Regulation of Internet of Things Devices to Protect Consumers

UTS

accan

Regulation of Internet of Things Devices to Protect Consumers

David Lindsay
Genevieve Wilkinson
Evana Wright

June 2022

Regulation of Internet of Things Devices to Protect Consumers

Authored by **David Lindsay, Genevieve Wilkinson and Evana Wright**

Published in **2022**

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.

University of Technology Sydney
Website: www.uts.edu.au
Email: david.lindsay@uts.edu.au
Telephone: 02 9514 3761

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: **978-1-921974-74-8**
Cover image: **Design by Nathaniel Morrison with images from Shutterstock**

This work can be cited as: Lindsay, D., Wilkinson, G. & Wright, E. 2022, *Regulation of Internet of Things Devices to Protect Consumers*, Australian Communications Consumer Action Network, Sydney.

Table of Contents

Figures and Tables

Figures

Tables

Acknowledgements

We would like to acknowledge the invaluable assistance and guidance of the following people:

Henry Fraser, Neva Collings, Fiona Tito Wheatland and Olivia Rawlings-Way for their excellent research assistance. In particular, Henry provided invaluable assistance with the section on cyber security, Neva with the section on security labelling and Fiona with the section on consumer protection and the Report summary. Olivia assisted with editing and all matters relating to the production of the final report. Louise Buckingham provided research assistance for preparatory work for the project.

Kris Wilson, an Adjunct Fellow at UTS:Law, who contributed to the early stages of the project.

The following academics and experts, for providing important guidance and insights on aspects of the Report: Mike Briers, Malcolm Crompton, Hassan Gharakheili, Graham Greenleaf, Peter Leonard, Justin Lipman, Monique Mann, Kayleen Manwaring, Jeannie Paterson, Holly Raiche, Megan Richardson, Ian Warren and Frank Zeichner. We are fortunate to have such generous and knowledgeable colleagues.

Members of the Technology and Intellectual Property Research Cluster at UTS, for providing a stimulating and supportive research environment.

Lesley Hitchens and Anita Stuhmcke, successive Deans of Law at UTS, for supporting the project.

Nikki Lengkeek and Shital Kotecha, for assistance in administering the grant.

All of the key stakeholders who contributed their valuable time and expertise.

We are especially grateful to Tanya Karliychuck, Wayne Hawkins, Catherine Wyburn and Andrew Williams from ACCAN, for constant guidance, support and encouragement. We hope that this Report, and the other project outcomes, justify your faith in the project.

Aspects of this Report were presented to the symposium *(Legal) Challenges of the Cyber Physical World,* organised by Kayleen Manwaring at the UNSW Allens Hub for Technology, Law & Innovation, on 25 March 2022. We are grateful for feedback from attendees at the symposium.

Needless to say, the authors of the Report are responsible for its contents, including any errors or inaccuracies. To the extent possible, the law is stated as at 30 April 2022.

Recommendations

Recommendation 1

Legislation should be introduced to regulate the security of Consumer Internet of Things (CIoT) devices. The legislation should impose mandatory minimum obligations on relevant entities, namely: manufacturers, importers and distributors of CIoT devices.

Recommendation 2

Australia should not mandate adoption of ETSI EN 303 645 but should build on the security principles in the current Code of Practice.

Recommendation 3

Legislation imposing security standards should adopt a staged approach by, in the first instance, mandating the most important standards. Consideration should be given, in the first instance, to mandating the five 'must haves' identified by the World Economic Forum (WEF), namely: no universal default passwords, implementing a vulnerability disclosure policy, keeping software updated, securely communicating and ensuring that personal data is secure.

Recommendation 4

Legislation setting minimum security standards should, in general, follow the model adopted by the UK Product Security and Telecommunications Infrastructure Bill 2021 by imposing duties on manufacturers, importers and distributors relating to compliance with minimum standards, statements of compliance and compliance failures.

Recommendation 5

Legislation imposing security standards should adopt a flexible tiered system of enforcement, potentially incorporating compliance notices, stop notices and recall notices.

Recommendation 6

Consideration should be given to establishing a role for the newly established Cyber and Infrastructure Security Centre (CISC) in regulating the security of CIoT devices.

Recommendation 7

If legislation imposing mandatory standards on CIoT devices is introduced, consideration should be given to how it relates to the broader cyber security regulatory framework, including the regulatory regime applying to critical infrastructure assets. Ideally, cyber security regulation should be extended beyond critical infrastructure to apply across industry sectors. While the regulation of CIoT devices presents distinct policy issues, it should be harmonised with economy-wide efforts aimed at improving incentives to enhance cyber security.

Recommendation 8

Over time, a mandatory security labelling scheme should be introduced as part of a comprehensive CIoT security regulatory regime. The labelling scheme must be properly resourced to ensure satisfactory testing, certification and enforcement. The scheme should be consistent, to the extent possible, with other relevant national labelling schemes.

Recommendation 9

Prior to the introduction of a mandatory labelling scheme, a voluntary scheme with government backing, similar to Singapore's Cybersecurity Labelling Scheme (CLS), should be introduced and properly resourced. The Australian Government's role in supporting the scheme should extend to accrediting certification bodies and enforcement. The scheme should incorporate arrangements for certification by independent third parties and should not be based on self-certification.

Recommendation 10

In conjunction with the introduction of a labelling scheme, government should fund a public education campaign to increase consumer awareness of both the scheme and security issues relating to CIoT devices.

Recommendation 11

The Australian Consumer Law (ACL) should be amended to introduce a prohibition on suppliers and manufacturers failing to provide a remedy to consumers when legally obliged to do so under the consumer guarantees, which in the event of a major failure, would be enforced by the Australian Competition and Consumer Commission (ACCC) issuing a civil penalty notice, and a civil penalty or injunction issued by a court. Consideration should be given to providing consumers with the ability to initiate actions to enforce the prohibition.

Recommendation 12

Further consideration should be given to how enforcement of the consumer guarantees could be improved by the introduction of alternative dispute resolution schemes, such as ombudsman schemes.

Recommendation 13

A new sui generis category for digital products, distinct from 'goods' and 'services', should be introduced to the ACL. The new category should include both digital content and CIoT devices. A new category is justified because digital products are sufficiently different from traditional consumer products to merit new, specifically tailored consumer guarantees. A new category would also reduce current uncertainties in determining whether elements of a CIoT device are 'goods' or 'services'. In introducing a new legislative category, care is needed in defining the category, especially in determining when elements of a complex product are sufficiently integrated so as to form part of that product.

Recommendation 14

In association with the introduction of a new category of digital products, a set of consumer obligations should be developed for these products. The obligations should at least include the following: any software elements, including security software, should be up to date and regularly updated; the devices should be reasonably secure from intrusions; and the elements of a hybrid device – including software, hardware, data and associated services – should be properly integrated.

Recommendation 15

Suppliers of digital products, including CIoT devices, should be required to ensure that clear explanations of prescribed contractual terms, including warranties, are made available to consumers before purchase. Full contractual terms and conditions should also be publicly available on supplier websites. The conditions for complying with these obligations should be specified in regulations.

Recommendation 16

Additional measures should be investigated for improving access to and understandability of terms and conditions for CIoT devices. Such measures could include tools to assist in locating consumer contracts that, under Recommendation 15, would be legally required to be disclosed before purchase. In addition, measures should be investigated to assist consumers in identifying and interpreting key contractual terms, including terms in complex, interconnected contracts for CIoT devices and market comparisons between supplier terms and conditions.

Recommendation 17

As proposed by the ACCC, a statutory prohibition of unfair trading should be introduced. The prohibition should extend to prohibiting certain predatory and manipulative conduct associated with data-driven business models. The boundaries of any prohibition must be carefully calibrated so that it is proportionate and does not extend to legitimate business practices. Like statutory unconscionability and the unfair contract terms law, the prohibition should be regarded as a general 'safety net' that forms one part of a layered regulatory regime.

Recommendation 18

Legislation aimed at strengthening the remedies and enforcement of the unfair contract terms law should be reintroduced. In reintroducing the legislation, consideration should be given to including a rebuttable presumption that terms found by a court to be unfair will be presumed unfair if included in a similar contract.

Recommendation 19

Consideration should be given to reforming the unfair contract terms law by introducing a black list of prohibited terms, a grey list of presumptively unfair terms or, preferably, a combination of both.

Recommendation 20

Consideration should be given to resourcing regulators, such as the ACCC, to investigate and potentially design machine learning tools to assist in the identification of unfair terms in standard form consumer contracts. If, as recommended in this Report, the unfair contract terms law were to be amended to include prescriptive lists, such tools could enhance enforcement of the law.

Recommendation 21

Relevant stakeholders should provide consumer guidance on what may constitute a 'safety defect' with respect to CIoT devices (or digital products more generally), including guidance on the 'reasonable expectations' of the community in relation to product security.

Recommendation 22

The defence set out in Section 142(a) of the ACL should be amended such that the ACL covers defects that may be introduced by the manufacturer at a point after the original supply, for example, through software updates. Such an amendment could be enacted by introducing a new sub-section under Section 142(a), such as: 'in the case of digital products – at the time at which the digital products were supplied or subsequently modified or updated by their actual manufacturer'. This drafting is contingent upon the introduction of a category of 'digital products' being introduced into the ACL, as recommended in this Report.

Recommendation 23

In the event that a product liability claim involves a CIoT device with components, the consumer should be able to bring an action against the ultimate supplier or manufacturer, with the burden resting with the supplier or manufacturer to reach a determination as to liability between the providers of the component parts.

Recommendation 24

The liability of manufacturers under Part 3-5 of the ACL should be expanded to cover liability for all loss or damage suffered by a person because of the safety defect, regardless of whether the loss or damage is tangible or intangible, and should extend to including compensation for data loss.

Recommendation 25

The recall provisions under Part 3-3 of the ACL should be expanded to allow for recall (both voluntary and compulsory) of consumer goods where such goods will or may cause injury to any person or otherwise cause loss or damage, regardless of whether such loss or damage is tangible or intangible. Products should be able to be recalled where they cause or are likely to cause significant intangible harms, such as data loss or invasion of privacy.

Recommendation 26

A mandatory information standard for CIoT devices should be established under Part 3-3 of the ACL. The information standard should contain information to be provided to consumers that extends to the security and privacy risks associated with consumer IoT devices, the availability of software updates and the measures consumers may adopt to secure their devices.

Recommendation 27

Australian data privacy law should be reformed to better reflect a new paradigm for regulating ubiquitous collection and processing of data that has been emerging from instruments, such as the European Union's General Data Protection Regulation (GDPR) and the European Commission's proposal for a Regulation on Artificial Intelligence. Recognising the difficulties of regulating at scale, measures should be introduced that better calibrate regulation to reflect the risks of near-ubiquitous data processing practices, while allowing for more effective regulatory oversight. Such measures could include targeted privacy impact statements, data protection by default and by design, and targeted monitoring and auditing.

Recommendation 28

The principle of privacy by design is an essential element of the new regulatory paradigm and should be codified as a distinct privacy principle. However, in codifying the principle, lessons should be learnt from flawed attempts to implement the principle in data privacy laws, such as the GDPR.

Recommendation 29

The principle of privacy by default is an essential element of the new regulatory paradigm and should be codified as a distinct privacy principle. However, in codifying the principle, consideration should be

given to how the principle applies in particular contexts, with a case for stricter application of the principle to high risk acts and practices.

Recommendation 30

Risk-based regulation is an essential element of the new regulatory paradigm and it should be more expressly incorporated into the design of the Privacy Act. For example, the Act could distinguish between acts and practices that pose unacceptable risks, high risks or low risks. However, in implementing this approach, it is important to take into account the significant limitations of and problems with risk-based approaches.

Recommendation 31

As proposed by the recent Privacy Act Review Discussion Paper produced by the Attorney-General's Department (the AGDP), the definition of 'personal information' in the Privacy Act should be amended so that it more closely aligns with the approaches taken in comparable jurisdictions and, in particular, the definition of 'personal data' under the GDPR.

Recommendation 32

The amendments proposed by the AGDP to support the recommended new definition, including a non-exhaustive list of the types of personal information, a list of factors to determine when a person is 'reasonably identifiable', and an amended definition of 'collection' that covers inferred information, should also be introduced.

Recommendation 33

Resources should be allocated to an appropriate body, such as the Office of the Australian Information Commissioner (OAIC), to investigate the potential for risk-based approaches, including a risk-based approach to defining the scope of the Privacy Act, addressing the problems of regulating data collection and processing at scale.

Recommendation 34

The notice provisions of the Privacy Act should be strengthened. Notice should be concise, transparent, intelligible and easily accessible, and it should clearly set out how an Australian Privacy Principles (APP) entity collects, uses and discloses personal information. Resources should be expended on ensuring

that user-friendly ways of presenting notices are adopted, such as layered notices and/or standardised icons. This should be based on rigorous consumer testing.

Recommendation 35

The consent provisions of the Privacy Act should be strengthened. Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed, and any settings for additional data should be preselected to 'off'. Measures should be introduced to minimise consent fatigue, such as the use of standardised icons or phrases, which should be based on rigorous consumer testing.

Recommendation 36

As proposed in the AGDP, a new privacy principle should be introduced requiring the collection, use or disclosure of personal information to be fair and reasonable. This principle should operate in addition to other principles that apply to the collection, use or disclosure of personal information, and, in the event of inconsistencies, should prevail. As further proposed in the AGDP, the principle should be supplemented by a list of non-exhaustive statutory factors. Consideration should be given to whether the statutory factors proposed in the AGDP could be improved, such as by ensuring that a more objective standard is applied in assessing the risk of data processing.

Recommendation 37

Except where data processing is essential for the security and functionality of CIoT devices, default settings allowing for data processing by means of such devices should be pre-selected to 'off'.

Recommendation 38

As recommended by the AGDP, APP 11 should be amended to clarify what amounts to 'reasonable steps' to secure personal information, including by expressly providing that such steps include technical and organisational measures and a list of factors indicating what reasonable steps may be required.

Recommendation 39

Given the extent to which CIoT devices pose fundamental legal and regulatory challenges, they should be subject to a public policy law reform process, potentially as extensive as the ACCC process investigating the regulation of digital platforms. As part of this process, further research is needed on how best to ensure that all applicable laws and regulations are aligned, including by minimising

unnecessary gaps, overlaps or inconsistencies. This process could extend beyond CIoT to include the legal and policy implications of other IoT implementations.

Recommendation 40

Consideration should be given to establishing a dedicated, multi-disciplinary expert body that proactively investigates the social and legal implications of powerful new technologies. While not directly responsible for regulating, such a body could investigate or apply forward-looking practices such as horizon scanning, promoting the appropriate use of RegTech, and aligning applicable laws and technical standards. Consultation with diverse stakeholders, including consumer representatives and representatives of vulnerable groups, would be an important part of this work.

Recommendation 41

As part of a whole-of-society approach to addressing the risks posed by CIoT devices, a public education campaign should be resourced to assist consumers with managing these risks. If the recommendation for establishing the new advisory body is accepted, this body could play a role in consumer education.

Recommendation 42

Further research is needed on how to promote accessibility and inclusivity in relation to CIoT devices to promote the interests of vulnerable groups. This should include research on establishing a framework for promoting inclusive design of CIoT devices. Any public policy law reform process established to comprehensively address the issues raised by CIoT devices should incorporate a distinct component that investigates how to maximise the benefits and minimise the harms posed for vulnerable groups by CIoT devices.

Introduction

This is the Final Report for the Australian Communications Consumer Action Network (ACCAN)-funded project, *Regulation of Internet of Things Devices to Protect Consumers.*

This Report is the result of a research project that commenced in August 2020 and culminated in June 2022 with the release of this Report. The Report responds to the legal and policy challenges posed by Consumer Internet of Things (CIoT) devices, which are increasingly common in the homes of Australians. As explained in this Introduction, there have been important policy developments during the course of this project that have significantly influenced the research project, including the scope of the issues it addresses. The research and the recommendations arising from this Report have also taken into account valuable feedback received from stakeholders, experts and colleagues, including feedback from two well-attended roundtables, which are explained in this Introduction.

This Introduction first sets out the Objectives of the research project resulting in this Report. Following this, it explains the scope of the Report, including issues that are not addressed in the Report. The Introduction then explains the way the project proceeded, including how the research was undertaken and the process for incorporating feedback on the research. It then introduces the Australian policy context for the analysis undertaken in the Report; further, it identifies the most important recent and current public policy developments that have shaped or influenced the recommendations made in the Report. The Introduction next outlines three general themes that have emerged from the research project, which are not dealt with in detail in the Report but are taken up again in the Conclusion. Finally, it sets out the structure of the Report.

Objectives

In the context of CIoT devices in the home, the overall objectives of this project were:

1. To make recommendations for legal and regulatory reform to improve consumer security and privacy;
2. To comprehensively analyse current Australian consumer, data security and privacy laws to identify weaknesses and gaps, with the object of producing international best practice laws and regulation;

3. To provide accessible information for consumers and consumer representatives to better understand: (a) existing consumer legal rights, and (b) practical steps for consumers to better protect their security and privacy when using IoT devices;
4. To increase understanding of the vulnerabilities of devices currently on the market, for the benefit of consumers, consumer representative groups and other stakeholders; and
5. To produce informed commentary on, and analysis of, best practice guidelines for implementing high level principles for securing consumer IoT devices.

This Report mainly addresses objectives (1) and (2) in that it sets out recommendations for legal and regulatory reform based on comprehensive analyses of Australian cyber security, consumer and privacy regulation, and laws. To a lesser extent, it also addresses objectives (4) and (5) through an analysis of the security vulnerabilities of CIoT devices and how security principles can be implemented. This analysis underpins the recommendations in this Report about how to regulate to improve device security. Objective (3) has been addressed by the production of two consumer tip sheets aimed at informing consumers of CIoT devices about their rights and about how to secure their devices.

Scope of this Report

This project was confined to analysing legal and policy issues relating to **CIoT devices for the home,** such as connected appliances and smart assistants; consequently, this Report does not extend to all CIoT devices, such as mobile devices and (with one exception) 'wearables'. The decision to target CIoT devices for the home was made to ensure that the project was manageable, but it was also based on the assumption that limiting the focus of the research in this way would deliver important insights. The one exception that falls outside the scope of CIoT devices for the home was the decision to include a case study for the VTech Smartwatch, which was chosen because it is a device that is specifically marketed at children and for which the terms and conditions are readily available in Australia.

Despite the decision to confine the project to devices in the home, there are clearly common issues that arise in the regulation of all CIoT devices and, for that matter, in the regulation of current generation 'disruptive technologies' more broadly. In particular, these technologies are based on business practices that largely rely on the collection, analysis and use of data at scale. Therefore, the regulation of CIoT devices for the home represents a microcosm of the issues that arise more generally in relation to rapidly-moving, current generation technologies and business practices. The project therefore necessarily addresses these more general issues but does so through the specific lens of the regulation of CIoT devices for the home. This point is expanded upon below.

As set out in objective (2), this Report focuses on three substantive areas of law and regulation, which the project has determined are most relevant to the regulation of CIoT devices: **cyber security, consumer protection and data privacy laws.** This does not mean that areas of the law that are not the focus of this project are irrelevant to the regulation of CIoT devices. On the contrary, areas such as competition law and contract law are also highly relevant to the regulation of these devices. Nevertheless, from the perspective of consumers and for the immediate future, we are confident that the three identified areas are the most important and relevant.

