your knowledge, is a security emphasis enough to offset these risks. Or, alternately, are other forms of regulation or prevention of risk necessary? Please provide insight into your answer.

Section 3: Privacy Protections

Q3.1 In your experience, what privacy issues are associated with use of IoT devices?

3.1.1. How do these issues vary from other forms of technology in your knowledge?

3.1.2 Please identify the novel issues presented by these technologies, in your view.

Q3.2 Do you believe the Australian Privacy Principles are equipped to respond to these issues? Please elaborate.

3.2.1 Is current federal or state law equipped to deal with the specific privacy issues relevant to IoTs? Please elaborate.

3.2.2. Should existing laws be modified to deal with this and other new home-based technologies? Please identify the benefits/problems of this approach.

3.2.3 Is it possible to view the Australian Privacy Principles as a method of sanctioning mass data collection? Do you think this is a fair appraisal and justified under the current operation of these requirements? Please explain your response.

Q3.3 What are the major challenges for Australian privacy law more generally?

3.3.1 How do these challenges impact consumers?

3.3.2 Is the emphasis of privacy being diluted by the overriding concern for information and online security? Please explain your response

3.3.3 What factors are central to ensuring a viable privacy system?

- a) information control
- b) access to information once it has been provided to a corporate entity;
- c) correction of information;
- d) anonymity and pseudonymity;
- e) health privacy;
- f) preserving confidentiality online;
- g) preventing sharing of information to individuals or organisations that originally did not solicit the information (whether for payment or other purposes)?
- h) any others?

3.3.4 Do Current Australian laws and the Australian Privacy Principles meet these objectives? Why or why not?

3.3.5 In contrast to a privacy regulatory structure, how might a consumer-focused regulatory approach better deal with these issues?

3.4 Do you think the current corporate uses of privacy policies, in a more general sense, are sufficient to counter privacy risk to consumers? Why/Why not?

Q3.4.1 Does the location of the corporation matter? Should it matter? Why/Why not?

Q3.4.2 Are the considerations for IoTs different compared with other online technologies?
Why/why not?

Q3.5 Do you believe that the current method of obtaining consumer consent under existing corporate privacy policies is suitable?

Q3.5.1 When do you believe consent should be sought from consumers?

Q3.5.2 How do you believe consent should be handled when devices are placed within a multi-person home?

Q3.5.3 Is consent relevant with the new generation of technologies? If not, what is a viable alternative to obtaining consent from:

- a) Device users
- b) Residents who have not set up the device;
- c) Children
- d) Guests to homes with IoT devices
- e) Renters or tenants

3.5.4 Does it matter if the device is installed voluntarily by a consumer, or is mandated by a government agency, such as with a smart meter? Should there be a distinction regarding privacy protections in either case? Please provide reasons for your answer.

Q3.6 Are there any individuals or groups in which privacy risk or concern from IoTs is more significant?

Q3.6.1 Should privacy policies be scaled for different groups?

Q3.6.2 How would you develop this scaling?

Q3.7 Are you aware of the term Privacy by Design? How would this operate in the context of IoTs? Is privacy by design likely to offset many of the difficulties identified with IoTs in this interview so far? Please explain your response.

Section 4: Consumer Protections

Q4.1 In your view, do consumer law protections adequately respond to the risks of IoT you have identified?

Q4.2 In your view, do consumer law protections provide adequate support to consumers of IoT devices?

Q4.3 Do you think that altering the timing of privacy notification may offer an additional benefit to consumers to make informed decisions about purchasing IoT devices? Why/Why not?

Q4.4 Are there any other jurisdictions you believe to be making significant strides to protect consumers?

Q4.5 How can consumer protection approaches to IoT offset the limits of other regulatory methods, such as privacy law?

Q4.6 Do you believe a market regulating mechanism is enough to protect and better inform consumers or do you believe a proactive state intervention is required?

Q4.6.1 If improved state or private regulation is required, how will this operate in practice?

Q4.7. It appears the ACCC is playing a very proactive role in advocating privacy law reform in Australia. What benefits or problems emerge from this development?

Q4.8. What is the optimum form of privacy regulation in Australia? Explain how this might work. Explain how this might work in relation to promoting greater privacy awareness for IoTs specifically.