Given the scope of each of the three areas of law and regulation addressed by this Report, it is impossible to cover all legal and policy issues that arise in applying the laws to CIoT devices. Consequently, the project has been necessarily selective in identifying those law reform issues that are the most pressing in relation to consumer protection, both in the short term and in a longer term perspective. However, this means that there have been some issues that are clearly relevant and important, but which it has not been possible to accommodate within the scope of this Report. For example, in the context of consumer privacy protection, the Report has not been able to analyse the issues relating to the application of state and territory surveillance device and listening device laws to CIoT devices.[1] Moreover, the Report does not attempt to deal comprehensively with the full range of issues involving legal liability for harms raised by often complex supply chains, which can involve multiple entities that are responsible for different elements of CIoT devices. Finally, while acknowledging the extent to which CIoT products and services purchased by Australian consumers are often sourced from overseas, the Report does not attempt to address the cross-jurisdictional issues that may arise from applying Australian law to overseas entities involved in the manufacture and supply of these products.

Progress of the Project

This Report is the result of legal and policy analysis that has been undertaken over the duration of the project. Beginning with an extensive literature review in August 2020, this project has engaged in policy-oriented research on the application of the three areas of law and regulation to CIoT devices. The research has benefitted considerably from constructive feedback provided by experts and stakeholders throughout the course of the project.

In accordance with the project plan, a preliminary report was released in July 2021, which was the subject of an online stakeholder roundtable held on 15 July 2021. Participants in the roundtable

[1] See, for example, Surveillance Devices Act 1999 (Vic); Surveillance Devices Act 2007 (NSW).

included academic experts, regulators, industry stakeholders and consumer representatives. The feedback provided at the roundtable was incorporated into the research resulting in considerable changes to the research focus and some of the proposed recommendations. The roundtable discussion was especially important in providing a reality check as to the feasibility of some of the proposals made in the preliminary report. The feedback was incorporated in a draft report, which was released in February 2022, so as to provide time for the incorporation of feedback on revised proposals in time for the final report. The draft report provided the basis for a second online roundtable, which was held on 31 March 2022. Meanwhile, the draft report incorporated substantial material on relevant policy and legal developments, both Australian and international, which occurred following the preliminary report. For example, during this time the UK Government introduced legislation specifically aimed at enhancing the security of CIoT devices. Similar to the first roundtable, the second roundtable included a cross-section of academic experts, regulators, members of federal government departments, industry stakeholders and consumer representatives. Some participants in the online roundtable attended in the capacity of observers. In addition, the draft report was posted to the Social Science Research Network (SSRN) and feedback solicited.[2]

The feedback on the draft report resulted in some modifications to the research focus and changes to the recommendations made in that report, which have been incorporated into this final report. Meanwhile, the research undertaken for this project has resulted in two substantial submissions to relevant Australian policy development processes:

- Evana Wright, David Lindsay, Genevieve Wilkinson, Henry Fraser and Neva Collings, Submission to Department of Home Affairs Discussion Paper on Strengthening Australia's Cyber Security Regulations and Incentives, 27 August 2021.[3]
- David Lindsay, Submission to Attorney General's Discussion Paper on the Privacy Act Review, 21 January 2022.[4]

[2] See David Lindsay, Evana Wright and Genevieve Wilkinson, *Regulating to Protect Security & Privacy in the Internet of Things (IoT)* (Draft Report, ACCAN, UTS, 11 February 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4052068>.
[3] See Evana Wright et al, Submission to Department of Home Affairs, *Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper* (27 August 2021) <https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/wright-lindsay-wilkinson-fraser-and-collings.pdf>.
[4] See David Lindsay, Submission to Attorney General's Department, *Privacy Act Review Discussion Paper* (21 January 2022) <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/view_respondent?_b_index=120&uuId=692946534>.

As would be expected from a project such as this, the rapidly evolving policy context has had a significant impact on the directions taken by this project; this is explained in the next section of this Introduction.

The Evolving Policy Context

Given that, as referred to above, the issues involved with the regulation of CIoT devices are part of the broader context of how law and regulation can be best adapted to apply to rapidly evolving technologies and business practices, it is unsurprising that there have been significant recent policy initiatives that have impinged, more or less directly, on the research project. One of the challenges faced by the project has been responding to the rapidly evolving policy context. While for the most part, the policy initiatives do not specifically target the regulation of CIoT devices, they raise issues – and often include policy proposals – that impact on and are often directly relevant to the Objectives of the project.

Many of the current processes for reforming Australian consumer protection and privacy laws to better reflect technological change have their source in the comprehensive 2019 Australian Competition and Consumer Commission (ACCC) *Digital Platforms Inquiry* (*DPI*). The report produced by this inquiry, known as the *DPI Report*,[5] addressed fundamental legal and regulatory issues relating to the data-centric business models and practices of digital platforms, but extended beyond the specific issues raised by the platforms. The scope of the *DPI Report,* and the ongoing work of the ACCC arising from the report, is illustrated by the extent to which its reverberations have been felt across a range of policy areas.

As set out in this Report, the research undertaken for this project indicates that IoT applications, including CIoT devices, have implications that are as significant for law reform as those raised by digital platforms. These are transformative technologies and, as such, ultimately require paradigm shifts in regulatory responses. In short, what is needed is a policy process to investigate and address the fundamental policy challenges of IoT devices, especially from the perspective of consumers, that is as comprehensive as the ACCC's digital platforms process. It is our hope that this Report will make a contribution to this process.

The most immediate pressing concern for CIoT devices is the inadequate security of many products, particularly those installed in homes. In Australia, there has been much-needed recent policy attention

[5] Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry* (Final Report, June 2019) <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.

given to enhancing cyber security, including recent reforms designed to enhance the security of critical infrastructure.[6] As explained in this Report, a separate process led by the Department of Home Affairs has canvassed proposals for improving the security of CIoT devices which, at the time of writing this Report, seemed likely to result in law reforms.[7]

The most important policy developments that occurred during the course of the project and that have been taken into account in this Report are as follows:

- Department of Home Affairs, *Discussion Paper on Strengthening Australia's Cyber Security Regulations and Incentives*, released on 13 July 2021.[8] The Discussion Paper, arising from Australia's Cyber Security Strategy, canvased options for setting cyber security expectations, increasing transparency and protecting consumer rights, including setting mandatory minimum security standards for smart devices.
- Attorney-General's Department, *Discussion Paper on the Privacy Act Review*, released on 25 October 2021.[9] The *Privacy Act Review*, which arose from the ACCC's *DPI*, is a fundamental review of Australian data privacy law. It includes a review of the scope of the *Privacy Act 1988* (Cth), the protections contained in the Australian Privacy Principles (APPs), and how the *Privacy Act* is regulated and enforced.
- Productivity Commission, *Final Report on the Right to Repair Inquiry*, released on 29 October 2021.[10] The report addressed important consumer protection issues relating to connected IoT devices, including the durability of such devices, and recommended introducing a new consumer guarantee to provide reasonable software upgrades.

[6] See *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth).
[7] During the 2022 federal election campaign, the Minister for Home Affairs, Karen Andrews, announced the intention of the government to introduce mandatory minimum security standards for CIoT devices, to be aligned with those to be introduced in the UK. At the same time, the announcement indicated that it was proposed to introduce a voluntary security labelling scheme: see Justin Hendry, 'Gov Pledges to Mandate IoT Cyber Security Standards', *IoTHub* (online, 13 May 2022) <**Error! Hyperlink reference not valid.**https://www.iothub.com.au/news/gov-pledges-to-mandate-iot-cyber-security-standards-579966>.
[8] Department of Home Affairs (Cth), *Strengthening Australia's Cyber Security Regulations and Incentives: A Call for Views* (Discussion Paper, 13 July 2021) <https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf>.
[9] Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf>.
[10] Productivity Commission, *Right to Repair* (Inquiry Report No 97, 29 October 2021) <https://www.pc.gov.au/inquiries/completed/repair/report/repair.pdf>

In addition, since the publication of its *DPI Report,* the ACCC has engaged in important ongoing work in reviewing the competition and consumer issues arising from digital platforms,[11] which this Report has also taken into account.

Apart from these significant policy-oriented processes, this Report has further addressed current proposed legislative amendments, particularly proposals for enhancing enforcement of the consumer guarantees by introducing a prohibition on failing to provide a remedy for breaching a guarantee,[12] and the February 2022 legislation for strengthening the remedies and enforcement of the unfair contract terms law.[13]

While taking into account these important policy initiatives and proposed reforms, this Report places them in the specific context of the challenges of regulating CIoT devices. As illustrated by sections of this Report, this helps cast light on the connections between what are commonly regarded as distinct areas of the law and the discrete policy processes. As explained later in this Introduction, one of the important themes identified in this Report is the need for greater coherence in policy development and regulatory responses in the face of transformative technologies.

Overarching Themes Emerging from this Research

The substantive sections of this Report, which include recommendations for reforming cyber security, consumer protection and data privacy law and regulation, address the regulatory and policy issues in some detail. However, there are three overall themes that have emerged from the course of the research, which are areas that this Report suggests deserve further research attention. These three areas are:

1. The challenge of aligning laws and 'joining up' regulation
2. Improving consumer education
3. Enhancing accessibility and inclusivity for vulnerable groups

[11] See, for example, Australian Competition and Consumer Commission (ACCC*), Digital Platform Services Inquiry. Discussion Paper for Interim Report No 5: Updating Competition and Consumer Law for Digital Platform Services* (Discussion Paper, 28 February 2022) <https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry.pdf> ('*Discussion Paper for Interim Report No 5*'); ACCC, *Digital Platform Services Inquiry. Interim Report No. 4: General Online Retail Marketplaces* (Interim Report, 31 March 2022) <https://www.accc.gov.au/publications/serial-publications/digital-platform-services-inquiry-2020-2025/digital-platform-services-inquiry-march-2022-interim-report>.

[12] Department of the Treasury on behalf of Consumer Senior Officials, *Improving the Effectiveness of the Consumer Guarantee and Supplier Indemnification Provisions under the Australian Consumer Law* (Consultation Regulation Impact Statement, December 2021) <https://treasury.gov.au/sites/default/files/2021-12/c2021-224294-cgsicris_2.pdf>.

[13] Treasury Laws Amendment (Enhancing Tax Integrity and Supporting Business Investment) Bill 2022 (Cth).

This Report introduces these themes here and returns to them in the conclusion.

Aligning Laws and 'Joining Up' Regulation

Transformative technologies, such as CIoT, can disrupt laws, resulting in laws and regulations that overlap, are inconsistent or misaligned. One reason for this is that laws and law reform processes – such as those mentioned above – are based on pre-existing legal and policy paradigms, which each have their own rationales and are challenged by new and emerging technologies. This Report identifies the rationales for each of the three areas of law and regulation in introducing the regulatory challenges posed by CIoT devices.

The current wave of technologies is based on the mass collection, analysis and use of data. However, there is no clear set of coherent legal principles or laws that applies to these processes. Instead, as this Report explains in some detail, we have a patchwork of laws with diverse objectives and overlaps; but as they were designed to apply to previous generations of technologies, they are often ill-suited to regulate current and emerging technologies.

The proliferation of CIoT devices represents a step change in the data-centred business model that underpins the digital economy. This model, as illustrated by the practices of the digital platforms, involves collecting data about consumers at scale, which are analysed and used for targeted advertising or for potentially other practices involving the use of 'dark patterns'.[14] CIoT devices feature the large-scale collection and processing of data as integral parts of the products, and they potentially take these practices further – especially as the processing of data can have physical or cyber effects on consumers. Moreover, as the devices are connected, they commonly incorporate continuous data collection and software updates that are capable of altering functions, such as by adding or disabling features.

The 'always-on' connected nature of smart devices, together with their limited power, makes them vulnerable to security breaches. Moreover, as the collected data is often personal and may be extremely sensitive, the devices expose consumers to privacy breaches. In addition, the devices are often complex, making it difficult to diagnose and fix a problem when something goes wrong, including security problems. As this Report explains, this can raise complex consumer protection issues. Overall, these features of the devices reinforce the extent to which security and data privacy have become central to consumer protection in the digital economy. Protecting purchasers and users of CIoT devices

[14] See ACCC, *Discussion Paper for Interim Report No 5* (n 11).

therefore cuts across the categories of cyber security, consumer protection and data privacy laws and regulation. As Helberger et al have explained:

> *In data-driven consumer markets, the distinction between consumer law and data protection law is far from clear-cut. With the integration of more and more data into consumer products, many data protection issues also become consumer issues, and vice versa.*[15]

The difficulties posed by siloised laws and law reform processes were highlighted by a report by the Communications and Digital Committee of the UK House of Lords, released in December 2021, which found that:

> *… regulation was fragmented across different areas, with gaps and overlaps stemming from the piecemeal process by which regulation had developed. The solution was not to be found in more regulation, but in a different approach to regulation, with a coordinated response across policy areas.*[16]

As explained in the Conclusion to this Report, this 'different approach' means that attention must be given to aligning discrete areas of the law so as to avoid gaps, overlaps and potential inconsistencies.

While much of this Report focuses on proposals for law reform, reforming the substantive law can only ever be part of the solution: reform of regulatory institutions is also required in order to ensure consistency in regulatory practices. In the UK, a Digital Regulation Cooperation Forum (DRCF) was established in 2020 to promote greater cooperation between the competition, privacy and communications regulators in regulating new technologies.[17] However, the House of Lords Committee report referred to above doubted if this was enough, favouring the establishment of an independent statutory authority.

In Australia, there are established mechanisms for coordinating the activities of regulators. These include a Memorandum of Understanding (MoU) between the ACCC and the Office of the Australian Information Commissioner (OAIC) on sharing information,[18] and the recently-established Digital

[15] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 *Common Market Law Review* 1427, 1428.
[16] Communications and Digital Committee, House of Lords (UK), *Digital Regulation: Joined-Up and Accountable* (Report No 3 of Session 2021–22, 13 December 2021) 5 <https://committees.parliament.uk/publications/8186/documents/83794/default/>.
[17] See Competition & Markets Authority, Information Commissioner's Office and Ofcom, *Digital Regulation Cooperation Forum* (Report, July 2020) <**Error! Hyperlink reference not valid.**https://www.ofcom.org.uk/__data/assets/pdf_file/0021/192243/drcf-launch-document.pdf>.
[18] Office of the Australian Information Commissioner (OAIC), *MOU with ACCC – Exchange of Information* (MoU, August 2020) <https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-of-understanding/mous/mou-with-accc-exchange-of-information>.

Platform Regulator's Forum, involving the ACCC, OAIC, the Australian Communications and Media Authority (ACMA) and the e-Safety Commissioner.[19] There are also less formal channels for cooperation between regulatory agencies and government departments.

The challenge of promoting coherency and consistency across government and regulatory agencies – which is commonly known as the problem of 'joined-up regulation' or 'joined-up government'[20] – is not new. However, the extent to which transformative technologies raise issues that cut across regulatory silos makes addressing it more pressing. This issue is taken up in the Conclusion to this Report.

Consumer Education

At present, the burden for dealing with the complex issues raised by CIoT devices, including security and other consumer protection concerns, is disproportionately borne by consumers. Many of the recommendations in this Report, including recommendations about regulating the design of CIoT products, are aimed at placing at least some of that burden back on manufacturers or suppliers. That said, consumers must bear a degree of responsibility for potentially harmful devices installed in the home. This means that more attention should be given as to how best to assist consumers with navigating the complexities and problems associated with CIoT devices. While this Report focuses on law reforms, consumer education must play a critical role in effectively addressing the concerns experienced by consumers that purchase CIoT products.

Although it is common to suggest that problems faced by consumers should be addressed by providing more information, this can actually exacerbate 'information overload', thereby compounding the problems. Therefore, much depends upon the way in which information is provided to consumers. As recommended in this Report, labelling schemes have the potential to improve consumer understanding of security vulnerabilities. However, to be effective, such schemes need to be founded on rigorous consumer testing. This Report also recommends that attention should be given to how critical consumer information, including contractual terms and conditions, is presented by suppliers to consumers. Considerable attention is being given as to how 'design thinking' can be used to enhance consumer understanding of documents, including (but not confined to) visual design.[21] While

[19] ACCC, 'Agencies Form Digital Platforms Regulators Forum' (Media Release, ACCC, 11 March 2022) <https://www.accc.gov.au/media-release/agencies-form-digital-platform-regulators-forum>.
[20] See, for example, Vernon Bogdanor (ed), *Joined-Up Government* (Oxford University Press, 2005); World Economic Forum (WEF), *Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators* (Report, December 2020) <https://www3.weforum.org/docs/WEF_Agile_Regulation_for_the_Fourth_Industrial_Revolution_2020.pdf>.
[21] See, for example, Thomas Kaldor, '5 Reflections about Legal Design and Reimaging Contract', *LegalVision* (13 July 2020) <**Error! Hyperlink reference not valid.**https://legalvision.com.au/legal-design-and-reimagining-contracts/>.

showing some promise, there is scope for more attention to be focused on how this can be best applied in particular contexts, such as CIoT devices.

Further issues involved with enhancing consumer education are taken up in the Conclusion to this Report. However, for the purpose of this Introduction, it is important to note that the recommendations for law reform that are made in this Report cannot hope to be successful unless there is a whole-of-society approach to strengthening consumer protection; consumer information and education initiatives must be an essential part of this.

Vulnerable Groups and CIoT Devices

Like many new technologies, CIoT devices can have significant effects on vulnerable groups, both positive and negative. CIoT devices, including some that feature in the case studies in this Report, hold out the promise of empowering vulnerable groups, such as by increasing accessibility and functionality for vulnerable people and thereby increasing their independence. For example, people with disabilities can benefit from technologies with appropriate human-machine interfaces that allow control of everyday home devices, such as lights, televisions and smart doors. Similarly, voice activated devices – or smart doorbells with facial recognition technology – can assist people with vision impairment or low vision. However, if the devices do not work properly or if there is a security breach that discloses sensitive information, this may compound the difficulties faced by vulnerable people.

This highlights the importance of not treating consumers as a homogeneous group and recognising that technologies can impact people in different ways. Sharing data collected from CIoT devices can assist a vulnerable person who may depend upon a network of carers. Some of this data could, for example, help to determine if a person needs assistance. Conversely, remote access to IoT data can create significant threats in contexts such as partner abuse or domestic violence.[22]

One particular area of concern is the potential for CIoT data to be used to manipulate vulnerable people, including through practices designed to elicit consent. As this Report explains, if these practices are a concern for consumers in general, they are even more of a concern for members of some vulnerable groups. It is therefore important for the presentation of critical information about

[22] Diarmid Harkin, Monique Mann and Ian Warren, 'Consumer IoT and its Under-Regulation: Findings from an Australian Study' (2022) 14 *Policy & Internet* 96; Ignacio Rodríguez-Rodríguez et al, 'Towards a Holistic ICT Platform for Protecting Intimate Partner Violence Survivors Based on the IoT Paradigm' (2020) 12(1) *Symmetry* 37.

CIoT products, including contractual terms and conditions and privacy policies, to be designed in ways that take into account the needs of vulnerable groups.[23]

Moreover, this is but one aspect of the importance of taking into account the needs and interests of vulnerable groups in the design of products and services. For example, CIoT devices fail to reach their potential when they are not designed on the basis of the principles of accessibility and inclusivity. As Moon et al point out, the best way to address this fundamental problem is by applying the principles of inclusive design to incorporate the needs of vulnerable people into the design of CIoT products:

> *An inclusive design process, taking into consideration the characteristics and needs of a wide range of users, during the conceptualization of the devices, rather than after they have been developed, can proactively address such issues as technology abandonment or discontinuance while enhancing acceptance of these technologies as socially acceptable and culturally appropriate.*[24]

In short, as this Report contends, while incorporating consumer protection into the design of CIoT devices is an important element of any future regulatory framework, particular attention is needed to address how to incorporate the needs of vulnerable groups into design processes. As with consumer education, achieving desirable design outcomes requires a whole-of-society approach, which in the case of inclusive design, can extend to law reforms and technical standards. Importantly, as emphasised in feedback received on this project, this means establishing effective mechanisms for consulting with vulnerable groups, both in inclusive design of technologies and in legal and policy reform processes. As this Report concentrates on general reforms to strengthen the protection of consumers of CIoT devices, and given the range and complexity of issues involved in developing a framework for the promotion of inclusive design, it does not explore these issues in depth. That said, given the importance of enhancing the accessibility and inclusivity of CIoT devices for vulnerable groups, the Report returns to this issue in the Conclusion.

[23] Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR when Vulnerable People use Smart Devices' (2022) *International Data Privacy Law* (forthcoming).
[24] Nathan W Moon, Paul MA Baker and Kenneth Goughnour, 'Designing Wearable Technologies for Users with Disabilities: Accessibility, Usability, and Connectivity Factors' (2019) 6 *Journal of Rehabilitation and Assistive Technologies Engineering* 1.

Structure of this Report

This Report has five main Parts.

First, following this Introduction, Part 1 introduces CIoT devices for the home and identifies the features of those devices that pose specific challenges for cyber security, consumer protection and data privacy laws and regulation. This Part also sets out the objectives and rationales for these three areas of law and regulation, which helps frame the policy analysis in later sections of the Report.

Secondly, in Part 2, the Report sets out the case studies undertaken for this project. The case studies focus on specific CIoT devices and are used to identify and illustrate common problems faced by consumers of CIoT devices. Each case study describes the device and explains the most important legal issues raised by the devices by means of an analysis of the terms and conditions and other publicly available information on the devices. The case studies are referred to at relevant points in the analysis of the legal and policy issues addressed in the following substantive sections of the Report.

In Parts 3 to 5, the Report identifies the legal challenges and makes recommendations for law reform in each of the three areas of law and regulation addressed by the Report: cyber security, consumer protection and data privacy law. For each of these areas, the current law is explained and analysed, identifying gaps and weaknesses in the application of each of the areas of law and regulation to CIoT devices. Where relevant, legal developments in comparable jurisdictions are drawn upon. Each of these Parts of the Report identifies recommendations for law reform and explains the reasons for the recommendations. The recommendations include proposals for immediate reforms, which mainly fit within current law reform policy processes, as well as proposals for more fundamental reforms, including developing new regulatory paradigms.

The Report concludes with a Conclusion, which sets out the main points arising from the Report and takes up some of the issues identified in this Introduction.

A Summary Report that summarises the main findings of the research and our recommendations has also been prepared and is available on the ACCAN website, www.acaan.org.au.

1 Regulatory Challenges of CIoT Devices

Introduction

Part 1 of the Report explains the regulatory challenges that are posed by CIoT devices and therefore forms the essential background to the substantive parts of the Report that analyse the adequacy of Australian cyber security regulation, consumer protection law and data privacy law.

First, this Part addresses the scope of the Report by explaining the consumer products that fall within the Report's definition of CIoT devices. It then identifies the distinctive features of CIoT devices, which pose challenges for cyber security regulation, consumer law and data privacy law. In explaining the challenges, each section begins by identifying the objectives of each of the three areas of regulation and law. Subsequently, the particular features of CIoT devices that pose challenges are outlined. As will be seen, taken together these features mean that CIoT devices are radically different from traditional, tangible consumer products. In short, CIoT devices differ from traditional consumer products because they include significant digital elements and they are always connected. But as will be seen, the specific challenges differ depending upon the legal regime.

While this Part of the Report attempts to comprehensively identify all of the challenges posed by CIoT devices, as explained in the Introduction to this Report, it is not possible to address all of the challenges within the scope of one report. Instead, the Report focuses on the challenges that this project has identified as those which are the most important for consumers.

1.1 What are CIoT Devices?

There is no single accepted definition of the Internet of Things (IoT).[1] In colloquial terms, it refers to physical products with embedded software that are connected ('always on') to the Internet.[2] The following more formal and technical definition was adopted by the International Telecommunication Union (ITU) in 2012 and remains applicable today:

[1] Andrew Whitmore, Anurag Agarwal and Li Da Xu, 'The Internet of Things – A Survey of Topics and Trends' (2015) 17 *Information System Frontiers* 261.
[2] Natasha Tusikov, 'Regulation Through "Bricking": Private Ordering in the "Internet of Things"' (2019) 8(2) *Internet Policy Review* 1, 2.

> *A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*[3]

An essential characteristic of an IoT device is that it incorporates 'sensors', which enable data to be collected, distributed and acted upon.[4]

Given the potential for a vast array of products in diverse contexts to be classified as IoT devices, it is important to distinguish between differing implementations of the IoT, such as industrial IoT (IIoT), consumer IoT (CIoT) and healthcare IoT (HIoT).[5] Due to the distinct and significant security challenges arising from consumer devices, initial IoT-specific regulation has focused on CIoT, which a 2019 European technical specification defines as:

> *[N]etwork-connected (and network-connectable) devices and their associated services that are usually available for the consumer to purchase in retail and that are typically used in the home or as electronic wearables.*[6]

The specification includes an illustrative list of CIoT devices, including: connected children's toys and baby monitors; connected safety-relevant products, such as smoke detectors and door locks; smart cameras, TVs and speakers; wearable health trackers; connected home automation and alarm systems; connected appliances (eg, washing machines, fridges); and smart home assistants.[7]

In general, this Report adopts this approach to the scope of CIoT devices but, as explained in the Introduction, it generally confines itself to consumer smart devices that are used in the home. It therefore excludes devices that are intended to be worn on the person, such as health monitors (which raise specific regulatory issues) and other wearables (with the single exception of a case study on a children's smartwatch, which was selected because of the specific issues it raises for children). It also excludes devices that have a primary purpose of communicating (including internet access), such as conventional smartphones, tablets, desktop computers and laptops, which also raise particular

[3] International Telecommunication Union (ITU), *Overview of the Internet of Things* (Recommendation No ITU-T Y.2060, June 2012) <https://www.itu.int/rec/T-REC-Y.2060-201206-I>.
[4] Tusikov (n 2) 2.
[5] The European Union Agency for Cybersecurity (ENISA), for example, has developed different security recommendations for different IoT sectors, such as smart manufacturing, smart cars and smart hospitals: ENISA, *Industry 4.0 Cybersecurity: Challenges and Recommendations* (Report, 20 May 2019) <https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations>; ENISA, *Good Practices for Security of IoT: Secure Software Development Lifecycle* (Report, 19 November 2019) <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>.
[6] European Telecommunications Standards Institute (ETSI), *Cyber Security for Consumer Internet of Things* (Technical Specification No ETSI TS 103 645 v1.1.1, February 2019) [3.1] <https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf>.
[7] Ibid 6.

regulatory issues. As a result, most but not necessarily all of these communication devices are commonly excluded from regulations that apply to CIoT devices.

1.2 Cyber Security Challenges

At its core, the rationale for regulating the safety and security of CIoT devices mirrors that for regulating other consumer products: markets unaided do not deliver adequate protection due to insufficient consumer information about the safety of products, behavioural biases of consumers and information overload.[8] However, insecure CIoT devices give rise to the following problems – largely associated with their connected 'always on' characteristic – over and above the safety concerns relating to traditional 'unconnected' products.

1.2.1 Vulnerability and Weak Security

CIoT devices are vulnerable because they have limited processing power, which creates challenges for the processing of data necessary to ensure security. Moreover, the high numbers of connected CIoT devices with poor security creates a large attack surface for malicious actors.[9] As summed up in Hyponnen's law, '(w)henever an appliance is described as "smart", it's vulnerable'.[10] This means that the security of sensitive CIoT devices, such as IoT-enabled locks, temperature-control devices or children's toys, may be compromised.

1.2.2 Capacity to Inflict Harm Remotely

Whereas safety defects may be 'baked in' to conventional consumer products, the 'always connected' nature of consumer IoT devices enables malicious third parties to cause harms remotely, such as unauthorised access to data or adverse effects on the operation of devices.

1.2.3 Insecurity at Scale: System-Wide Risks

Apart from individual harms, the vulnerabilities of IoT devices create system-wide risks of large attacks launched by networks of insecure devices.[11] The best known of these attacks have involved the Mirai

[8] Gillian K Hadfield, Robert Howse and Michael J Trebilcock, 'Information-Based Principles for Rethinking Consumer Protection Policy' (1998) 21 *Journal of Consumer Policy* 131; Christian Twigg-Flesner, 'Information Disclosure about the Quality of Good – Duty or Encouragement?' in Geraint Howells, André Janssen and Reiner Schultz (eds), *Information Rights and Obligations: A Challenge for Party Autonomy and Transactional Fairness* (Routledge, 2005) 135.
[9] Marie O'Neill, 'Insecurity by Design: Today's IoT Device Security Problem' (2016) 2 *Engineering* 48; Eliza Chapman and Tom Uren, *The Internet of Insecure Things* (Issues Paper, Australian Strategic Policy Institute, 2018) <https://www.aspi.org.au/report/InternetOfInsecureThings>.
[10] Mikko Hypponen and Linus Nyman, 'The Internet of (Vulnerable) Things: On Hyponnen's Law, Security Engineering, and IoT Legislation' (2017) 7(4) *Technology Innovation Management Review* 5.
[11] Department for Digital, Culture, Media & Sport (UK), *Secure by Design: Improving the Cyber Security of Consumer Internet of Things* (Report, 7 March 2018) <https://www.gov.uk/government/publications/secure-by-design-report>.

malware, which has used common factory default usernames and passwords to infect IoT devices, such as cameras and home routers, to launch distributed denial of service (DDoS) attacks.[12]

Therefore, insecure IoT devices differ from unsafe traditional consumer products, such as medicines without child safety caps, in that harms may be caused remotely and may be very widespread. As Winn observed in relation to IT products more generally, a significant 'difference between the impact of IT standards and standards for tangible products is the type and magnitude of externalities found in markets for IT networks versus markets for traditional tangible products'.[13]

1.3 Consumer Protection Challenges

There are three main forms of rationale for consumer protection laws. First, economic rationales conceive consumer protection as necessary to correct market failures that arise from consumers having inadequate information or behavioural biases.[14] Second, consumer law can be seen as being necessary to protect the positive rights of consumers and as a result, protecting consumer autonomy and dignity.[15] Third, taking inequality as a starting point, consumer law can be conceived as a means for promoting distributive justice through policies aimed at redistributing wealth and guaranteeing access to basic goods and services.[16]

As explained at 4.1, the objectives of the *Australian Consumer Law* (*ACL*), which were drawn from a 2008 Productivity Commission report,[17] are based on the economic understanding that effective market-based competition is the principal mechanism for enhancing consumer welfare with the main role of consumer law being to enhance and supplement market-based competition, such as by establishing mandatory standards (the 'consumer guarantees') to address the information asymmetry

[12] Joel Margolis et al, 'An In-Depth Analysis of the Mirai Botnet' in Juan E Guerrero (ed), *Proceedings — 2017 International Conference on Software Security and Assistance (ICSSA)* (Conference Paper, Institute of Electrical and Electronics Engineers, 2018).
[13] Jane K Winn, 'Information Technology Standards as a Form of Consumer Protection Law' in Jane K Winn (ed), *Consumer Protection in the Age of the 'Information Economy'* (Ashgate, 2006) 99.
[14] Hans-W Micklitz, Lucia A Reich and Kornelia Hagen, 'An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law"' (2011) 34 *Journal of Consumer Policy* 271; Amitai Etzioni, 'Behavioural Economics: Next Steps' (2011) 34 *Journal of Consumer Policy* 277.
[15] Gretchen Larsen and Rob Lawson, 'Consumer Rights: An Assessment of Justice' (2013) 112 *Journal of Business Ethics* 515; United Nations Conference on Trade and Development (UNCTAD), *Manual on Consumer Protection* (United Nations Publication No UNCTAD/WEB/DITC/CLP/2016/1, 2016) <https://unctad.org/system/files/official-document/webditcclp2016d1.pdf>.
[16] Thomas Wilhelmsson, 'Consumer Law and Social Justice' in Iain Ramsay (ed), *Consumer Law in the Global Economy: National and International Dimensions* (Ashgate, 1997) 217; UNCTAD (n 15).
[17] See Productivity Commission, *Review of Australia's Consumer Policy Framework* (Inquiry Report, No 45, 30 April 2008) v1 <https://www.pc.gov.au/inquiries/completed/consumer-policy/report/consumer1.pdf>.

between consumers and suppliers.[18] Nevertheless, some elements of the regime can be interpreted as aimed at enhancing consumer rights.

While CIoT devices deliver benefits to consumers, they also pose threats of harms that are different and distinct from the potential harms arising from other consumer products. This part of the report identifies the specific challenges posed by CIoT devices for consumer law and policy. Some of these challenges exacerbate existing problems, especially problems relating to software-enabled devices, whereas others are unique to CIoT devices. Many of the challenges relate to the complexity of CIoT devices and IoT supply chains when compared with other consumer products. Other important challenges relate to the extent to which 'always connected' devices are 'tethered' to service providers, which gives the service providers significant ongoing power over the devices.[19]

1.3.1 Hybrid Nature of CIoT Devices

CIoT devices are complex products, which may consist of hardware, software, data and service components.[20] Moreover, the extent to which the functions of the devices depend upon software that may be automatically updated by AI (Artificial Intelligence) algorithms, means that the functions and nature of the devices are not necessarily fixed but may be subject to significant and potentially unpredictable change as devices evolve over time.[21] The complex nature of CIoT devices may even mean that it is difficult to determine what is meant by the 'product' covered by a consumer contract with a supplier.[22]

1.3.2 Opacity of CIoT Devices

CIoT devices are subject to software updates, which are necessary to ensure the security and functionality of the devices but may result in significant changes to the product. At times, however, software updates may be irritating and time-consuming and may even – as explained below – adversely affect the usability of a product. Furthermore, the often complex interactions between software, data and hardware mean that it may be difficult for consumers to know how their devices work or about changes in the way in which devices work. Therefore, consumers often have imperfect

[18] Jeannie Marie Paterson, 'Critique and Comment: The New Consumer Guarantee Law and the Reasons for Replacing the Regime of Statutory Implied Terms in Consumer Transactions' (2011) 35(1) *Melbourne University Law Review* 252.
[19] Tusikov (n 2).
[20] Consumers International, *The Internet of Things and Challenges for Consumer Protection* (Report, April 2016) 33 <https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>.
[21] Guido Noto La Diega and Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 7(2) *European Journal of Law and Technology* 1, 4.
[22] Ibid 8.

information about the nature of the product they are purchasing, how it might be changed and how it works.[23]

1.3.3 'Tethered' Nature of Connected Devices

With traditional consumer products, the manufacturer or distributor has a limited role in the product following purchase. However, the dependence of CIoT devices on software updates, including security updates, means that consumers are in an ongoing relationship with service providers. This confers significant power on service providers, including the ability to impair or destroy the functionality of software-dependent devices, which is known as 'bricking'.[24]

1.3.4 Complexity of Legal Liability

The complex nature of CIoT devices and IoT supply chains means that multiple parties are involved in the supply of such devices. These parties may include manufacturers, software providers, third party app providers, cloud service providers, other third party service providers, internet service providers (ISPs) and payment facilitators.[25] Moreover, CIoT devices are often subject to multi-layered contracts with, for example, separate contracts relating to device hardware and software services.[26] The complexity of CIoT devices, supply chains and contractual arrangements means that it may be difficult to determine what has gone wrong with a device and which party is legally liable if something does go wrong.

1.3.5 Complexity of Ownership

The hybrid nature of CIoT devices means that the same device may be subject to different ownership regimes. In particular, while property in the hardware may pass to the consumer, the software is likely to be subject to a licensing agreement, such as an End User Licence Agreement (EULA), with ownership remaining in the software provider. This split in ownership means that unlike traditional consumer appliances, the consumer depends on a long-term relationship with a software provider, which may have implications for ongoing use of the device.

1.3.6 Obstacles to Repairing Devices

As noted previously, the complex nature of CIoT devices may make it difficult to determine what has gone wrong with a device where there is a fault or defect. Furthermore, as CIoT devices are controlled by software, consumers may encounter obstacles in having devices repaired. For example, the

[23] Consumers International (n 20) 28–29.
[24] Tusikov (n 2).
[25] Consumers International (n 20) 29.
[26] Noto La Diega and Walden (n 21).

software may be subject to a technological protection measure (TPM), such as encryption, which can inhibit or prevent repair.[27]

1.3.7 Consumer Lock-In

The complex nature of CIoT devices means that they may depend upon a number of interacting components or products. Key component providers, such as software providers, may leverage their position to ensure that consumers are locked-in to purchasing interactive elements or products, such as apps, from either the software supplier or another preferred supplier. Moreover, given the degree to which some CIoT devices generate or depend upon a significant amount of consumer data, software providers may restrict the ability of consumers to port their data to other devices, thereby effectively locking a consumer into a particular supplier's IoT ecosystem.[28]

1.3.8 Jurisdictional Issues

Some of the multiple parties involved in supplying CIoT devices may not be located in Australia and some of the services supplied may be provided from outside of Australia. For example, data required to make a device function may be stored in the cloud in another legal jurisdiction, or a particular app may be operated from another jurisdiction. This can give rise to questions relating to the jurisdiction of Australian courts and applicable law, not to mention potential practical difficulties in enforcing the law against a foreign party.[29]

1.4 Data Privacy Challenges

Data privacy laws, such as the Australian *Privacy Act 1988* (Cth) (*Privacy Act*), are primarily concerned with regulating the collection, storage, use and disclosure of personal information. The main rationales for data privacy laws are either consequentialist or rights-based. Consequentialist justifications focus mainly on the harms that may result from privacy breaches, whereas rights-based justifications are based on protecting the autonomy and human dignity of individuals.[30] The objectives of the *Privacy Act* include both consequentialist and rights-based considerations.[31]

The main features of CIoT devices that challenge data privacy laws are as follows.[32]

---

[27] Consumers International (n 20) 34.
[28] Ibid 37–39.
[29] Noto La Diega and Walden (n 21) 13–14.
[30] See David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131; Sacha Molitorisz, *Net Privacy: How We Can Be Free in an Age of Surveillance* (New South Publishing, 2020).
[31] See *Privacy Act 1988* (Cth) s 2A.
[32] See generally: Internet Society, *Internet Society Policy Brief: IoT Privacy for Policymakers* (Report, September 2019) <https://www.internetsociety.org/wp-content/uploads/2019/09/IoT-Privacy-Brief_20190912_Final-EN.pdf>;

1.4.1 Mass, Undifferentiated Data Collection

CIoT devices are characterised by a variety of sensor technologies, including video cameras, microphones and infrared detectors. These devices may be 'always on', resulting in continuous sensing, watching or listening to activities in the home. However, even if the devices are not 'always on' and the sensors need to be activated, they can result in dragnet collection of data that can be linked to individuals.[33] Once linked to an individual, these data can reveal a considerable amount about a person and can be used to build a profile, as explained below.