Section 5: Privacy Icons

Preamble: as part of this project we think one way to enhance consumer protection is through the use of icons which will be used to represent various privacy risks associated with IoT devices. This approach is advocated by ACCC in its Platforms Inquiry, and across the European Union under the General Data Protection Regulation. and is one form of simplifying privacy and safety notification. We have developed these icons and would like your feedback

Q5.1 What do you believe to be the strengths of the use of icons?

Q5.2 What are the weaknesses of this approach?

Q5.3 What barriers do you foresee to the roll out and implementation of an icon-based warning or privacy notification system?

Q5.4 How do you think we could overcome these barriers?

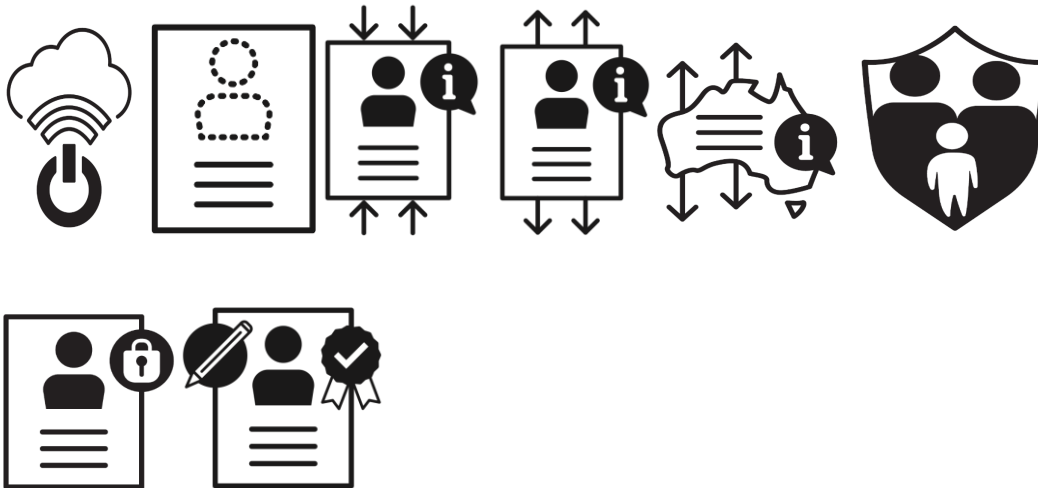
Q5.5 Are there any other mechanisms which you believe would be a viable alternative to better protect and inform consumers?

Q5.6 Do you believe this system places too much reliance on consumer consent?

Q5.6.1 What are the benefits of this?

Q5.6.2 What are the risks of this?

Q5.7 Please examine the following icons and explain, for each, what you believe they are trying to depict.



Q 5.8 Open discussion of our designed icons

5.8.1 Does the colour of the icon matter?

5.8.2 What types of narrative would be required to make these icons more descriptive?

5.8.3 Is it sufficient to contain privacy policies inside the box, or online when you register a device, or would any of these icons (or variants) on the box at the point of sale be sufficient?

5.8.4 Should these be accompanied with instructions at the point of selling IoT devices, or with leaflets, or on the box?

Q5.9 Are there other conceptions of privacy that might be as or more effective than icons?

Q5.10 Should icons be used to reflect the Australian Privacy Principles or should they encompass new developments that meet the challenges of IoTs and other emerging technologies?

Q5.11 Which organisations should be responsible for making consumers aware of privacy issues via icons:

- a) State government agencies
- b) Federal government agencies
- c) Private industry (IoT manufacturers)
- d) Retailers
- e) App developers or distributors
- f) Other

Please provide reasons for your preference

Q5.12 In light of the problems you have identified with icons, what other developments would be needed to improve consumer awareness of privacy issues relating to IoTs? How would these additional developments operate in practice?

Section 6: Additional issues

Q6.1 We recognise that icons cannot explain all of the consumer risks when engaging with IoT devices. What else do you believe is needed alongside the icons to better improve the regulation of IoT under consumer protection or privacy approaches?

Q6.2 What other regulatory responses would you like to see?

Section 7: Conclusion

7.1 A large part of this research is about raising consumer awareness of information privacy. Do you have anything to add that might assist in this process?