1.4.2 Data Matching to Draw Inferences

In a process known as 'sensor fusion',[34] data collected from CIoT devices may be combined with other data, including data from other IoT sensors, to draw highly revelatory inferences about individuals and their behaviour. As Richardson et al point out:

> *[T]he giving out of … anodyne personal data can pose a significant threat to data subjects where their data are accumulated, combined and drawn on to construct personal profiles of these individuals (along with others in their networks and groups) extending to their bodies, habits, personal characteristics and aspirations.*[35]

In general, the fusion of data across devices is poorly disclosed by CIoT businesses and poorly understood by consumers.[36]

1.4.3 Blurring of Boundaries

Traditionally, the home has been regarded as a 'private sphere', immune from monitoring and surveillance. However, by facilitating ubiquitous data collection and monitoring, CIoT devices have the potential to break down boundaries between private and public, as well as boundaries between online and offline. This threatens what Nissenbaum terms 'contextual integrity', which essentially means the ability of people to manage contexts in which information about them is revealed and used.[37]

Gilad Rosner and Erin Kenneally, *Clearly Opaque: Privacy Risks of the Internet of Things* (Report, Internet of Things Privacy Forum, May 2018) <https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54>.

[33] Scott R Peppet, 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent' (2014) 93 *Texas Law Review* 85.

[34] Ibid.

[35] Megan Richardson et al, 'The Internet of Things (IoT) and the Meaning of "Personal Data": A Case Study in Regulation for Rights' (2020) 3 *European Journal of Consumer Law* 503, 510.

[36] Rosner and Kenneally (n 32) 42.

[37] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009).

1.4.4 Opaque Data Collection

Many CIoT devices – which can involve sensors embedded in conventional household items, such as televisions, coffee machines or bathroom scales – are designed to be unobtrusive. This can result in data being collected without people being aware. Even if household members are initially aware that data are being collected, they may become inured to this over time. Moreover, visitors to a house or possibly some house members will not necessarily be aware that data is being collected or that they are effectively being monitored.

1.4.5 Difficulties in Getting Informed Consent

Following from the extent to which CIoT devices may collect data about a person without that person knowing, it is difficult or impossible to get the consent of people, such as household members and visitors to a home, for the collection of data.

1.4.6 Increased Possibility of Consumer Manipulation

By extending online models of the collection and use of data into the offline world, the CIoT increases the potential for commercial entities to use the data to influence or manipulate consumers. As Zuboff reported one manager at an IoT company as acknowledging:

> *It's no longer simply about ubiquitous computing. Now the real aim is ubiquitous intervention, action, and control. The real power is that now you can modify real-time actions in the real world. Connected smart sensors can register and analyse any kind of behavior and then actually figure out how to change it. Real-time analytics translate into real-time action.*[38]

1.4.7 System-Wide Erosion of Privacy

By accepting the large-scale use of devices in the home that effectively monitor behaviour in return for the convenience offered by the devices,[39] consumers may become habituated to everyday surveillance. Through myriad intrusions, this can contribute to the system-wide erosion of privacy and user autonomy, including the sense of what amounts to a 'reasonable expectation' of privacy.

[38] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019) 293.
[39] Melissa W Bailey, 'Seduction by Technology: Why Consumers Opt Out of Privacy in Buying into the Internet of Things' (2016) 94(5) *Texas Law Review* 1023.

2 Case Studies

Introduction

While the previous Part of this Report identified the challenges posed by CIoT devices to the regulatory regimes addressed in this Report, Part 2 illustrates the challenges by means of a series of case studies. The case studies were selected principally to provide a good cross-section of consumer products but also on the basis of availability of products in Australia, as well as accessible information about the products. With the exception of the VTech Smartwatch, which was chosen because it is specifically marketed at children, the case studies all feature CIoT products for the home. The case studies are based on an analysis of the terms and conditions for each of the products, as well as other publicly available information, including information available on websites.

The case studies in this Part of the Report are as follows.

1. Ring Doorbell
2. Roomba
3. Google Nest
4. Vtech Smartwatch
5. August Smartlock
6. Tapo Smartbulb

With minor variations, each of the case studies outlines the following: *product overview,* which briefly explains the CIoT device; *nest of agreements,* which identifies the relevant consumer contracts and associated policies; *contract formation,* which explains the conditions for entering into contracts and the incorporation of terms into consumer contracts; *data storage and use,* which explains the arrangements for storing and securing consumer data; *software updates,* which explains the legal arrangements that apply to software updates and changes to services; and *consumer protection issues,* which identifies particular consumer protection issues arising from the terms of service in some of the case studies.

2.1 Ring Doorbell Case Study

2.1.1 Product Overview

Ring is a United States (US) based company (owned by Amazon) that provides a range of home security devices and services, including video doorbells, security cameras and home monitoring plans. The Ring Terms of Service apply to the 'use or access to our services, software, mobile application, and our websites (the 'Services') and Ring hardware products or devices ('Products')'.[1]

2.1.2 The Nest of Agreements

The use of Ring Products and Services is governed by a suite of legal terms and conditions, including policy documents incorporated by reference. These agreements are as follows:

- Ring Australia Terms of Service (last updated 6 May 2020)
- Ring Privacy Notice (effective date 12 March 2020)
- Ring Copyright Policy (effective 25 November 2016)
- Ring Neighbor's Community Guidelines
- Other terms and conditions as may be posted on the Ring website[2]

The use of multiple documents, including material posted on various web pages, may result in consumer uncertainty as to the nature of the arrangement they are entering into with Ring. Ring states that '[s]pecific areas or pages of our websites may include additional or different terms relating to the purchase or use of our Products and Services or Third Party Services'. For those consumers who do attempt to read and understand the legal terms and conditions, it is difficult to determine which documents apply, especially where reference is made to other terms and conditions posted on the Ring website without reference as to where or what these may be.

2.1.3 Contract Formation

2.1.3.1 Acceptance of terms of service

The Ring Terms of Service state that if the user does not agree to the terms they should not purchase or use the Ring Products or Services.[3] It may be possible for Ring to insist that users not 'use' products or services if they do not agree to the Terms of Service where such Terms of Service are made available

[1] See 'Ring Australia Terms of Service', *Ring* (Web Page, last updated 6 May 2020) <https://ring.com/au/en/terms#TOS-AU>.
[2] The Ring Terms of Service state: 'Specific areas or pages of our websites may include additional or different terms relating to the purchase or use of our Products and Services or Third Party Services. In the event of a conflict between such specific terms and these Terms, the specific terms shall control'. Ibid.
[3] The Ring Terms of Service state: '*If you do not agree with these Terms, please do not purchase or use our Products or Services or Third Party Services.*' Ibid.

at the installation time (although purchasers must then have the right to return the product if they have a 'change of mind'). However, it seems impractical to suggest that users are aware of the Terms of Service before purchase or that purchase of Products or Services constitutes effective agreement to the Terms of Service.

2.1.3.2 Updates to terms and conditions

The Ring Terms of Service provide that the terms and conditions may be updated by Ring from time to time, with only 'material changes' (as determined by Ring) notified to the user through publication on the website, through the Service, email or some other means. Ring encourages users to check the website for updates from time to time. The Terms of Service provide that continued use of the Product or Services constitutes acceptance of the revised terms and conditions. This provision may raise questions as to the certainty of the consumer contract. Users may not regularly monitor the Ring website for updated terms and conditions, and notification of material changes to the terms and conditions may be made through the Ring website[4] or some other means, rather than by a direct communication to the user.

2.1.3.3 Change to products or services

Another interesting provision of the Ring Terms of Service deals with changes to the 'Products' or 'Services'. The Terms provide that Ring may 'suspend or discontinue any part of the Services, or we may introduce new features or impose limits on certain features or restrict access to parts or all of the Products or Services'. This means that consumers may purchase the Products and Services and then find that they change without notice, or without there being any consumer recourse.

2.1.4 Data Storage and Use

Ring characterises its approach to privacy and security as 'defence-in-depth' – ensuring that protections are layered in a way that no one failure compromises the security of a system.[5] Where users have a 'Ring Protect' plan, Ring stores video recordings for a set period of time (in accordance with the user settings). Two step verification of accounts has been mandatory since 2020.[6] Ring encrypts communication between Ring devices and cloud storage (AWS – Amazon Web Services), both in transit and at rest. According to the Ring website:

[4] *Ring* (Website) < https://ring.com/au/en>.
[5] Ring, *End-to-End Encryption* (White Paper, January 2021) 3, n 2 <https://assets.ctfassets.net/a3peezndovsu/7bwgu7ybi1XoyH61pDraYT/94e4bab9347d4abe07f8d843fdfd4bd4/Ring_Encryption_Whitepaper_FINAL.pdf> ('*Ring White Paper*').
[6] Ibid.

Ring secures video recordings in transit and stores them on secure AWS servers. We use a combination of AES encryption (Advanced Encryption Standard) and TLS (Transport Layer Security) to secure data between Ring devices and AWS, and we encrypt data between Ring devices using AES encryption, TLS and SRTP (Secure Real Time Protocol).[7]

From January 2021, end-to-end encryption has been available as an option for users seeking additional security. This is provided as an option because the use of end-to-end encryption limits some user features and therefore requires a trade-off between security and product features.[8] The move to provide end-to-end encryption and implement two step verification may address concerns raised in 2019/2020 regarding the potential for Ring devices to be hacked due to the lack of encryption.

2.1.5 Software Updates

According to the Terms of Service, Ring may provide updates in their sole discretion. There is no specific requirement to provide updates; nor is there any requirement to provide notice to users of Ring products and services or obtain consent to such installation.

2.1.6 Consumer Protection Issues

2.1.6.1 Application of Australian Consumer Law

The consumer warranties provision is structured in a manner that may be difficult for the ordinary consumer to understand. First, the provision sets out the application of the *Australian Consumer Law* (*ACL*), then the section states that products and services are provided 'as is', followed by the explicit exclusion of certain warranties, and then concluding with the statement that the exclusions may not apply in accordance with applicable law. Such provisions rely on the consumer having a good understanding of their rights under applicable law, including the statutory guarantees under the *ACL*.

2.1.6.2 No warranty as to safety and availability

The Ring Terms of Service state that 'Ring makes no warranty or representation that use of the Products or Services will affect or increase any level of safety'. Ring states that the products and services are 'not intended to be 100% reliable and are not a substitute for a third-party monitored emergency notification system'. This may surprise consumers given that the Ring website makes statements such as 'Don't miss a thing', 'You'll never miss a moment at your front door', and 'Convenience and peace of mind are always at your fingertips whether you're home or away'.

[7] 'Your Privacy with Ring', *Ring* (Web Page) <https://support.ring.com/hc/en-us/articles/360043469371-Your-Privacy-with-Ring>.
[8] Ring, *Ring White Paper* (n 6).

2.2 Roomba Case Study

2.2.1 Product Overview

Roomba is a robot vacuum that is WiFi enabled, controlled by a mobile app and maps your house. The Roomba vacuum is available via the iRobot website or may be purchased in retail stores.

2.2.2 The Nest of Agreements

The purchase and use of Roomba products and services (including the mobile app) in Australia is governed by a suite of agreements including:

- IXL Home Terms and Conditions of Purchase[9] (accessed via iRobot Australia website)
- IXL Home Terms of Use (accessed via iRobot Australia website)
- iRobot Terms of Service (accepted via mobile app)
- iRobot End User Licensing Agreement (accepted via mobile app)
- iRobot Privacy Policy (acknowledged via mobile app)
- IXL Privacy Policy (accessed via iRobot website)
- App Store Terms of Service (Apple)
- Other additional guidelines, terms or rules, posted on the Services (site, web app or mobile app)

The number of agreements, and the overlap in terms and conditions between different documents, may create confusion for consumers. This situation arises partly due to the distribution arrangements for iRobot Roomba products in Australia, with IXL Home Pty Ltd operating as the exclusive local distributor with its own local IXL Terms and Conditions of Purchase and IXL Privacy Policy. However, the mobile application that controls Roomba products is provided by iRobot and, accordingly, is governed by the iRobot Terms of Service, iRobot End User Licensing Agreement (EULA) and the iRobot Privacy Policy, each of which is accepted or acknowledged via the mobile app. Each of the documents deal with a different aspect of the use of Roomba products and services (with some overlap) and it is unclear what the order of priority is with respect to the different documents. In addition, there are different provisions dealing with governing law, with the iRobot terms referring to either the laws of the US or the laws of Massachusetts, whereas the IXL Home Terms and Conditions refer to the laws of Victoria, Australia.

[9] 'IXL Home Terms and Conditions of Purchase', *ShopiRobot* (Web Page, 2022) <https://www.shopirobot.com.au/terms-and-conditions/>.

2.2.3 Contract Formation

2.2.3.1 Acceptance of terms and services

Users are deemed to agree to the iRobot Terms of Service upon setting up an account or accessing the Services.[10] Users are advised that if they do not agree to the iRobot Terms of Service, they should 'not browse or otherwise access or use the Services'.[11] While it may be possible to insist that users not use the mobile application if they do not agree to the iRobot Terms of Service, it seems impractical to suggest that users may not browse the Services, including the website Global iRobot,[12] or that users are deemed to have accepted the Terms of Service upon browsing or accessing the website. After all, in some cases, browsing the website is necessary to even locate the terms and conditions. Furthermore, the IXL Terms and Conditions of Purchase state that the user is required to read the terms before accessing or using the iRobot website, and that by agreeing to the IXL Terms and Conditions of Purchase, the user is also agreeing to the IXL Home Terms of Use.[13]

2.2.3.2 Updates to terms and conditions

The iRobot Terms of Service state that iRobot may update the terms from time to time and that continued use of the Service constitutes acceptance of the new terms. According to clause 18.2, the changes to the iRobot Terms of Service 'will usually occur because of new features being added to the Service, changes to the law or where we need to clarify our position on something'.[14] iRobot will provide notice of changes 'where possible and reasonable', either through the Service (such as the mobile application) or via email; however, urgent changes may be made without notice. While the iRobot Terms of Service provide a URL that should contain the current version of the Terms of Service, the current URL directs the user to a blank page. The iRobot Privacy Policy states that the policy may be updated from time to time and that the iRobot website will be amended to reflect the new version. The IXL Home Terms and Conditions of Purchase have similar provisions regarding updates to terms and conditions and advises users to review terms carefully before using the site or making new purchases.

[10] Service are defined as the Site (<global.irobot.com>), the Web App and Mobile Apps.
[11] 'iRobot Terms of Service', *iRobot* (Web Page, last updated 30 September 2016) s 2.2 <https://webapi.irobot.com/Legal/Documents/Asia-Pacific/Australia/Legal-Documents/Terms-of-Service.aspx?sc_lang=en-GB&utm_source=App&utm_campaign=App&utm_medium=App>.
[12] *Global iRobot* (Website) <www.global.irobot.com>.
[13] 'IXL Home Terms and Conditions of Purchase' (n 10).
[14] 'iRobot Terms of Service' (n 12) cl 18.2.

2.2.4 Data Storage and Use

The iRobot Terms of Service require that users create and use a 'strong' password with their accounts that involves a 'combination of upper and lower case letters, numbers and symbols'. Furthermore, users are advised that they are responsible for maintaining the secrecy of their log in credentials.

iRobot publishes information on data security on its website and advises that the company takes 'a defence-in-depth approach to security' with data encrypted in transit and at rest. iRobot also states that the company will:

> *… monitor and adhere to all supplier and industry alerts regarding security patches to systems and components used in our products. Additionally, we actively promote and sponsor private bug bounty programs and hacking events to … responsibly address any vulnerabilities that may be discovered.*[15]

All software updates are cryptographically signed to verify their authenticity. Despite the statements on the iRobot website regarding data security, both the iRobot Privacy Policy and the IXL Home Privacy Policy state that, while the companies will take steps to secure personal information, security systems may not be entirely secure and there are no guarantees as to the security of systems.

2.2.5 Software Updates and Changes to the Services

Both the iRobot Terms of Service and the iRobot EULA contain provisions dealing with software updates. The terms are broadly consistent and provide that iRobot may develop and install updates without additional notice or consent. Continued use of the products and services is deemed to constitute acceptance of the update, and of the terms and conditions. Should a user not want to accept the update, the iRobot Terms of Service state that the user should terminate their account and stop using the products and services. On the other hand, the iRobot EULA states that the user should not connect their product to the internet.

Furthermore, the iRobot Terms of Service advise that iRobot may make changes to the Services and that continued use of the Service will be deemed acceptance of any changes. Changes may include updates, resets, discontinued offerings or discontinued support for the services or any features. This means that consumers may purchase products and services and then find that they change without notice or recourse. The iRobot Terms of Service specifically state 'You agree that we will not be liable to you or to any third party for any change to the Services'.

[15] 'iRobot & Data Security', *iRobot* (Web Page) <https://webapi.irobot.com/Legal/Documents/Asia-Pacific/Australia/Legal-Documents/Data-Security.aspx?sc_lang=eu-GB>.

2.3 Google Nest Case Study

2.3.1 Product Overview

The Google Nest Hub is a home assistant device that can be purchased from Google or other retailers. The Nest Hub enables the user to watch online content, listen to music, control other smart devices, including online doorbells or cameras, and engage with Google Assistant. This case study was prepared based on purchase of a 'Google Nest Hub 2nd Generation'.

2.3.2 The Nest of Agreements

The purchase and use of the Google Nest Hub is governed by a number of documents:

- Google Terms of Service
- Google Nest Terms of Service
- Google Devices Terms of Sale
- Google Privacy Policy

The Google Nest Terms of Service will prevail in the event of any inconsistency with the terms set out in the Google Terms of Service. In addition to the terms referenced above, there are a number of policies published on the Google website that apply to use of the Google Nest Hub and associated services:

- Nest Commitment to Privacy in the Home
- Google Privacy and Security Principles
- Google Safety Centre
- Google Warranty Centre
- Google Privacy Notice for Audio Collection from Children's Features on Google Assistant

The use of multiple agreements, including material posted on various web pages, may result in consumer uncertainty as to the nature of the rights and obligations governing the use of the Google Nest Hub. There is some degree of overlap between the different terms and conditions and webpages; the only document that establishes any order of precedence is the Google Nest Terms of Service. The status of information published on web pages, including the ability of Google to change or update this information, is unclear, even where that information is cross-referenced in legal terms and conditions.

2.3.3 Contract Formation: Updates to Terms and Conditions

According to the Google Terms of Service, Google may update the Google Terms of Service or the Google Nest Terms of Service from time to time. Users will be provided with advanced notice of

'material changes', along with the 'opportunity to review the changes, except (1) when we launch a new service or feature, or (2) in urgent situations, such as preventing ongoing abuse or responding to legal requirements'.[16] Users are advised to remove their content and stop using the services in the event that they do not agree with the new terms. There is no discussion as to how non-material changes will be managed, or how Google will determine whether a change is 'material'.

Similarly, the Google Privacy Policy provides that Google has the right to make changes to the policy from time to time, although it also assures that Google '[w]ill not reduce your rights under this Privacy Policy without your explicit consent'.[17]

2.3.4 Privacy

The Google Privacy Policy emphasises the role of the user in controlling their privacy and their ability to manage privacy controls via a Google Account. Google provides a 'Privacy Check-Up' service that can assist with privacy settings. This places a significant burden on the consumer to understand how the Nest Hub works, and the kinds of information that may be collected and shared. In short, users are expected to be technologically savvy enough to know how to access and adjust the privacy controls. It should be noted that changing privacy settings or limiting the amount of information shared with Google may reduce the utility or functionality of products or services.

The Nest Commitment to Privacy in the Home positions Google as a guest that is 'invited' into the home. According to this document, the Google Nest Hub will only send audio to Google when the user interacts with Google Assistant, and a visual indicator will be displayed when data is being transmitted to Google. The main advice provided to users if they wish to avoid sharing data with Google is simply to turn the microphone off.

The Google Nest Terms of Service provides that the user is responsible for ensuring compliance with any laws relating to recordings, including that the user must obtain consent from any third parties. It provides that, 'You (and not Google) are responsible for ensuring that you comply with any applicable laws when you use Nest devices and services, including any video recording, biometric data or audio recording laws that require you to give notice or obtain consent from third parties relating to Nest Cam Audio/Video Data'.[18]

[16] 'Google Terms of Service', *Google* (Web Page, last updated 5 January 2022) <https://policies.google.com/terms?hl=en>.
[17] 'Google Privacy Policy', *Google* (Web Page, last update 10 February 2022) <https://policies.google.com/privacy?hl=en>.
[18] 'Nest Additional Terms of Service', *Google Support* (Web Page, last updated 28 February 2022) <https://support.google.com/product-documentation/answer/9327735?hl=en&ref_topic=10083519>.

2.3.5 Data Security

The Google Safety Center provides a wealth of publicly available information on security and privacy of Google products.[19] Users are advised that Google uses 'multiple layers of security, including leading encryption technology such as HTTPS and Transport Layer Security'. Google also uses other security features such as optional two step verification of accounts and notifications of logins from new devices. Similar to the approach taken to privacy, Google provides a number of tools for users to monitor security and provides a Security Check-Up. This places a burden on consumers to understand how to assess security impacts and implement advised security fixes.

Google publishes security information for products, including the Google Nest Hub. According to the Support Center, Google commits to release security updates for a minimum of five years from the first date of sale on the Google Store.[20] Furthermore, Google has products externally reviewed and validated by external third parties. For example, the Google Nest Hub has been reviewed by the NCC Group ioXt Validation lab against the ioXt Security pledge and the results of the review have been published online.[21]

Google provides monetary rewards and public recognition for security researchers who identify security vulnerabilities as part of its Google Vulnerability Reward Programme.[22]

2.3.6 Software Updates and Changes to Services

Both the Google Nest Terms of Service and the Google Terms of Service provide that software updates may be automatically installed without notice or consent. Under the Google Nest Terms of Service, users are advised that if they do not agree to an update, they should stop using the Nest device and services.

All software updates are cryptographically verified and Google uses 'Verified Boot' to determine whether the correct software is being used every time a device restarts.

Under the Google Terms of Service, Google commits to provide advance notice of 'material changes' that may negatively impact the use of services or if they stop offering a service. There are limited circumstances in which Google will not provide advance notice of a change, 'such as preventing abuse,

[19] See 'Security and Privacy', *Google Safety* (Web Page) <https://safety.google/security-privacy/>; 'Built-In Security', *Google Safety* (Web Page) <https://safety.google/security/built-in-protection/>; 'Authentication', *Google Safety* (Web Page) <https://safety.google/authentication/>.
[20] 'Security Updates and Security Validation Results for Google Nest Devices', *Google Support* (Web Page, 2022) <https://support.google.com/product-documentation/answer/10231940#>.
[21] Ibid.
[22] 'Bug Hunters', *Google* (Web Page) <bughunters.google.com>.

responding to legal requirements or addressing security and operability issues'.[23] The Terms of Service do not provide any details on how Google will determine whether a change is 'material'. Consumers may find that they have purchased products and services and then find that they have been changed without notice or recourse.

[23] 'Google Terms of Service' (n 17).

2.4 VTech Smartwatch Case Study

2.4.1 Product Overview

The VTech Smart Watch DX device is marketed to children as a wearable device that can be used to play games, take photos and record videos (these photos and videos can be uploaded to a computer). The watch is available from Australian retailers. The device is linked to an app called Learning Lodge that can be downloaded to a desktop computer or laptop. By connecting the device to the Learning Lodge App, users can download software to use on the watch, including games. Although downloaded software from the Learning Lodge App is not necessary for the watch to function, certain features advertised on the device packaging are dependent on software downloads.

2.4.2 The Nest of Agreements

There is significant complexity in relation to the agreements governing use of the VTech Australia website and VTech devices, particularly where this involves the download of software from Learning Lodge. Australian users of Learning Lodge software are bound by two Agreements: the VTech Australia Consolidated Terms and Conditions regarding the Learning Lodge for Installation and Use ('Vtech Australia Learning Lodge Terms')[24] and the VTech Australia Privacy Policy ('the Australian Agreements').[25] However, to install and use the Learning Lodge, users must accept to be bound by three further agreements with VTech Electronics Europe Plc: European Terms and Conditions on Installation and Use of Software; European Terms and Conditions of Account Registration; and the European Privacy Policy ('the European Agreements').[26]

2.4.3 Contract Formation

2.4.3.1 Acceptance of terms of service

The European Agreements require explicit assent through an 'I agree' checkbox prior to any download of the Learning Lodge Software but the position in relation to the Australian Agreements is more complex. The VTech Australia Learning Lodge Terms note that it will be necessary to explicitly agree to the terms and conditions of the agreement and 'below stated privacy policy of VTech' before using the Learning Lodge. The 'privacy policy' is referenced further, but the VTech Australia Privacy Policy is not hyperlinked to the page. In practice, the user only provides explicit assent to the terms of the

[24] 'Consolidated Terms and Conditions for Learning Lodge (Australia)', *VTech Electronics (Australia)* (Web Page, last updated 7 April 2016) <https://www.vtech.com.au/assets/data/terms_html/VTech-Consolidated_Terms_and_Conditions_for_Learning_Lodge_Australia.html>.
[25] 'Privacy Policy', *VTech Australia* (Web Page, last updated 17 March 2020) <https://www.vtech.com.au/privacy_policy>.
[26] On 31 March 2020, in response to an email enquiry, a customer service representative of VTech Australia confirmed that Australian products that use the Learning Lodge application are subject to European terms and conditions.

European Agreements. There is no explicit reference to the contracts from different jurisdictions on the website or in the agreements. This is likely to result in consumer uncertainty as to the nature of the arrangement into which they are entering.

The VTech Australia Learning Lodge Terms provide that the 'Terms and Conditions' may be updated by VTech from time to time and minor changes will be posted on the Australian website or the Learning Lodge. Notification of any 'material changes' will be made by email or through notification on the Learning Lodge App. 'Terms and Conditions' are defined as the VTech Australia Learning Lodge Terms; no reference is made to the European Agreements that consumers must accept before they download the Learning Lodge App. VTech further reserves the right to suspend or terminate use at any time and for any reason, without prior notification. This termination provision is also included in the European Terms and Conditions on Installation and Use of Software. Combined with the onus on the consumer to accept updates and software changes, the termination clause makes it difficult for consumers to understand the nature of the product and services that they are purchasing.

2.4.3.2 Forum and choice of law

The governing law and jurisdiction for the Australian Agreements is Victoria. For the European Agreements, the governing law and jurisdiction is England and Wales.

2.4.4 Data Storage and Use

The VTech Australia Privacy Policy and the European Privacy Policy note that locations processing the personal data of users can include Hong Kong, China and the US. To download any software it is necessary to become a registered user and agree to the European Privacy Policy. The European Privacy Policy provides that it protects data from 'accidental or deliberate manipulation, partial or complete loss, destruction, or unauthorised third-party access' using 'appropriate technical and administrative security' and 'security measures are being continuously improved in accordance with technological developments'.[27]

Both the Australian Privacy Policy and the European Policy recognise that the relevant VTech entities will process personal data of children but will endeavour not to do so without parental consent. However, both policies make unrealistic recommendations for children to adopt when they disclose personal information on the app. The European Agreements require assent by someone aged 18 or over but also contain a 'special note to children' that parental permission is required before children provide personal information when using VTech Services. Children are advised to seek guidance when

[27] 'Privacy Policy VTech', *Leap Frog* (Web Page, 24 May 2018) < https://www.leapfrog.com/en-gb/legal/vtech-privacy-policy/vtech-privacy-policy-uk>.

using VTech Services and are directed to not provide personal information without parental consent. The Australian Privacy Policy directs children to inform parents that personal information may be 'transferred to, and processed in, countries where laws may not provide your personal data with the same level of protection as Australia'. Both privacy policies contain a note to parents and/or guardians that urges families 'to follow common sense whenever disclosing personal information on our Website, via other VTech Services or anywhere else on the internet'.

2.4.5 Software Updates

The VTech Australia Learning Lodge Terms provide that there may be upgrades, updates and changes to the Learning Lodge from time to time, placing a heavy onus on the user to install those updates to avoid damage resulting from failure to accept advice to apply an update or the upgrade offered. Notification of changes, withdrawals, restrictions or rules regarding software programs will be given where material but the terms assert that VTech will not be liable for these changes. The European Terms and Conditions on Installation and Use of Software state that updates may be provided and users must follow instructions and download updates, disclaiming liability for loss or damage resulting from failure to follow instructions.

2.4.6 Consumer Protection Issues

2.4.6.1 Application of Australian Consumer Law

The website recognises the application of Australian consumer guarantees to goods and services supplied by VTech Electronics (Australia) Pty Ltd on a web page entitled Consumer Guarantees, which provides summarised information about those guarantees.[28] An Australian warranty is provided in the Device packaging. However, the Consumer Guarantees web page states that the warranties are limited to goods sold by authorised retailers (eBay is excluded) and they cannot be transferred. A consumer may incorrectly infer from this that consumer guarantees do not apply to these types of purchases.

2.4.6.2 Security

Despite assurances about vigilance in data protection in the European Privacy Policy, and a statement of compliance with the *Data Protection Act 1998* (UK) in the European Terms and Conditions of Account Registration, the latter agreement provides that VTech shall not be liable if 'the Learning Lodge and/or other software applications the Learning Lodge provides access to or any related

[28] 'Consumer Guarantees', *VTech Australia* (Web Page) <https://www.vtech.com.au/consumerguarantees>.

services suffer an outage, corruption, attack, virus, interference, hacking, intrusion, data loss, theft or unlawful removal, or any other loss, damage, compromise or impairment'.

2.5 August Smart Lock Pro Case Study

2.5.1 Product Overview

August Smart Lock Pro is a lock control device that permits control over a door lock using Bluetooth technology. It also permits users to tell if their door is locked and track activity with the mobile app. Additional technology means that the door lock can be controlled by Alexa, Siri or the Google Assistant. In Australia, customers can import the August Smart Lock products through Amazon from US-based sellers, pursuant to the Amazon Global Store Conditions of Sale that apply to US Imports. The August Terms of Service provide that the August Services include the August website, the App, all related software provided by August, together with services provided via the site.[29]

2.5.2 The Nest of Agreements

The use of the August Smart Lock Pro is governed by the August End User Agreement, which is specifically identified as a legal agreement between August and the User.[30] The August End User Agreement explicitly incorporates the hyperlinked August Privacy Policy[31] and August Terms of Service. The August End User Agreement further references requirements for the user to abide by 'documentation provided to you in connection with the Device, Licensed Software, Application and Account'. In addition to the Terms of Service and Privacy policies, the webpage displaying the August End User Agreement hyperlinks other August Policies and Agreements, namely the Cookie Policy, Warranty, AVR (August Video Recording) and Terms Notices. The August Warranty page provides a limited warranty that is only available for Devices purchased and delivered to the end user in the US and Canada.[32] The use of multiple documents, including material posted on various web pages, may result in consumer uncertainty as to the nature of the arrangement they are entering into with August. The complexity of these agreements, separation of software and hardware rights, and requirements to comply with third party licensing terms impose onerous obligations on users.

2.5.3 Contract Formation: Acceptance of Terms of Service

The Smart Lock hardware cannot function without access to services provided through the August app and the August website. After purchase, users click 'I agree' on the August app or website and enter into a limited licence for 'personal non-commercial purposes in order to operate the device'. Only users of the August Smart Lock Pro who purchase and receive the device in the US or Canada can

[29] 'August Terms of Service', *August* (Web Page) <https://august.com/pages/terms-of-service>.
[30] 'August End User Agreement', *August* (Web Page) <https://august.com/pages/end-user-agreement>.
[31] 'August Privacy Policy', *August* (Web Page, 24 July 2020) <https://august.com/pages/privacy-policy-july-24-2020>.
[32] 'August Warranty', *August* (Web Page) <https://august.com/pages/warranty>.

return the hardware for a refund if they are unhappy with the August End Use Agreement within 30 days. Problematically for Australian users, no additional Australia-specific warranty is provided to Australian purchasers who use the Amazon Global Store and are unhappy with agreement terms.

Furthermore, the August End User Agreement provides that the terms and conditions may be modified by August from time to time, with only 'material changes' (as determined by August) notified to the user through publication on the website or direct communication. The modifications take effect following the user clicking 'I agree' or on the 30th day following notice of the modifications. This provision raises questions as to the certainty of the consumer contract. There is a heavy onus on users to continue to check the website for notices of material changes to terms and conditions, as notification of material changes to the terms and conditions may be by the website or some other means rather than a direct communication to the user.

2.5.4 Data Storage and Use

The supplier of the August Smart Lock Pro is not located in Australia and it is highly unlikely that data from the device would be stored in Australia. The August Privacy Policy specifies that Californian residents are entitled to rights in relation to personal data and its erasure and the sale of personal information. Although specific reference is made to UK and EU privacy regulation for users in those jurisdictions, no reference is made to Australia.

The information that is automatically collected by the August Smart Lock Pro includes lists of contacts invited to use the device, as well as information about usage of the device. The August Privacy Policy notes that August and its service providers store the majority of website and other collected information in the US, where August is based. The August Privacy Policy provides that August collects '[P]ersonal Information (including telephone numbers and email addresses) about other people who have access to your Products', such as other family members, guests, and service providers like gardeners, house cleaners and/or others (known as 'Invitees'). This data can be highly sensitive to the individual. Users who choose the Auto-Unlock function need to give consent to the App to track their location. This information is stored on the device, not on August servers. Users can delete or change information in their registration profile using the website or app, but Invitees can only remove information about themselves if the product owner requests it. Deletion or modification requests are dealt with 'as soon as practical, but some information may remain in archived/backup copies for our records or as otherwise required by law'.

2.5.5 Software Updates

The August End User Agreement places significant onus on the user to accept ongoing software updates. Ongoing use indicates consent to the updates, and failure to install them may expose the user to security risks and functionality problems. As it is not possible to use the hardware without the software, this makes it difficult for a user to reject changes without suffering the loss of the use of the device. Although August permits return of the device for customers who purchase it in Canada or the US, this is only for 30 days after purchase, so it is unlikely to address any concerns that unwanted updates may pose. The August End User Agreement states that users who do not accept software updates may be exposed to security risks or be provided with limited services.

2.5.6 Consumer Protection Issues

There is no other explicit recognition of Australian consumer guarantees in any of the documentation provided on the August website and there is no place of business for August in Australia. Amazon Global Store Conditions of Sale (Amazon GSCS) provide that its terms are not intended to exclude, restrict or modify *Australian Consumer Law*; yet determining how the Australian consumer guarantees apply to a purchaser is likely to be complex for the consumer. There may be complications related to the fact that the product is not designed for an Australian market, and this may influence an assessment of the guarantees of acceptable quality or fitness for purpose. The Amazon GSCS provide that the purchaser of goods from the Global Store is the importer.

2.5.6.1 No warranty as to safety and availability

The August End User Agreement disclaims warranties for use of the Licenced Software to the maximum extent permitted by law, expressly providing that 'August does not warrant that use of the licensed software will be uninterrupted or error-free, compatible with your home network, computer or mobile device, that defects will be corrected, or that the licensed software is free of malware, viruses or other harmful components'. The agreement then purports to limit any remedies allowable by law to 90 days from download or where limitations on warranties are permitted.

2.5.7 Security

August encourages the disclosure of vulnerabilities, particularly by security researchers. Its Security Center provides Reporting Guidelines and encourages the disclosure of vulnerabilities in exchange for credit and public acknowledgement of researchers who privately notify and work with August to coordinate a public announcement 'after a fix or patch has been developed and tested', consistent with 'industry best practices'. The policy discourages 'premature' disclosure of vulnerabilities.[33]

[33] 'Security Center', *August* (Web Page) <https://august.com/pages/security-center>.

2.6 Tapo Smart Light Bulb Case Study

2.6.1 Product Overview

The Tapo Smart Light Bulb allows users to control their lights remotely. They can use the Tapo App to turn lights on and off or set lights to be on at certain times. It is possible to control the device using the Tapo app or in conjunction with Google Assistant and Alexa. The device is sold by mainstream Australian retailers. Smart Light Bulbs are frequently identified as an example of home IoT devices that can benefit vulnerable individuals. The remote use feature of the Tapo Light Bulb can have great utility for users with mobility issues; however, these users are also very vulnerable to the impact of device failure.

2.6.2 The Nest of Agreements

The Tapo User Agreement and Tapo Privacy Policy are available on the Australian web page.[34] Users must accept both agreements so that they can use the Tapo app, thereby entering into agreements with TP-Link Corporation Limited. Services associated with the Tapo Smart Light Bulb ('Tapo Services') can be used in conjunction with the Tapo Smart Light Bulb hardware and in other ways. Tapo Services include the Tapo websites and technical support and services that are accessible through the sites, as well as mobile app software and subscription services that can be accessed using the Web Apps and Mobile Apps.

2.6.3 Contract Formation

2.6.3.1 Acceptance of terms of service

Users must agree to the Tapo User Agreement and the Tapo Privacy Policy when they download the Tapo app that is used to remotely control the device. Use of Tapo Services is not possible if the terms of both agreements are not accepted by the user. Although the Tapo User Agreement and Tapo Privacy Policy are available on the Tapo website and can be accessed prior to use, the Tapo Limited Warranty terms that are included with the device are not available on the Tapo Website prior to purchase. The device purchased for this research was sold in shrink-wrapped packaging that stated that the warranty length was two years but did not reference any other warranty conditions. The QR

[34] 'Privacy and Terms of Use', *Tapo* (Web Page, 24 July 2019) <https://www.tapo.com/au/privacy/#terms-of-use>.

code that the packaging indicated was linked to information about the warranty conditions did not actually link to the Limited Warranty terms.