7.2 Are specific requirements needed for IoTs and privacy regulation?

7.3 Do you have any additional things to add in relation to IoTs, privacy and consumer protection?

Thank you for your participation in this interview.

References

Albuquerque, O. de P., Fantinato, M., Kelner, J., & de Albuquerque, A.P. 2020, 'Privacy in smart toys: Risks and proposed solutions', *Electronic Commerce Research and Applications*, vol. 39, 100922. <https://doi.org/10.1016/j.elerap.2019.100922>

Andrejevic, M. & Burdon, M. 2015, 'Defining the Sensor Society', *Television and New Media*, vol. 16, no. 1, pp. 19-36.

Australian Competition and Consumer Commission (ACCC). 2020, *Digital Platform Services Inquiry 2020-2025 (including Interim Reports)*. Available at <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025>

Australian Competition and Consumer Commission (ACCC). 2019, *Digital Platforms Inquiry: Final Report*, June. Government of Australia, Canberra.

Australian Council of Learned Academies (ACOLA). 2020. *The Internet of Things: Horizon Scanning*, November, ACOLA, Melbourne. Available at <https://acola.org/hs5-internet-of-things-australia/> Accessed 1 Dec 2020.

Australian Government, 2020. *Code of Practice: Securing the Internet of Things for Consumers*, Commonwealth of Australia, Canberra. Available at <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>

Australian Government, e-Safety Commissioner. 2019, *Safety by Design*, May. Australian Government, Canberra. Available at <https://www.esafety.gov.au/sites/default/files/2019-10/LOG%207%20-Document8b.pdf>

Australian Human Rights Commission. 2021, *Human Rights and Technology (Final Report)*, AHRC, Sydney. Available at https://tech.humanrights.gov.au/downloads?_ga=2.18219770.2142736840.1622682501-1389152922.1620718400

Australian Institute of Health and Welfare (AIHW). 2020, *People with Disability in Australia*, AIHW, Canberra. Available at <https://www.aihw.gov.au/reports/disability/people-with-disability-in-australia/contents/people-with-disability/prevalence-of-disability>

Australian Law Reform Commission. 2014, *Serious Invasions of Privacy in the Digital Era*, Report 123, Australian Law Reform Commission, Canberra. Available at Australian Law Reform Commission: <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/>

Australian Communications and Media Authority (ACMA). 2020, *Internet of Things in Media and Communications*. Occasional Paper, July, ACMA, Melbourne. Available at <https://www.acma.gov.au/publications/2020-08/report/internet-things-media-and-communications-occasional-paper>

Australian Securities and Investments Commission and the Dutch Authority for the Financial Markets (ASIC/AFM). 2019, *Disclosure: Why It Shouldn't be the Default*, Report 632, October 14. Available at

<https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default//>

Belli, L. & Venturini, J. 2016, 'Private Ordering and the Rise of Terms of Service in Cyber-Regulation', *Internet Policy Review*, vol 5, no. 4). Available at: <https://policyreview.info/articles/analysis/private-ordering-and-rise-terms-service-cyber-regulation>

Braithwaite, J. 2017, 'Types of responsiveness', in P. Drahos (ed.) *Regulatory theory: Foundations and applications*, pp. 117-132. ANU Press, ACT.

Brass, I., Tanczer, L., Carr, M. & Blackstock, J. 2017, *Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things?* LSE. Available at: <http://www.lse.ac.uk/accounting/assets/CARR/documents/R-R/2017-Summer/riskandregulation-33-regulating-iot.pdf>

Burns, J. & Hood, M. 2017, *Transparency and Trust: A guide to data protection and privacy for landlords and tenants*, Housemark/Anthony Collins Solicitors and Amicus Horizon, UK. Available at https://www.anthonycollins.com/media/2323/dataprotection_report_v7.pdf.

Bygrave, L.A. 2015, *Internet Governance by Contract*, Oxford University Press, Oxford, UK.

Caron, X., Bousa, R., Maynard, S.B. & Ahmad, A. 2016, 'The Internet of Things and its Impact on Individual Privacy: An Australian Perspective', *Computer Law and Security Review*, vol. 32, no. 1, p. 4015.