2.6.4 Data Storage and Use

There is no reference to Australian legal standards or security information in the Tapo User Agreement or the Tapo Privacy Policy. The Tapo Privacy Policy references GDPR standards, including the right to make a complaint to the UK Information Commissioner's Office (ICO). User data is held in accordance with TP-Link's retention policy 'which is available on request'. Information about users can be used by affiliated companies. The contract provides that users provide data by consent; however, it is not possible to use the Tapo Services if terms are not accepted, and therefore consumers are forced to consent to use of data. Users are informed that their personal data may be used by third parties for the purposes of direct marketing, but consent for the use of personal data for marketing at any time can be withdrawn by contacting an email address.

2.6.5 Software Updates

Any use of the Tapo Services following changes to the terms of use is stated to be 'deemed as irrevocable acceptance' of any updates to those terms. Unilateral changes to Tapo Services can occur at any time, including permanent modification, suspension, discontinuance or restrictions of access to all Tapo Services, and changes to services that can render hardware devices, third party services, configurations or software setups inoperable. The changes can be made at TP-Link's sole discretion, with or without notice by email or website announcement. Updates may also be provided and installed automatically without notice or consent. The sole recourse for a consumer not agreeing to automatic software updates is to terminate the account and stop using the software and products.

2.6.6 Consumer Protection Issues

2.6.6.1 Application of Australian Consumer Law

The Tapo Limited Warranty states that the benefits it provides are 'in addition to other rights and remedies provided under Australian and New Zealand law'. It further states that 'goods come with guarantees that cannot be excluded under the *Australian Consumer Law*'. Such provisions rely on the consumer having a good understanding of their rights under applicable law, including the statutory guarantees under the *ACL*. The separate Tapo Terms of Use provide that, with the exception of warranties provided with the device, Tapo Services are 'provided 'as is' and 'as available' without warranties of any kind, either express or implied. All warranties are disclaimed 'to the fullest extent permissible pursuant to applicable law', including 'implied warranties of merchantability, fitness for a particular purpose, and non-infringement'. The Terms of Use specifically provide no warranty that 'the

functions contained in the services will be available, uninterrupted or error-free, that defects will be corrected, or that the services or the servers that make the services available are free of viruses or other harmful components'.

2.6.7 Unilateral Suspension of Tapo Services without Notice

The Tapo User Agreement provides that TP-Link 'may temporarily or permanently modify, suspend, discontinue, or restrict access to all or part of the Services and/or any related software, facilities, and services, with or without notice and/or to establish general guidelines and limitations on their use'. This means that consumers may purchase the device with the expectation of being able to use the Tapo Services and then find that their availability changes without notice or any recourse, and potentially become inoperable. The Tapo Terms of Use provide that termination of Tapo Services may occur without advance notice 'for any reason, but usually because it would be impractical, illegal, not in the interest of someone's safety or security, or otherwise harmful to the rights or property of TP-Link'.

2.6.8 Security

The user is responsible for the security of any username and password; TP-Link reserves its entitlement to monitor the password, require users to change the password and terminate users if they do not comply with requests to change their passwords. The Terms of Use provide 'TP-Link cannot guarantee that unauthorized third parties will never be able to defeat our security measures or use your personal information for improper purposes'. Users are required to provide personal information at their own risk and agree 'to immediately notify TP-Link of any unauthorized use, or suspected unauthorized use, of your account or any other breach of security of which you become aware'. TP-Link excludes liability for any loss or damage resulting from failure to provide this notification.

Conclusion

The case studies set out in this Part of the Report, while each raising some distinct issues, generally reinforce the analysis of the challenges posed by CIoT devices to the law identified in Part 1 of the Report. Consumers purchasing CIoT devices are usually faced with a complex nest of contracts and associated information, which are often difficult to locate and understand. The relationships between the nests of agreements are not always clear and there are sometimes inconsistencies. Many of the agreements are not specifically tailored to Australian circumstances and, even where they are, there is commonly reference to foreign laws. In many instances, it is inordinately difficult to access terms and conditions before entering into the relevant contracts. In some cases, the agreements make reference to other documents that are not accessible by links. Moreover, it is common for the agreements to provide for variation of the terms and conditions without sufficient notice to consumers, and sometimes on the basis that continued use of a device amounts to agreement to a variation.

While security policies apply to all of the devices in the case studies, there is considerable inconsistency between the policies. In the absence of baseline standards, this level of inconsistency can contribute to consumer confusion. All of the agreements make provision for software updates, as they must. But this commonly allows for unilateral modification, often without notice to the consumer, and with continued use constituting consent to the modifications. The only recourse for consumers who are unhappy with the updates is commonly to terminate an account and cease using the product.

Privacy policies for the CIoT devices in the case studies commonly place most responsibility for protecting privacy on consumers. In general, the privacy policies are not designed specifically for Australian privacy law, and sometimes reference foreign laws, particularly the GDPR. However, there is considerable diversity in privacy policies and standards. Similarly, there is a diversity of approaches to consumer warranties, with many consumer agreements not referencing the mandatory guarantees under the *ACL*, and some attempting to limit the guarantees to the extent possible. The ways that consumer warranties are dealt with in the majority of contracts can give rise to considerable uncertainty by consumers about their rights. Finally, given the complexities of the nest of consumer contracts, coupled with the extent to which the agreements involve international parties, there are underlying uncertainties about the liability of entities involved with the supply of CIoT products, and these are certainly not resolved by the contracts that were reviewed for the case studies presented in this Part of the Report.

The next sections of the Report, which analyse the implications of the analysis of the challenges posed by CIoT devices for three specific areas of law and regulation, take up most of the issues raised by the case studies, focusing on those that this project has identified as the most important. As pointed out in the Introduction to this Report, however, it has not been possible for this project to address every legal issue raised by CIoT, including those raised by the case studies. This does not mean that these issues are unimportant; simply that a project of this scope must concentrate on prioritising analysis of those gaps and weaknesses in current law and regulation that are the most significant, and on making recommendations for reform that are likely to have the most impact in improving the protection of consumers of CIoT devices.

3 Cyber Security and CIoT Devices

Introduction

There are two main sections to Part 3 of the Report: the first focuses on the role of regulation in promoting the security of CIoT devices, while the second addresses the potential for labelling schemes to improve device security.

The first section sets out the current state of play in regulating the security of CIoT devices, focusing on policy developments in Australia and the UK. It then makes recommendations for improving the regulation of the security of CIoT devices and explains the reasons for the recommendations. In summary, the Report recommends introducing legislation to mandate security standards for CIoT devices. Drawing from recent UK legislation,[1] the Report includes recommendations relating to the essential elements of a proposed regulatory regime, including minimum standards, statutory duties and enforcement. This section of the Report concludes by pointing to the importance of placing the regulation of the security of CIoT devices within the broader context of regulatory initiatives to enhance cyber security, including the recent critical infrastructure reforms.

The second section introduces CIoT security labelling schemes, focusing on two existing schemes that have been implemented in Singapore and Finland. Following that, this section makes recommendations for introducing a labelling scheme in Australia and explains the reasons for the recommendations. In summary, the Report recommends introducing a mandatory security labelling scheme, together with provision for monitoring and auditing of CIoT devices and sanctions for non-compliance.

3.1 Regulation of CIoT Security

This section introduces current issues in the regulation of CIoT security, firstly by explaining relevant global policy developments and secondly, by introducing the UK policy process, which has culminated in legislation mandating minimum security standards for CIoT devices. The Australian policy process, including the adoption of a voluntary Code of Practice and proposals for mandating minimum standards, is then introduced. Following that, the policy background to the UK legislation is introduced before the main elements of the legislation are explained. This section concludes with an analysis of

[1] The Product Security and Telecommunications Infrastructure Bill 2021 was introduced to the UK Parliament in November 2021 and is expected to be passed in November 2022.

the main current policy issues in the regulation of CIoT device security and of how the regulation of CIoT devices fits within the broader context of cybersecurity regulation.

Before turning to these issues, it is important to point out that most CIoT device suppliers have their own security policies. One example is the Google Nest Hub, which has adopted the ioXT Security Pledge and is explained in the following case study. The case study provides a good introduction to the issues that must be addressed by a CIoT security policy.

CASE STUDY: Google Nest Hub

Google publishes information on security and engages third parties in testing and validating the security of Google devices. The Google Nest Hub has been reviewed by the NCC Group ioXt Validation lab against the ioXt ('Internet of Secure Things') Security Pledge and Google has published the full report online.[2]

The ioXt Security Pledge[3] *has eight principles:*

1. No universal passwords: The product shall not have a universal password; unique security credentials will be required for operation.

2. Secured interfaces: All product interfaces shall be appropriately secured by the manufacturer.

3. Proven cryptography: Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.

4. Security by default: Product security shall be appropriately enabled by default by the manufacturer.

5. Signed software updates: The product shall only support signed software updates.

6. Automatically applied updates: The manufacturer shall act quickly to apply timely security updates.

7. Vulnerability reporting program: The manufacturer shall implement a vulnerability reporting program, which shall be addressed in a timely manner.

8. Security expiration date: The manufacturer shall be transparent about the period of time that security updates will be provided.

[2] 'Security Updates and Third-Party Assessments for Google Nest Devices', *Google Support* (Web Page, 2022) <https://support.google.com/product-documentation/answer/10231940#>.
[3] 'ioXt Security Pledge: The Global Standard for IoT Security', *ioXt* (Web Page, 2021) <https://www.ioxtalliance.org/the-pledge>.

3.1.1 Global Developments

Given the importance of securing IoT devices, the first steps in CIoT-specific regulation have unsurprisingly been aimed at enhancing security. To date, other than standard-setting activities, such as those of the International Organization for Standardization (ISO)[4] that have a technical focus, there have been few genuinely international initiatives. However, in July 2019, the 'Five Eyes' countries – Australia, Canada, New Zealand, the UK and the US – issued a joint communiqué that affirmed an intention to promote 'security by design' in IoT devices by the respective governments collaborating with industry and standards bodies.[5]

Apart from government initiatives, in February 2022, the World Economic Forum (WEF) in consultation with Consumers International, the Cyber Tech Accord and I Am the Cavalry, released a *Statement of Support* that represented a multi-stakeholder consensus on five CIoT security essentials or principles.[6] The consensus resulted from expert analysis of over 100 standards, specifications and guidelines, and it sets out the following five 'must haves': no universal default passwords; implementing a vulnerability disclosure policy; keeping software updated; securely communicating; and ensuring that personal data is secure.[7] This Report returns to the principles (at 3.1.6) after an explanation of the UK and Australian policy process.

3.1.2 UK Developments

As the approach taken to regulating the security of CIoT devices in Australia has been influenced by developments in the UK, this provides necessary context for understanding the Australian policy process. After a policy development process, which included input from the National Cyber Security Centre (NCSC), the UK first introduced a voluntary code of practice for CIoT security in October 2018.[8] The UK Code incorporated 13 security principles, arranged in order of importance. The security principles can be summarised as follows:

---

[4] See, for example, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Internet of Things (IoT) – Reference Architecture* (Standard No ISO/IEC 30141:2018(en), 2018) <https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en>.

[5] Five Country Ministerial Communiqué, 'Statement of Intent Regarding the Security of the Internet of Things', *GOV.UK* (Web Page, 29-31 July 2019, updated 23 October 2019) <https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things>.

[6] See Lisa Chamberlain, 'Global Consensus Emerges to Secure Internet-Connected Home and Wearable Devices', *World Economic Forum Blog* (Blog Post, 15 February 2022) <https://www.weforum.org/press/2022/02/global-consensus-emerges-to-secure-internet-connected-home-and-wearable-devices/>.

[7] World Economic Forum, with Consumers International, Cybersecurity Tech Accord and I Am the Cavalry, *Joint Statement of Support on Consumer IoT Device Security: Industry, Hackers, and Consumers for a Global Baseline for Consumer IoT Security* (Consensus Statement, 15 February 2022) <https://cybertechaccord.org/industry-hackers-and-consumers-for-a-global-baseline-for-consumer-iot-security/>.

[8] Department for Digital, Culture, Media & Sport (UK), *Code of Practice for Consumer IoT Security* (Guidelines, 14 October 2018) <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>.

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security sensitive data
5. Communicate securely
6. Minimise exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is protected
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

Following a further review of the CIoT security framework, in April 2021, the UK Government announced that it would introduce legislation to regulate the security of consumer connected products, such as smart speakers, smart televisions, connected doorbells and smartphones.[9] In November 2021, the UK Government introduced legislation known as the Product Security and Telecommunications Infrastructure Bill 2021 (the 'PSTI Bill') to implement the April 2021 decision. This Report analyses the background to the Bill and the Bill itself, following an introduction to the Australian policy developments. At the time of writing this Report, it was expected that the PSTI Bill would be enacted later in 2022.

Meanwhile, the UK Government published a table mapping the voluntary Code's guidelines against other national and international guidance and regulations relating to IoT security.[10] The table, like the expert analysis undertaken by the WEF, indicated considerable international alignment of the basic CIoT security principles but with some differences in implementation or recommended implementation. In October 2021, this project was re-oriented to map global CIoT security and privacy standards to the European Telecommunications Standards Institute (ETSI) standard for the *Cyber Security for Consumer Internet of Things: Baseline Requirements* (EN 303 645), which has arguably

[9] Department for Digital, Culture, Media & Sport (UK), *Government Response to the Call for Views on C*onsumer *Connected P*rod*uct Cyber S*ecurity *L*egislation (Policy Paper, 21 April 2021) <https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation> ('*DDCMS Policy Paper*').
[10] 'Mapping Security & Privacy in the Internet of Things', *Copper Horse* (Website, 3 October 2021) <https://iotsecuritymapping.uk/>.

become a de facto global standard.[11] The project, which is maintained by Copper Horse Ltd on behalf of the UK Department for Digital, Culture, Media & Sport (DDCMS), is an important resource for keeping track of CIoT security recommendations and standards.

3.1.3 Regulation of CIoT Security in Australia

The Australian response to securing CIoT devices has been developed through the overarching framework of the national Cyber Security Strategy, which was first established in 2016 and replaced by an updated strategy in 2020.[12] In December 2019, the Australian Government initiated a consultation on a voluntary draft Code of Practice for CIoT devices.[13] Following the consultation, in September 2020, the Government released the final version of the Code of Practice without change to the principles.[14] The Australian code essentially adopted the 13 principles from the UK Code of Practice but with some changes, including changes in the wording and ordering of the principles; the consultation document expressly indicating that it 'builds upon' the UK guidelines.[15]

The 13 security principles in the Australian code of practice can be summarised as follows:

1. No duplicated default or weak passwords
2. Implement a vulnerability disclosure policy
3. Keep software securely updated
4. Securely store credentials
5. Ensure that personal data is protected
6. Minimise exposed attack surfaces
7. Ensure communication security
8. Ensure software integrity
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy

[11] Ibid.
[12] Department of the Prime Minister and Cabinet (Cth), *Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity* (Report, 21 April 2016) <https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf>; Department of Home Affairs (Cth), *Australia's Cyber Security S*trategy 2020 (Report, 6 August 2020) <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>.
[13] Department of Home Affairs, Australian Signals Directorate and Australian Cyber Security Centre (Cth), *Securing the Internet of Things for Consumers: Draft Code of Practice* (Guidelines, December 2019) <https://www.iot.org.au/wp/wp-content/uploads/2019/11/19.11.2019-DRAFT-Voluntary-Internet-of-Things-Code-Of-Practice.pdf>.
[14] Department of Home Affairs, Australian Signals Directorate and Australian Cyber Security Centre (Cth), *Code of Practice: Securing the Internet of Things for Consumers* (Guidelines, September 2020) <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>.
[15] Ibid 2.

13. Validate input data

As part of *Australia's Cyber Security Strategy 2020,* in July 2021, the Government commenced consultations on options for regulatory reforms and voluntary incentives to strengthen cyber security based on a Discussion Paper (DP) prepared by the Department of Home Affairs.[16] The DP included options for setting cyber security expectations, increasing transparency and protecting consumer rights, including for smart IoT devices. Importantly, the DP reported on government qualitative research on industry uptake of the voluntary code, which found that:

- Many firms are aware of the Code of Practice but found it difficult to implement high-level principles.
- While all participants stated a commitment to strong cyber security, many had not yet implemented a vulnerability disclosure policy, which is one of the low cost, high priority elements of the Code of Practice.
- Products sold at the lower end of the market can have less reputation to protect and thus less incentive for high cyber security.[17]

Following from this research, the DP identified two options for implementing cyber security standards in Australia: maintain the status quo based on the voluntary Code of Practice; or introduce a mandatory product standard for smart devices.[18] In relation to the possible mandatory standard, the DP proposed adopting ETSI EN 303 645, and mandating compliance with either the whole of the standard or, following the UK, the top three requirements. While the DP pointed to challenges in implementing a mandatory code, including the difficulty of controlling imports of insecure devices, it observed that the benefits could outweigh the costs.[19]

The DP also canvassed options for introducing labelling for smart devices, which are introduced and analysed in the second section of this part of the Report.

3.1.4 Policy Background to the UK PSTI Bill

This section of the Report explains the specific policy developments in the UK that resulted in legislation mandating minimum security standards for connected CIoT devices.

[16] Department of Home Affairs (Cth), *Strengthening Australia's Cyber Security Regulations and Incentives: A Call for Views* (Discussion Paper, 13 July 2021) <https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf> ('*Department of Home Affairs Discussion Paper*').
[17] Ibid 31.
[18] Ibid 32–33.
[19] Ibid 33–34.

In May 2019, the UK Government first initiated a public consultation on regulatory options for making aspects of the UK voluntary code legally enforceable.[20] The consultation indicated that the increase in threats associated with the growth of consumer IoT resulted in an 'urgent need' for security safeguards set out in the voluntary Code to be mandated.[21] However, on the basis that implementing the 13 guidelines in the UK Code in full would dampen innovation, the UK Government expressed a preference for mandating the top three principles in the Code and the ETSI standard, as these were the most important security requirements.[22] Following further consultation on regulatory proposals launched in July 2020, in April 2021, the UK Government announced it would introduce legislation that would adopt a 'proportionate' approach to regulation and that would mandate security requirements aligning with the top three guidelines of the UK Code. In support of this decision, the announcement noted that:

> *… aspects of industry still persist in using out-of-date and dangerous practices (such as universal default passwords), and the risk to consumers can no longer be tolerated. Our proposed legislation will further close the door on insecure technology.*[23]

The announcement also indicated that an 'enforcement authority' would be responsible for investigating non-compliance and for applying corrective measures, sanctions and potentially criminal proceedings.

In November 2021, the PSTI Bill was introduced to the House of Commons. In accordance with the April 2021 announcement, the Bill introduces mandatory security standards for 'connected devices'; it is explained and analysed immediately below. At the time of writing, the Bill remains before the UK Parliament but is expected to be enacted later in 2022.

3.1.5 Product Security and Telecommunications Infrastructure Bill 2021 (UK)

Part I of the PSTI Bill establishes a regulatory framework for the security of connected devices, while Part II is intended to support the UK Electronic Communications Code[24] by introducing measures to enhance the development of digital telecommunications infrastructure. More specifically, Part I establishes an enforceable regulatory regime imposing minimum security obligations on

[20] Department for Digital, Culture, Media & Sport (UK), *Consultation on the Government's Regulatory Proposals Regarding Consumer Internet of Things (IoT) Security* (Report, 1 May 2019) <https://www.iotjournaal.nl/wp-content/uploads/2019/05/Consultation_on_the_Government_s_regulatory_proposals_regarding_consumer_Internet_of_Things_security.pdf>.
[21] Ibid 14.
[22] Ibid 7, 11.
[23] *DDCMS Policy Paper* (n 9).
[24] The Electronic Communications Code is set out in sch 3 of the *Communications Act 2003* (UK). It includes a set of rights that are designed to facilitate the installation and maintenance of electronic communications networks.

manufacturers, importers and distributors of connectable devices. Reflecting the evolving nature of IoT technologies, the Bill leaves most details, including the security requirements, to be determined by delegated legislation in the form of regulations. Until the regulations are drafted, it is impossible to have a complete picture of the UK regulatory regime.

Clause 1 of the Bill provides the Secretary of State for the DDCMS with the power to make regulations specifying security requirements to protect or enhance the security of connectable products and users of connectable products. Initially, as signalled by the earlier policy announcements, the mandatory requirements will be confined to the top three obligations in the UK Code and the ETSI standard, namely:

- **Security Requirement 1:** Ban universal default passwords
- **Security Requirement 2:** Implement a means to manage reports of security vulnerabilities
- **Security Requirement 3:** Provide transparency about the length of time for which a product will receive security updates. [25]

3.1.5.1 Scope of the UK PSTI Bill: 'Connectable products'

The security requirements must relate to consumer 'connectable products' of manufacturers, importers or distributors. Under clause 4 of the PSTI Bill, a 'relevant connectable product' is either an 'internet-connectable product' or a 'network-connectable product'. While an 'internet-connectable product' is simply a product that is capable of connecting to the internet, a 'network-connectable product' is a more complex concept, but is essentially a product that is capable of connecting to an 'internet-connected product'.[26] The security requirements will therefore apply to products such as: smartphones; connected cameras, TVs and speakers; connected children's toys and baby monitors; connected safety-relevant products such as smoke detectors and door locks; IoT base stations and hubs to which multiple devices connect; wearable connected fitness trackers; outdoor leisure products, such as handheld connected GPS devices that are not wearables; connected home automation and alarm systems; connected appliances, such as washing machines and fridges; and smart home assistants.[27] The Secretary of State, however, has the ability to designate excepted

[25] Explanatory Notes to the Product Security and Telecommunications Infrastructure Bill (UK) (Bill 199-EN) [19] ('PSTI Bill Explanatory Notes').
[26] Product Security and Telecommunications Infrastructure Bill (UK) cl 5 ('PTSI Bill').
[27] Department for Digital, Culture, Media & Sport (UK), *The Product Security and Telecommunications Infrastructure (PTSI) Bill – Product Security Factsheet* (Factsheet, 24 November 2021, updated 1 December 2021) <https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet>.

products, which will include products that might otherwise be subject to double regulation, such as smart metering devices, medical devices and road vehicles.[28]

Chapter 2 of the Bill sets out a number of statutory duties that apply to manufacturers, importers and distributors primarily in relation to 'UK Consumer Connectable Products' (UK CCP). Under clause 54, a connectable product is a UK CCP if either of the following two conditions are satisfied:

- the product is or has been made available to consumers in the UK; or
- the product is or has been made available in the UK to customers who are not consumers (that is, businesses) where identical products are or have been made available to consumers in the UK.

The second condition is intended to ensure that minimum security requirements apply to all products that might be expected to be used by consumers in the UK.

3.1.5.2 Statutory duties

In broad terms, the main duties that apply to manufacturers, importers and distributors of consumer connectable products are as follows:

- duty to comply with relevant security requirements; and
- duty not to make a product available in the UK without either a statement of compliance or a summary of a statement of compliance.

Manufacturers and importers of consumer connectable products also have the following important duties:

- duty to investigate potential compliance failures; and
- duty to maintain records of investigations of compliance failures.

However, the precise duties and the conditions for the duties to apply vary depending upon whether the relevant person is a manufacturer, importer or distributor. The statutory duties and the conditions for the duties to apply in relation to each category of relevant person, are summarised in Figure 1 and Table 1 below.

[28] PSTI Bill Explanatory Notes (n 25) [51].

Figure 1 Duties of Manufacturers, Importers and Distributors under Product Security and Telecommunications Infrastructure Bill 2021 (UK)

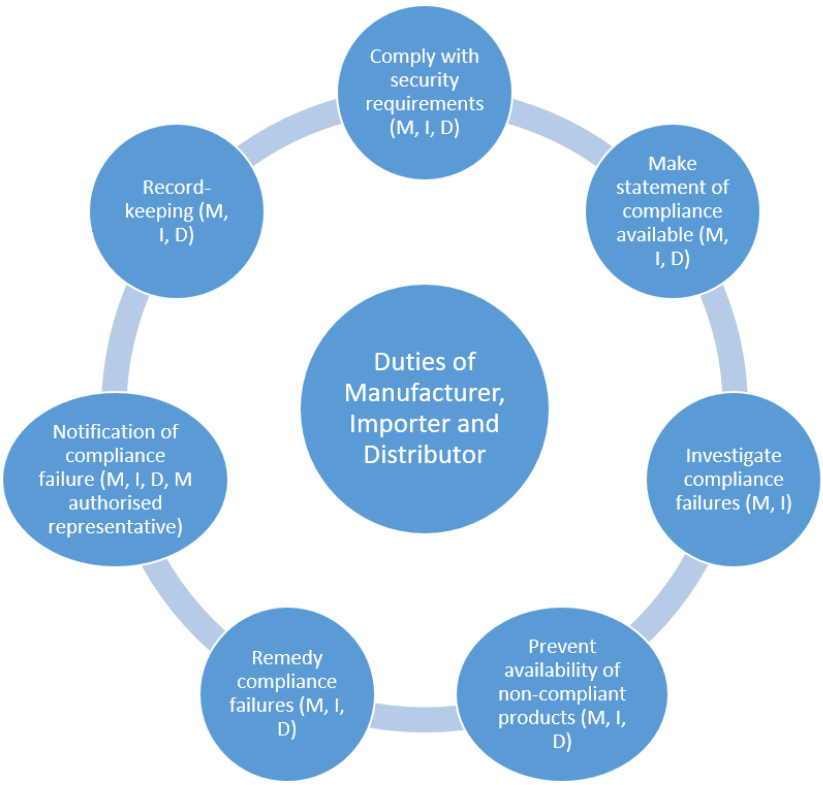


Table 1 Duties under the Product Security and Telecommunications Infrastructure Bill 2021 (UK)

Relevant Person	Statutory Duty	Conditions for Duty to Apply
Manufacturer	Duty to comply with relevant security requirements	• Manufacturer intends product to be a UK CCP, or is aware, or ought to be aware, that the product will be a UK CCP; or • Product is a UK CCP and, at the time it was made available, the above condition was satisfied
	Duty not to make a relevant connectable product available in the UK without a statement of compliance or a summary of the statement of compliance in prescribed form	• Manufacturer intends product to be a UK CCP, or is aware, or ought to be aware, that the product will be a UK CCP
	Duty to take all reasonable steps to investigate whether there is a compliance failure	After a relevant connectable product has been made available in the UK:

Relevant Person	Statutory Duty	Conditions for Duty to Apply
		• Manufacturer is informed that there is or may be a compliance failure; and • Manufacturer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty, as soon as practicable, to take all reasonable steps to: • Prevent product from being made available to customers in the UK; and • Remedy compliance failure	• Manufacturer is aware, or ought to be aware, of a compliance failure; and • Manufacturer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to notify persons, including the enforcement authority & customers, of compliance failure	• Manufacturer is aware, or ought to be aware, of a compliance failure; and • Manufacturer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to maintain records of: • any investigation of a compliance failure; and • compliance failures	
Authorised representative of manufacturer	Duty to notify manufacturer and enforcement authority of compliance failure	• Authorised representative is informed there is or may be a compliance failure; and • Authorised representative is aware, or ought to be aware, that the product is or will be a UK CCP
Importer	Duty to comply with relevant security requirements	• Importer intends product to be a UK CCP, or is aware, or ought to be aware, that the product will be a UK CCP; or • Product is a UK CCP and, at the time it was made available, the above condition was satisfied
	Duty not to make a relevant connectable product available in the UK without a statement of compliance or a summary of the statement of compliance in prescribed form	Importer intends product to be a UK CCP, or is aware, or ought to be aware, that the product will be a UK CCP
	Duty not to make a relevant connectable product available in the UK where compliance failure by the manufacturer	• Importer intends product to be a UK CCP or is aware, or ought to be aware, that the product will be a UK CCP; and • Importer knows or believes there is a compliance failure

Relevant Person	Statutory Duty	Conditions for Duty to Apply
	Duty to take all reasonable steps to investigate whether there is a compliance failure by the manufacturer or importer	After an importer of a relevant connectable product makes it available in the UK: • Importer is informed that there is or may be a compliance failure; and • Importer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty, as soon as practicable, to take all reasonable steps to remedy compliance failure by importer	• Importer is aware, or ought to be aware, of a compliance failure; and • Importer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to notify persons, including the enforcement authority & (subject to conditions) customers to whom the importer supplied the product, of compliance failure by importer	• Importer is aware, or ought to be aware, of a compliance failure; and • Importer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to contact the manufacturer about compliance failure by the manufacturer	• Importer is aware, or ought to be aware, of a compliance failure; and • Importer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty, as soon as practicable, to take all reasonable steps to prevent product from being made available to customers in the UK (where it has not already been made available)	• Importer is aware, or ought to be aware, of a compliance failure; and • Importer is aware, or ought to be aware, that the product is or will be a UK CCP; and • It appears to the importer that it is unlikely that the manufacturer will remedy the compliance failure
	Where the importer has contacted the manufacturer about compliance failure by the manufacturer, duty to notify the enforcement authority, any distributor and (subject to conditions) customers to whom the importer supplied the product, of compliance failure by manufacturer	• Importer is aware, or ought to be aware, of a compliance failure; and • Importer is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to maintain records of: • any investigation by the importer of a compliance	

Relevant Person	Statutory Duty	Conditions for Duty to Apply
	failure by the importer or a manufacturer; • any investigations of which the importer is aware that have been carried out by a manufacturer into a compliance failure by the manufacturer	
Distributor	Duty to comply with relevant security requirements	• Importer intends product to be a UK CCP, or is aware, or ought to be aware, that the product will be a UK CCP; or • Product is a UK CCP and, at the time it was made available, the above condition was satisfied
	Duty not to make a relevant connectable product available in the UK without a statement of compliance or a summary of the statement of compliance in prescribed form	Distributor intends product to be a UK CCP, or is aware, or ought to be aware, that the product will be a UK CCP
	Duty not to make a relevant connectable product available in the UK where compliance failure by the manufacturer	• Distributor intends product to be a UK CCP or is aware, or ought to be aware, that the product will be a UK CCP; and • Distributor knows or believes there is a compliance failure
	Duty, as soon as practicable, to take all reasonable steps to remedy compliance failure by distributor	After a distributor of a relevant connectable product makes it available to a customer in the UK: • Distributor is aware, or ought to be aware, of a compliance failure by the distributor; and • Distributor is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to notify the enforcement authority & (subject to conditions) customers to whom the distributor supplied the product, of compliance failure by distributor	After a distributor of a relevant connectable product makes it available to a customer in the UK: • Distributor is aware, or ought to be aware, of a compliance failure by the distributor; and • Distributor is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to contact the manufacturer about	• Distributor is aware, or ought to be aware, of a compliance failure; and

Relevant Person	Statutory Duty	Conditions for Duty to Apply
	compliance failure by the manufacturer	• Distributor is aware, or ought to be aware, that the product is or will be a UK CCP
	Duty to contact relevant person other than manufacturer that supplied product to distributor about compliance failure by the manufacturer	• Distributor is aware, or ought to be aware, of a compliance failure; and • Distributor is aware, or ought to be aware, that the product is or will be a UK CCP; and • It is not possible to contact the manufacturer
	Duty, as soon as practicable, to take all reasonable steps to prevent product from being made available to customers in the UK (where it has not already been made available)	• Distributor is aware, or ought to be aware, of a compliance failure; and • Distributor is aware, or ought to be aware, that the product is or will be a UK CCP; and • It appears to the distributor that it is unlikely that the manufacturer will remedy the compliance failure
	Where the distributor has contacted (or attempted to contact) the manufacturer about compliance failure by the manufacturer, duty to notify persons, including the enforcement authority and (subject to conditions) customers to whom the distributor supplied the product, of compliance failure by manufacturer	• Distributor is aware, or ought to be aware, of a compliance failure; and • Distributor is aware, or ought to be aware, that the product is or will be a UK CCP

3.1.5.3 Enforcement

The 'enforcement authority' responsible for enforcing Part I of the PSTI Bill is the Secretary of State for the DDCMS or a delegate. The Bill provides that the enforcement authority has all of the powers of investigation set out in schedule 5 of the *Consumer Rights Act 2015* (UK).[29]

The PSTI Bill establishes a tiered enforcement regime for the statutory duties, which provides for the enforcement authority to issue the following enforcement notices to relevant persons (that is, manufacturers, importers or distributors):

[29] For investigatory powers under sch 5 of the *Consumer Rights Act*, see Department of Business Innovation & Skills (UK), *Investigatory Powers of Consumer Law Enforcers: Guidance for Businesses on the Consumer Rights Act 2015* (Report, October 2015) <https://www.businesscompanion.info/sites/default/files/Investigatory-powers-of-consumer-law-enforcers-guidance-for-businesses-on-the-Consumer-Rights-Act-2015-Oct-2015.pdf>.

- **Compliance Notice:** A notice requiring the recipient to comply with a relevant duty within a specified time frame
- **Stop Notice:** A notice to stop carrying on an activity within a specified time frame
- **Recall Notice:** A notice requiring the recipient to make arrangements within a specified period for the return of the products to the recipient or to another person specified in the notice

A recall notice is obviously a more extreme measure and, as such, can only be given where: (a) the Secretary of State has reasonable grounds to believe that there is a compliance failure in relation to any UK CCP; (b) the Secretary of State considers that the action being taken by any relevant person in relation to the compliance failure is inadequate; and (c) the Secretary of State considers that no other action, such as a compliance notice or stop notice, would be sufficient to deal with risks posed by the compliance failure.

A failure to comply with an enforcement notice is an offence punishable by a fine. In addition, where a person has, on the balance of probabilities, failed to comply with a relevant statutory duty, the enforcement authority may give a penalty notice requiring the recipient to pay a fine of a specified amount within a specified time. Finally, apart from enforcement notices, on the satisfaction of certain conditions, the Secretary of State may apply to the court for an order for the forfeiture of products.[30]

3.1.6 Current Issues in Regulating CIoT Device Security in Australia

The Department of Home Affairs DP released in July 2021, and the UK PSTI Bill introduced in November 2021, raise the following issues concerning the future of regulation to secure CIoT devices in Australia:

1. Should legislation, such as the UK PSTI Bill, be introduced to mandate minimum security standards for CIoT devices?
2. If so, should minimum security standards be based on ETSI EN 303 645?
3. If mandatory standards are introduced, what standards should be mandated and what obligations imposed?
4. If mandatory obligations are introduced, how should they be enforced and who should be responsible for regulating?

Each of these issues is addressed immediately below. This section of the Report then examines how the regulation of CIoT devices fits within the broader Australian cyber security regulatory framework.

[30] PSTI Bill (n 26) cl 42.

3.1.6.1 Is there a need for legislation mandating CIoT security?

As the Department of Home Affairs DP reported, government research conducted after the release of the voluntary Code of Practice indicated that it is not working effectively to ensure the security of CIoT devices.[31] The main reason for this is that, unaided, markets fail to provide sufficient incentives for suppliers to adequately secure CIoT devices. The main causes of market failure are information asymmetries and negative externalities. First, as consumers have insufficient information to be able to distinguish between secure and insecure devices, they will make decisions based largely on price, which can benefit those supplying devices at the bottom end of the market.[32] Secondly, decisions by a business not to invest in security may result in costs that are borne not by itself but by others, resulting in a negative externality.[33] To the extent that businesses do not bear the costs of insecure devices, there is a misalignment of incentives for ensuring adequate cyber security.

The main arguments given for opposing legislatively mandating minimum security standards have been that IoT technologies are moving too rapidly for regulation to catch up and in any case, the diversity of CIoT devices means that a 'one size fits all' standard would be unlikely to be successful.[34] The first objection is a version of the 'Collingridge dilemma', which refers to the difficulty in timing the regulation of technology, as attempts to regulate a technology early in its development are impeded by insufficient information about the technology but once a technology has achieved mass penetration, it is difficult or impossible to effectively control.[35] Addressing the dilemma commonly involves the use of principles-based regulation and the use of 'soft law' or 'agile regulation', such as regulatory guidance or codes of practice.[36] Accordingly, the first objection is more about how to regulate than it is about whether to regulate. The UK PSTI Bill addresses this issue by confining itself to framing legislation with much of the detail, including minimum standards, left to 'soft law' in the form of regulations.

---

[31] *Department of Home Affairs Discussion Paper* (n 16) Annex A.
[32] George Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 *Quarterly Journal of Economics* 488; Ross Anderson and Tyler Moore, 'The Economics of Information Security' (2006) 314 *Science* 610.
[33] Anderson and Moore (n 32); *Department of Home Affairs Discussion Paper* (n 16) 10.
[34] Internet of Things Alliance Australia (IoTAA), Submission to the Department of Home Affairs, *Consultation on Securing the Internet of Things for Consumers: Draft Code of Practice* (1 March 2020) <https://www.iot.org.au/wp/wp-content/uploads/2020/03/IoTAA-Submission-to-IoT-Security-Code-of-Practice-1-Mar-2020-Final.pdf>; IoTAA, *Response to Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper* (Report, 26 August 2021) <https://iot.org.au/wp/wp-content/uploads/2021/11/IoTAA-Response-to-Strengthening-Australias-Cyber-Security-Regulations-and-Incentives-Discussion-Paper.pdf> ('*Response*').
[35] David Collingridge, *The Social Control of Technology* (Francis Pinter, 1980).
[36] Ryan Hagemann, Jennifer Huddlestone Skees and Adam Thierer, 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (2018) 17(1) *Colorado Technology Law Journal* 37; World Economic Forum, *Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators* (Report, December 2020) <https://www.weforum.org/about/agile-regulation-for-the-fourth-industrial-revolution-a-toolkit-for-regulators>.

The second objection should also be seen as raising questions primarily about the form of regulation. Whatever the context, rules, such as codes and technical standards, are necessarily expressed at a general level that is abstracted from particular factual circumstances. For example, codes, such as the UK and Australian voluntary codes, set out general principles that necessarily apply to a diverse range of CIoT devices; while more detailed, technical standards, such as ETSI EN 303 645, are also pitched at a general level. As in many other settings involving the regulation of technologies, the application of general rules in instruments such as legislation or regulations can also be supplemented by guidelines explaining how the rules apply to particular circumstances. Moreover, as is the case under the *Privacy Act 1988* (Cth), provision can always be made for the development of codes of practice for industry sectors, which would allow for general standards to be customised to particular circumstances. The *Privacy Act* and analogous data privacy laws are existing examples of how high-level principles, such as the data security principle in APP 11, can apply to a great diversity of particular circumstances.