Carter, J.W. & L. Chan. 2019, *Contract and the Australian Consumer Law*, The Federation Press, Annandale, NSW.

Childon, A.S. & Ben-Shahar, O. 2016, *Simplification of Privacy Disclosures: An Experimental Test*, Coase-Sandor Working Paper Series in Law and Economics, no. 737. Available at: <https://www.journals.uchicago.edu/doi/pdfplus/10.1086/688405>

Clapperton, D. & Sorones, S. 2007, 'Unfair Terms in "Clickwrap" and other Electronic Contracts', *Australian Business Law Review*, vol. 35, pp. 152-180.

Clifford, D. & Paterson, J. 2020, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law', *Australian Law Journal*, vol. 94, no. 10, pp. 741-751.

Cohen, J.E. 2017, 'Surveillance versus Privacy: Effects and Implications', in D. Gray and S. E. Henderson (eds) *The Cambridge Handbook of Surveillance Law*, pp. 1049-1081, Cambridge University Press, Cambridge, NY.

Consumers International. 2019, *Consumer IoT. Trust By Design 2019: Guidelines and Checklists*. Consumers International, February. Available at: <https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf>

Council of the European Union, 2021, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic

- Communications)', 10 February. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN
- Cranor, L. F. 2021, 'Informing California Privacy Regulations with Evidence from Research', *Communications of the ACM*, vol. 63, no. 3, pp. 29-32. Available at <https://cacm.acm.org/magazines/2021/3/250700-informing-california-privacy-regulations-with-evidence-from-research/fulltext>
- Cranor, L.F. 2012, 'Necessary but not Sufficient: Standardised Mechanisms for Privacy Notice and Choice', *Journal on Telecommunications and High Technology Law*, vol. 10, no. 2, pp. 273-307.
- Department for Digital Culture, Media and Sport, UK. (DCMS) 2018, *Code of Practice For Consumer IoT Security*. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
- Department for Digital Culture, Media and Sport, UK. (DCMS) 2019a, *Consultation on Regulatory Proposals on Consumer IoT Security*. Available at: <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>
- Department for Digital Culture, Media and Sport, UK. (DCMS). 2019b, *IoT Labelling Online Study*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798547/Make_it_Clear_Labelling_Online_Study_Report.pdf
- Dragiewicz M., Harris B., Woodlock D., Salter M., Easton H., Lynch A., Campbell H., Leach J., & Milne N. 2019. *Domestic Violence and Communication Technology: Survivor experiences of intrusion, surveillance, and identity crime*. Australian Communications Consumer Action Network (ACCAN), Sydney. Available at: <https://accan.org.au/grants/grants-projects/1429-domestic-violence-and-communication-technology-victim-experiences-of-intrusion-surveillance-and-identity-theft>
- Draper, N.A. & Turow, J. 2019, 'The Corporate Cultivation of Digital Resignation', *new media and society*, vol. 21, no. 8, pp. 1824-1839.
- Electronic Privacy Information Centre. 2018, 'Evaluation of the Toy Safety Directive (2009/48/EC)', December. EPIC. Available at: <https://epic.org/comments/EPIC-Comments-EU-Toy-Safety-Directive.pdf>
- Emami-Naeni, P., Bhagavatula, S., Agarwal, U., & Cranor, L.F. 2019, 'Exploring How Privacy and Security Factor Into IoT Device Purchase Behaviour', CHI, 4-9 May, paper 534. Available at: <https://www.cs.cmu.edu/~pemamina/publication/CHI'19/>
- European Union Agency for Network and Information Security (ENISA) 2018a, 'IoT Security Standards Gap Analysis: Mapping of Existing Standards against Requirements on Security and Privacy in the Area of IoT. V 1.0', December. ENISA. Available at: <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>

European Union Agency for Network and Information Security (ENISA) 2018b, 'Good Practices for Security of Internet of Things in the context of Smart Manufacturing', November. ENISA. Available at: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>

European Union Agency for Network and Information Security (ENISA) 2018c, 'Towards a Secure Convergence of Cloud and IoT', September. ENISA. Available at: <https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot>

Fairfield, J.A.T. 2017, *Owned: Property, Privacy and the New Digital Serfdom*. Cambridge University Press. Cambridge, UK.

Federal Trade Commission, 2015, 'Internet of Things: Privacy and Security in a Connected World', FTC Staff Report, January. Available at: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

Forbrukerrådet. 2016, #Toyfail: *An analysis of consumer and privacy issues in three internet-connected toys*, December. Forbrukerrådet, Norway. Available at: <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf>

Forbrukerrådet. 2017, #WatchOut: *Analysis of Smartwatches for Children*, October. Forbrukerrådet, Norway. Available at: <http://www.conpolicy.de/en/news-detail/watchout-analysis-of-smartwatches-for-children/>

Friedman, B. & Nissenbaum, H. 1996, 'Bias in computer systems', *ACM Transactions on Information Systems*, vol. 14, no. 3, pp. 330-347.

Genaro Motti, V & Caine, K. 2016, 'Towards a Visual Vocabulary for Privacy Concepts', Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Available at: <https://doi.org/10.1177/1541931213601249>

Gilmore, J. N. 2017, 'From Ticks and Tocks to Budes and Nudges: The Smartwatch and the Haptics of Informatic Culture', *Television and New Media*, vol. 18, no. 3, pp. 189-202.

Greengard, S. 2015, *The Internet of Things*, The MIT Press, Cambridge, MA.

Gunningham, N. & Sinclair, D. 2017, 'Smart regulation'. In Drahos, P. (ed.) *Regulatory Theory: Foundations and Applications*, pp. 133-148, ANU Press, ACT.

Haber, E. 2020, 'The internet of children: Protecting children's privacy in a hyper-connected world', *University of Illinois Law Review*, vol. 4, pp. 1209-1248.

Harris Interactive 2019, 'Consumer Internet of Things Security Labelling Survey Research Findings'. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.pdf

Hildebrandt, M. 2015, *Smart Technologies and the End(s) of Law*. Edward Elgar, Cheltenham UK.

Hildebrandt, M. & Koops, B.-J. 2010, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era', *The Modern Law Review*, vol. 73, no. 3, pp. 428-460.

Holloway, D. 2019, 'Surveillance capitalism and children's data: The Internet of toys and things for children', *Media International Australia*, vol. 170, no. 1, pp. 27-36.

<https://doi.org/10.1177/1329878X19828205>

Holtz, L.-E., Nocun, K. & Hansen. 2011, 'Towards Displaying Privacy Information with Icons', in S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes & G. Zhang (eds) *Privacy and Identity Management for Life: Privacy and Identity 2010* (IFIP Advances in Information and Communication Technology), pp. 338-348, Springer, Berlin.

Holtz, L.-E., Zwingelberg, H. & Hansen, M. 2011, 'Privacy Policy Icons', in J. Camenisch, S. Fischer-Hübner & K. Rannenber (eds) *Privacy and Identity Management for Life*, pp. 279-285, Springer, Berlin.

IoT Alliance Australia (IoTAA). 2017, 'Internet of Things Security Guidelines. Vers 1.0', February. Available at: <http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.0.pdf>

Internet of Toys Certification Scheme (UK), at https://iotoys.org.uk/about_us

IoT Security Foundation (IoTSF). 2018, *IoT Cybersecurity: Regulation Ready: A Landscape Report - Concise Version*. IoT Security Foundation. Available at: <https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Cybersecurity-Regulation-Ready-White-Paper-Concise-Version.pdf>

Kennedy, H., Elgesem, D. & Miguel. C. 2017, 'On Fairness: User Perspectives on Social Media Data Mining', *Convergence: The International Journal of Research into New Media Technologies*, vol. 23, no. 3, pp. 270-288.

Kim, N.S. 2019, *Consentability: Consent and its Limits*, Cambridge University Press, Cambridge UK.

Koops, B. 2014, 'The trouble with European data protection law', *International Data Privacy Law*, vol. 4, no. 4, pp. 250-261.

Koops, B. Newell, B. Timan, T. Skorvanek, I. Chokrevski, T & Galic, M. 2017, 'A Typology of Privacy', *University of Pennsylvania Journal of International Law*, vol. 38, no. 2, pp. 483-576.

Kryla-Cudna, K. 2018, 'Consumer Contracts and the Internet of Things', in V. Mak, E. Tjong Tjin Tai & A. Berlee (eds) *Research Handbook in Data Science and Law*, pp. 83-107, Edward Elgar, Cheltenham, UK.

Leese, M. 2014, 'The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union', *Security Dialogue*, vol. 45, no. 5, pp. 494-511.

Leszczynski, A. 2015, 'Spatial Big Data and Anxieties of Control', *Environment and Planning D: Society and Space*, vol. 33, no. 6, pp. 965-984.

Levi-Faur, D. 2011a, 'Regulation and Regulatory Governance', in D. Levi-Faur (ed.) *Handbook on the Politics of Regulation*, pp. 3-21, Edward Elgar, Cheltenham, UK.

Levi-Faur, D. 2011b, 'The regulatory state and regulatory capitalism: An institutional perspective', in D. Levi-Faur (ed.) *Handbook on the Politics of Regulation*, pp. 662-671, Edward Elgar, Cheltenham, UK.

Lloyds. 2018, *Networked World: Risks and Opportunities in the Internet of Things: Emerging Risk Report, 2018, Technology*. Lloyds, London. Available at <https://www.lloyds.com/~media/files/news-and-insight/risk-insight/2018/internet-of-things/interconnectedworld2018-final.pdf>

Logsdon Smith, A. 2018, 'Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy through Voice-Captured Personal Data', *The Catholic University Journal of Law and Technology*, vol. 27, no. 1, pp. 187-226.

Loi, M. & Christen, M. 2019, 'Two Concepts of Group Privacy', *Philosophy and Technology*, vol. 33, no. 2, pp.207–224. <https://doi.org/10.1007/s13347-019-00351-0>

Lupton, D. 2016, *The Quantified Self: A Sociology of Self-Tracking*, Polity Press, Cambridge, UK.

Mahmoud, M., Hossen, M. Z., Barakat, H., Mannan, M. & Youssef. A. 2017, 'Towards a Comprehensive Analytical Framework for Smart Toy Privacy Practices', Proceedings for the STAST2017 (Association for Computing Machinery) Conference, 5 December, 2017, Orlando FL, USA. Available at: <https://doi.org/10.1145/3167996.3168002>

Malaysian Communications and Multimedia Commission. 2018, *Regulatory Challenges of the Internet of Things*, White Paper. MCMC. Available at: [https://www.skmm.gov.my/skmmgovmy/media/General/pdf/WHITE-PAPER-REGULATORY-CHALLENGES-OF-INTERNET-OF-THINGS-\(IOT\).pdf](https://www.skmm.gov.my/skmmgovmy/media/General/pdf/WHITE-PAPER-REGULATORY-CHALLENGES-OF-INTERNET-OF-THINGS-(IOT).pdf)

Mann, M. & Matzner, T. 2019, 'Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination', *Big Data and Society*, vol. 6, no. 2, <https://doi.org/10.1177/2053951719895805>

Manwaring, K. 2018, 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation', *Competition and Consumer Law Journal*, vol. 28, pp. 141-181.

Manwaring, K. 2017a, 'Six things every consumer should know about the 'Internet of Things'', *The Conversation*, 8 June. Available at: <https://theconversation.com/six-things-every-consumer-should-know-about-the-internet-of-things-78765>

Manwaring, K. 2017b, 'Emerging Information Technologies: Challenges for Consumers', *Oxford University Commonwealth Law Journal*, vol. 17, no. 2, pp. 265-289.

Manwaring, K. & Clarke, R. 2021, 'Is Your Television Spying on You? The Internet of Things Needs More than Self-Regulation', *Australian and New Zealand Computer Law Journal*, vol. 93, pp. 31-36.

Manwaring, K. & Clarke, R. 2015, 'Surfing the Third Wave of Computing: A Framework for Research into eObjects', *Computer Law and Security Review*, vol. 31, no. 5, pp. 586-603.

Mascheroni, G. 2018, 'Researching datafied children as data citizens', *Journal of Children and Media*, vol. 12, no. 4, pp. 517-523.

McMahon, K. 2018, 'Tell the Smart House to Mind its Own Business: Maintaining Privacy and Security in the Era of Smart Devices', *Fordham Law Review*, vol. 86, no. 5, pp. 2511-2551.

McRae, L., Ellis, K. & Kent, M. 2018, 'Internet of Things: Education and Technology: The Relationship between Education and Technology for Students With Disabilities', February. Curtin University. Available at: https://www.ncsehe.edu.au/wp-content/uploads/2018/02/IoTEducation_Formatted_Accessible.pdf

Nissenbaum, H. 2010, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press. Stanford, California.

Noble, S.U. 2018, *Algorithms of oppression: How search engines reinforce racism*, NYU Press, New York.

Noto La Diega, G. & Walden, I. 2016, 'Contracting for the 'Internet of Things': Looking into the Nest', *European Journal of Law and Technology*, vol. 7, no. 2. Available at: <http://ejlt.org/article/view/450>

Obar J.A. & Oeldorf-Hirsch, A. 2018, 'The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media', *Social Media + Society*, vol. 4, no. 3, DOI: 10.1177%2F2056305118784770.

OECD. 2021, *Children in the Digital Environment: Revised Typology of Risks* (OECD Digital Economy Papers, no. 302). January. OECD Publishing, Paris. Available at: <https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1611534962&id=id&accname=guest&checksum=3955B01BE910F037E214291C0B3B012A> Accessed 25 Jan 2021.

OECD. 2018, *Consumer Policy and the Smart Home* (OECD Digital Economy Papers, no. 268). April. OECD Publishing, Paris. Available at: https://www.oecd-ilibrary.org/science-and-technology/consumer-policy-and-the-smart-home_e124c34a-en Accessed 19 Jan 2021.

Office of the Australian Information Commissioner (OAIC). 2021, 'OAIC welcomes additional funding for data protection and FOI', 12 May. Available at <https://www.oaic.gov.au/updates/news-and-media/oaic-welcomes-additional-funding-for-data-protection-and-foi/>

Office of the Australian Information Commissioner (OAIC). 2020, *Privacy Act Review - Issues Paper: Submission by the Office of the Australian Information Commissioner*, 11 December, OAIC. Available at <https://www.oaic.gov.au/assets/engage-with-us/submissions/Privacy-Act-Review-Issues-Paper-submission.pdf>

Office of the Australian Information Commissioner (OAIC). 2017, 'What is Personal Information?' OAIC. Available at: <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/#ftnref8>.

Office of the Australian Information Commissioner (OAIC). 2014, *The Australian Privacy Principles: From Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012*. OAIC. Available at: <https://www.oaic.gov.au/assets/privacy/australian-privacy-principles/the-australian-privacy-principles.pdf>

Office of the Victorian Information Commissioner. 2021, 'Internet of Things and Privacy - Issues and Challenges', OVIC, Melbourne. Available at <https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/>

O'Neil, C. 2016, *Weapons of math destruction: How big data increases inequality and threatens democracy*, Penguin, Random House, London, UK.

Parker, C. 2013, 'Twenty years of responsive regulation: An appreciation and appraisal', *Regulation and Governance*, vol. 7, no. 1, pp. 2-13.

Peppet, S.R. 2014, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent', *Texas Law Review*, vol. 93, no. 1, pp. 85-178.

Perzanowski, A. & Schultz, J. 2016, *The End of Ownership: Personal Property in the Digital Economy*, MIT Press, Cambridge, MA.

Posadas, D.V. Jr. 2017, 'After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy', *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 28, no. 1, pp. 69-108.

The Privacy Act (Commonwealth) 1988. Office of the Information Commissioner. Available at: <https://www.oaic.gov.au/privacy/the-privacy-act/>

Quirk, P. & Rothchild, J.A. 2010, 'Consumer Protection and the Internet', in G. Howells, I. Ramsay, T. Wilhelmsson and D. Kraft (eds) *Handbook of Research on International Consumer Law*, pp. 333-365, Edward Elgar, Cheltenham, UK.

Radin, M.J. 2013, *Boilerplate: Fine Print, Vanishing Rights and the Rule of Law*, Princeton University Press, Princeton, NJ.

Richardson, M., Bousa, R., Clark, K., Webb, J., Ahmad, A. & Maynard, S. 2017, 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives', *Internet Policy Review*, 6(1), <https://doi.org/10.14763/2017.1.455>. Available at <https://policyreview.info/articles/analysis/towards-responsive-regulation-internet-things-australian-perspectives>

Rosner, G. & Kenneally, E. 2018, *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*, White Paper. Centre for Long Term Cybersecurity. University of California, Berkeley. Available at: https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf

Rossi, A. & Palmirani, M. 2019, 'DaPIS: a Data Protection Icon Set to Improve Information Transparency under the GDPR', Jan 21. Available at: http://gdprbydesign.cirsfid.unibo.it/wp-content/uploads/2019/01/report_DaPIS_jan19.pdf

Sadowski, J. 2020, *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World*, MIT Press, Cambridge, MA.

Sandvig, C. Hamilton, K. Karahalios, K. & Langbort, C. 2016, 'When the algorithm itself is a racist: Diagnosing ethical harm in the basic components of software', *International Journal of Communication*, vol. 10, pp. 4972-4990.

Schaub, F., Balebako, R., Durity, A.L. & Cranor, L.F. 2018, 'A Design Space for Effective Privacy Notices', in E. Selinger, J. Polonetsky & O. Tene. (eds) *The Cambridge Handbook of Consumer Privacy*, pp. 669-721, Cambridge University Press, Cambridge, UK.

Sivaraman, V., Gharakheili, H.H. & Fernandes, C. 2017, *Inside Job: Security and Privacy Threats for Smart Home IoT Devices*. ACCAN, Sydney, NSW. Available at: <https://accan.org.au/grants/completed-grants/1442-inside-job>

Solove, D.J. 2013, 'Introduction: Privacy Self-Management and the Consent Dilemma', *Harvard Law Review*, vol. 126, no. 5, pp. 1880-1903.

Stoliova, M., Livingstone, S. & Nandagiri, R. 2020, 'Digital by default: Children's capacity to understand and manage online data and privacy', *Media and Communication*, vol. 8, no. 4, pp. 197-207. DOI: 10.17645/mac.v8i4.3407.

Stoliova, M., Nandagiri, R. & Livingstone, S. 2019, 'Children's understanding of personal data and privacy online – a systematic evidence mapping', *Information, Communication & Society*, Online First: 17 Sept. DOI: 10/1080/1369118X.2019.1657164.

Things/Mozilla Open IoT Studio. 2017, *A Trustmark for IoT: Building consumer trust in the Internet of Things by empowering users to make smarter choices*. Things.com. Available at: <https://thingscon.org/report-a-trustmark-for-iot/>

Tonkin, C. 2019, 'Government to Tackle IoT Security: Introduces a Draft Voluntary Code of Practice', *ACS Information Age*. Available at <https://ia.acs.org.au/article/2019/government-to-tackle-iot-security.html>

Tusikov, N. 2019, 'Regulation through 'Bricking': Private Ordering in the 'Internet of Things'', *Internet Policy Review*, vol. 8, no. 2, <https://doi.org/10.14763/2019.2.1405> . Available at <https://policyreview.info/articles/analysis/regulation-through-bricking-private-ordering-internet-things>

van der Hof, S. 2017, "'I agree ... or do I?' – A rights based analysis of the law on children's consent in the digital world', *Wisconsin International Law Journal*, vol. 34, no. 2, 410-445.

Wachter, S. & Mittelstadt, B. 2019, 'A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI', *Columbia Business Law Review*, vol. 2, pp. 1-130.

Weber, R.H. 2015, 'Internet of Things: Privacy Issues Revisited', *Computer Law and Security Review*, vol. 31, no. 5, pp. 618-627.

Williams, M., Nurse, J.R.C. & Creese, S. 2017, "'Privacy is the Boring Bit": User Perceptions and Behaviour in the Internet of Things', Available at <https://arxiv.org/abs/1807.05761>

Zomet, A. and Urbach, S.R. 2016 'United States Patent Application Publication: Privacy-Aware Personalised Content for the Smart Home', Filed 4 March 2015, Published 8 Sept. Available at <https://patentimages.storage.googleapis.com/a4/2d/3b/f4c35feb228ded/US20160260135A1.pdf>

Zuboff, S. 2019, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, London, UK.



Enhancing Consumer Awareness of Privacy and the Internet of Things