In summary, voluntary standards are unable to ensure adequate device security as there are insufficient incentives for all businesses to comply. While there are legitimate concerns about introducing mandatory standards, including the costs of compliance, these are relevant to the form of regulation rather than whether or not regulation is justified. This Report therefore recommends that Australia should introduce legislation to mandate minimum security standards for CIoT devices.

The arguments in favour of mandated security standards were recognised by the outgoing Coalition Government during the 2022 federal election campaign, when the former Minister for Home Affairs, Karen Andrews, indicated an intention to replace the current voluntary code with legislation mandating minimum standards, aligned with the UK Act.[37] The announcement also rejected introducing a mandatory expiry label, instead favouring a voluntary labelling scheme to be co-developed with industry.

Recommendation 1

Legislation should be introduced to regulate the security of CIoT devices. The legislation should impose mandatory minimum obligations on relevant entities, namely: manufacturers, importers and distributors of CIoT devices.

[37] Justin Hendry, 'Gov pledges to mandate IoT cyber security standards', *IoTHUB* (13 May 2022) <https://www.iothub.com.au/news/gov-pledges-to-mandate-iot-cyber-security-standards-579966>.

3.1.6.2 Should Australia adopt ETSI EN 303 645?

As explained previously, the Department of Home Affairs DP on strengthening Australia's cyber security proposed that Australia consider adopting ETSI EN 303 645.[38] The DP suggested that adopting the ETSI standard would ensure international consistency and encourage best practice. Moreover, the DP reported that participants in research on the effectiveness of the Australian Code of Practice preferred that government communicate its expectations of industry through internationally recognised standards.[39] That said, there are potential disadvantages in the wholesale adoption of the ETSI standard.

The ETSI standard is more detailed that either the UK or Australian Codes of Practice and as previously mentioned, it has achieved a degree of international recognition.[40] Nevertheless, ETSI is a Europe-based organisation, originally established in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT) following a proposal from the European Commission.[41] It would be unusual for Australian legislation to mandate a European standard, which could be amended or replaced without Australian involvement. Furthermore, as one of the three European Standards Organizations (ESOs), ETSI has a special role in Europe, supporting European legislation and regulations.[42] As such, ETSI standards, such as EN 303 645, may be developed against the background of European legislation and regulations. For example, the ETSI standard, as well as the UK Code, assumes the existence of the General Data Protection Regulation (the GDPR). Therefore, the ETSI standard does not need to emphasise privacy protection as much as an Australian instrument as the GDPR affords stronger and more widely applicable privacy protection than is available in Australia. While the current privacy law reform process explained in Part 5 of this Report may result in greater alignment between Australian law and the GDPR, this is by no means guaranteed.

In addition, the ETSI standard has not been universally adopted. For example, the US *Internet of Things Cybersecurity Improvement Act of 2020* requires the National Institute of Standards and Technology (NIST) to publish standards and guidance for use and management of IoT devices, 'including minimum information security requirements for managing cybersecurity risks associated with such devices'.[43] The *Security of Connected Devices* legislation in California requires manufacturers of connected devices, such as CIoT devices, to equip devices 'with a reasonable security feature or features'.[44]

[38] *Department of Home Affairs Discussion Paper* (n 16) 32.
[39] Ibid.
[40] See 'Mapping Security & Privacy in the Internet of Things' (n 10).
[41] 'About Us', *ETSI* (Web Page, 2022) <https://www.etsi.org/about/about-us>.
[42] Ibid.
[43] *Internet of Things Cybersecurity Improvement Act of 2020*, HR 1668, 116th Congress (2019-2020) Pub L No 116-207, § 4(a)(1).
[44] *Security of Connected Devices*, 1.81.26.a, CA Civ Code § 1798.91.04 (a) (2018).

Similarly, the Oregon House Bill 2395 requires that manufacturers implement 'reasonable security features'.[45] The California Department of Justice, when explaining the meaning of reasonable security measures, points to the Critical Security Controls maintained by the Center for Internet Security (CIS).[46] It is likely that the NIST 'minimum security requirements' would also inform interpretation of 'reasonable security features' in the California and Oregon legislation. Given the size of the US market and the fact that many CIoT devices are developed by US companies, the NIST standards may become more important.[47]

Furthermore, according to the UK's mapping of cyber security standards globally, referred to earlier, there are more than 100 global standards; among them there are other candidates for a standard that might be adopted.[48] NIST standards on IoT cyber security are highly referenced, as are standards from NGOs, such as GSMA (Global System for Mobile Communications), IETF (Internet Engineering Task Force) and IEEE (Institute of Electrical and Electronics Engineers).[49] Therefore, a decision to adopt a standard ought to at least consider other promising candidates and, given the disconnect between the Australian and European regulatory contexts, assess their suitability for Australia.

This Report therefore recommends that Australia should draw lessons from the ETSI standard, as well as other globally applicable standards, but for the present should refrain from mandating any particular technical standard. Instead, in implementing mandatory standards, the Report recommends focussing attention on making improvements to the current Australian Code of Practice.[50]

---

[45] OR HB2395, ch 193, § 1(2), 2019.
[46] Kamala D Harris, *California Data Breach Report 2012-2015* (Report, California Department of Justice, Attorney General, February 2016) v, 30–31 <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>. See eg, 'CIS Critical Security Controls v 7.1', *Center for Internet Security* (Web Page, 2019) <https://www.cisecurity.org/controls/v7>.
[47] Michael Fagan et al, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* (Draft NIST Special Publication No 800-213, National Institute of Standards and Technology, US Department of Commerce, December 2020) <https://doi.org/10.6028/NIST.SP.800-213-draft>; Michael Fagan et al, *IoT Device Cybersecurity Capability Core Baseline* (Report No NISTIR 8259A, National Institute of Standards and Technology, US Department of Commerce, May 2020) <https://doi.org/10.6028/NIST.IR.8259A>; Michael Fagan et al, *IoT Non-Technical Supporting Capability Core Baseline* (Report Draft No NISTIR 8259B, National Institute of Standards and Technology, US Department of Commerce, December 2020) <https://doi.org/10.6028/NIST.IR.8259B-draft>; Michael Fagan et al, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline* (Report Draft No NISTIR 8259C, National Institute of Standards and Technology, US Department of Commerce, December 2020) <https://doi.org/10.6028/NIST.IR.8259C-draft>; Michael Fagan et al, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* (Report Draft No NISTIR 8259D, National Institute of Standards and Technology, US Department of Commerce, December 2020) <https://doi.org/10.6028/NIST.IR.8259D-draft>.
[48] 'Mapping Security & Privacy in the Internet of Things' (n 10).
[49] Ibid.
[50] See Evana Wright et al, Submission to Department of Home Affairs, *Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper* (2021) <https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/wright-lindsay-wilkinson-fraser-and-collings.pdf>.

Recommendation 2

Australia should not mandate adoption of ETSI EN 303 645 but should build on the security principles in the current Code of Practice.

3.1.6.3 What standards should be mandated and what obligations imposed?

There is a high level of agreement among security standards, specifications and guidelines about the most important security principles for CIoT devices, which is generally reflected in the 13 principles in the UK and Australian codes of practice. As explained, the UK Government has decided initially to mandate the top three principles in the UK Code and the ETSI standard, namely: no default passwords; implement a vulnerability disclosure policy; and keep software updated. In addition to these principles, the WEF's five security 'must haves' include: securely communicating, and ensuring that personal data is secure. Both of these appear in the UK and Australian codes but with differences in ranking.

At this stage, the UK has elected to mandate only the top three principles on the basis that mandating all 13 principles might dampen innovation. However, if the principles are considered important enough to include in a voluntary code, and as the arguments in favour of mandating principles must apply equally to all principles, it would appear that eventually all of the principles will need to be mandated. The argument in favour of a staged implementation of the security principles is therefore not primarily about whether or not industry should comply with the principles but about the time that may be required for industry to adjust to compulsory principles as well as the costs of compliance. As the main objective of regulating security must be to encourage compliance, these considerations are important and support a case for staged implementation. However, if Australia were to follow this path, there is a good argument for building on the UK model by mandating all five of the WEF's 'must haves', including secure communication and ensuring the security of personal data. This would send a firm message to industry about the importance of doing more than the bare minimum to secure devices. In that event, the imposition on industry could be managed by a flexible, tiered enforcement regime, including provision for warning or compliance notices.

As explained at 3.1.5.2, the UK PSTI Bill implements the CIoT regulatory regime by imposing statutory duties on manufacturers, importers and distributors. The duties include duties relating to compliance with minimum mandatory security principles, statements of compliance and compliance failures. Given the popularity of CIoT devices, any regulatory regime must, to an extent, rely upon self-certification. Therefore, there is a good case for requiring relevant entities to produce self-certifying statements of compliance. Obligations to produce statements of compliance in a prescribed form can

have two additional advantages. First, the requirement could elicit additional information about how an entity is complying with the security principles. Secondly, if, as recommended in this Report, a mandatory labelling scheme were to be introduced, information in a compliance statement could assist in evaluating the accuracy of a security label.

In practice, much of the regulation of device security must depend upon consumer complaints about compliance failures. Therefore, it is important for relevant entities to be required to respond to complaints by investigating potential compliance failures and taking timely action to remedy any security defects in a device. In addition to responding to consumer complaints, the UK PSTI Bill imposes duties of investigation and rectification where an entity is aware or ought to be aware of a compliance failure. Imposing duties in relation to compliance failures is therefore an essential element of any regime imposing mandatory security standards.

Recommendation 3

Legislation imposing security standards should adopt a staged approach by, in the first instance, mandating the most important standards. Consideration should be given, in the first instance, to mandating the five 'must haves' identified by the WEF, namely: no universal default passwords; implementing a vulnerability disclosure policy; keeping software updated; securely communicating; and ensuring that personal data is secure.

Recommendation 4

Legislation setting minimum security standards should, in general, follow the model adopted by the UK Product Security and Telecommunications Infrastructure Bill 2021 by imposing duties on manufacturers, importers and distributors relating to compliance with minimum standards, statements of compliance and compliance failures.

3.1.6.4 How should the statutory duties be enforced and who should regulate?

As explained at 3.1.5.3, the UK PSTI Bill incorporates a tiered enforcement regime, including compliance notices, stop notices and recall notices, with penalties imposed in the event of failure to comply. It is generally acknowledged that, applying the principles of responsive regulation, a tiered enforcement model can encourage industry engagement and compliance.[51] While there is no 'one

[51] See Mary Ivec and Valerie Braithwaite with Charlotte Wood and Jenny Job, *Applications of Responsive Regulatory Theory in Australia and Overseas: Update* (Occasional Paper 23, Regulatory Institutions Network, Australian National University, March 2015)

size fits all' solution to non-compliance, regulatory responsiveness is enhanced whenever regulators have a flexible range of regulatory responses. The UK model therefore provides the basis for a proportionate regulatory approach, provided always that there is a credible threat of regulatory escalation resulting in penalties.

The more difficult issue is determining who should be responsible for regulating the security of CIoT devices. As explained at 3.1.5.3, the UK PSTI Bill provides for the 'enforcement authority' to be the Secretary of State for the DDCMS, or a delegate. Although, like the UK, Australia has no general dedicated cyber security regulator, in September 2021, the Department of Home Affairs established the Cyber and Infrastructure Security Centre (CISC) to be responsible for 'an all-hazards critical infrastructure resilience regime'.[52] This coincides with the recent increased focus on regulating to ensure the cyber security of critical infrastructure, culminating with the passage of the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth) (the '*SLACIP Act*'), which is the final component of the current wave of critical infrastructure reforms. While these reforms, which are explained further immediately below, are aimed at responding to the cyber threats faced by Australian businesses, as this Report has explained, the security threats facing consumers with connected devices in their homes are serious. The newly established CISC faces immediate challenges in establishing the new critical infrastructure regulatory regime; extending the Centre's role to encompass consumer security issues would represent not only an expansion of the CISC's jurisdiction, but raise very different regulatory issues. On the other hand, it might be possible for the CISC to leverage expertise in cyber security, and its networks with government and industry, to enhance the regulation of consumer IoT. Moreover, as it is generally accepted that responding to cyber security threats requires holistic responses, cutting across data and information technology ecosystems – for example, compromised CIoT devices can pose a threat to business – giving the CISC a role in regulating CIoT devices, could assist in developing a whole-of-economy approach. Consideration should therefore be given to establishing a role for the CISC in regulating the security of CIoT devices.

Recommendation 5

Legislation imposing security standards should adopt a flexible tiered system of enforcement, potentially incorporating compliance notices, stop notices and recall notices.

<https://regnet.anu.edu.au/sites/default/files/publications/attachments/2015-05/Occasional%2520Paper%252023_Ivec_Braithwaite_0.pdf>; Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

[52] Department of Home Affairs and Cyber and Infrastructure Security Centre (Cth), *Protecting Australia Together: Securing Australia's Critical Infrastructure with Asset Owners and Operators, Governments and the Community* (Report, April 2022) <https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/protecting-australia-together.pdf>.

Recommendation 6

Consideration should be given to establishing a role for the newly established Cyber and Infrastructure Security Centre (CISC) in regulating the security of CIoT devices.

3.1.7 Placing the Regulation of CIoT Device Security within the Cybersecurity Regulatory Framework

As explained above, considerable recent attention, culminating in the *SLACIP Act*, has been given to regulation designed to enhance the security of critical infrastructure. The *SLACIP Act* amends the *Security of Critical Infrastructure Act 2018* (Cth) (the '*SOCI Act*') by introducing two new key obligations for owners and operators of critical infrastructure assets:

- a 'positive security obligation' requiring responsible entities to create and maintain a critical infrastructure risk management program; and
- 'enhanced cyber security obligations', which must be complied with by operators of Systems of National Significance (SoNS).

While the *SOCI Act* defines 'critical infrastructure assets' by reference to industry sectors – ranging from telecommunications, to banking and finance, energy, food and grocery and transport – the definitions are expanded upon by the *Security of Critical Infrastructure (Definitions) Rules 2021* (Cth).[53] SoNS are a subset of the most important critical infrastructure assets and will be declared by the Minister for Home Affairs.[54] The enhanced obligations imposed on SoNS are: to adopt, maintain and comply with an incident response plan; undertake cyber security exercises; undertake vulnerability assessments; and provide access to the Australian Signals Directorate (ASD) to system information.

The critical infrastructure reforms are a recognition of the increasing risks posed by threats to cyber security, including risks of significant economic harm. Given the risks, it is understandable for priority to be given to securing infrastructure assets that are nationally significant. Nevertheless, enhancing cyber security cannot be achieved solely by sector specific approaches in isolation from the broader cyber security environment. For example, there are commonalities in the challenges faced across

[53] *Security of Critical Infrastructure Act 2018* (Cth) s 9; *Security of Critical Infrastructure (Definitions) Rules 2021* (Cth).
[54] See *Security of Critical Infrastructure Act 2018* (Cth) pt 2C.

industry sectors, such as the vulnerability of devices to ransomware[55] attacks and other cyber breaches, which have become increasingly prevalent.

It is therefore important for cyber security to be enhanced across industry sectors, which means going beyond the targeting of critical infrastructure assets. Once the critical infrastructure reforms are in place, consideration should be given to how to expand proportionate cyber security regulation across industry. The proposed legislation for establishing mandatory minimum security standards for CIoT devices recommended by this Report should therefore be seen within the broader context of the society-wide imperative of improving cyber security. To promote system-wide approaches to increasing the overall level of cyber-security and to enhance consistency across sectors, consideration should be given to folding CIoT legislation into a broader regulatory framework. Such a broader framework may well include elements such as mandatory standards, industry codes of practice or labelling schemes.

Recommendation 7

If legislation imposing mandatory standards on CIoT devices is introduced, consideration should be given to how it relates to the broader cyber security regulatory framework, including the regulatory regime applying to critical infrastructure assets. Ideally, cyber security regulation should be extended beyond critical infrastructure to apply across industry sectors. While the regulation of CIoT devices presents distinct policy issues, it should be harmonised with economy-wide efforts aimed at improving incentives to enhance cyber security.

3.2 Security Labelling Schemes

This second section of the Report addresses the potential for labelling schemes to enhance the security of CIoT devices. First, it introduces the essential policy rationale for establishing a CIoT security labelling scheme and identifies the policy options for introducing a labelling scheme. It then explains the labelling schemes which have been introduced in Singapore and Finland which, to date, are the only two countries to have introduced government-led CIoT security labelling schemes, and introduces the Memorandum of Understanding (MoU) between Singapore and Finland. Finally, this part critically

[55] The Australian Cyber Security Centre describes ransomware as a type of malicious software that prevents access to or use of devices and files by locking or encrypting them. Ransomware is used to demand a payment from users in order to restore access and use of the device or files. See Australian Cyber Security Centre, *Ransomware* (Webpage) <https://www.cyber.gov.au/ransomware>.

evaluates the case for introducing a mandatory security labelling scheme for CIoT devices and makes recommendations.

3.2.1 The Rationale for Security Labelling

As this Report has explained, a major reason for insecure CIoT devices is that consumers have insufficient information to incorporate device security into purchasing decisions. Product information and information concerning security and privacy settings can be complex, difficult to understand and difficult to locate, especially when it is embedded in terms and conditions. Research has revealed complacency on the part of consumers in seeking out such security and privacy information.[56] This complacency points to the need for regulators to introduce measures that facilitate informed decision making among consumers when purchasing smart devices to mitigate risks of harm that may be caused by security and privacy breaches. Furthermore, most consumers fail to read or understand the terms and conditions governing the use of smart devices and associated services.[57] Consumers are also seldom provided with the time or assistance to read and understand the terms and conditions at the time of purchase. Where a consumer has low literacy, poor eyesight or reads languages other than English, they may face additional barriers. One mechanism proposed for addressing this information deficit is to establish a security labelling scheme. The July 2021 DP on strengthening cyber security released by the Department of Home Affairs suggested that based on evidence that consumers think cyber security is an important purchasing consideration, 'we think that a cyber security labelling scheme could be successful in Australia'.[58]

As explained above, the Department of Home Affairs DP canvassed proposals for introducing labelling for smart devices and in doing so, identified the following three options:[59]

1. Maintain the status quo, of no labelling scheme;
2. Introduce a voluntary star rating labelling scheme, similar to that implemented in Singapore or Finland; or

[56] Harris Interactive, *Consumer Internet of Things Security Labelling Survey Research Findings* (Report, prepared for the UK Government DDCMS, 2019) 3 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf>.
[57] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2018) 23(1) *Information, Communication & Society* 128. In a recent survey conducted by Warren, Mann and Harkin, 47% of participants indicated that they did not read privacy policies. See Ian Warren, Monique Mann and Diarmaid Harkin, *Enhancing Consumer Awareness of Privacy and the Internet of Things* (Report, Deakin University, ACCAN, August 2021) 6 <https://accan.org.au/files/Grants/2021%20Deakin%20IoT/Deakin%20grants%20report_v5_web.pdf>.
[58] *Department of Home Affairs Discussion Paper* (n 16) 36.
[59] Ibid 37–41.

3. Introduce a mandatory expiry date label, in accordance with a recommendation from the Cyber Security Strategy Industry Advisory Panel.

3.2.2 Singapore's Consumer Label Scheme (CLS)

The Consumer Label Scheme (CLS) is a voluntary security labelling scheme that was developed, and is supported by, the Singapore Government. The CLS was developed by the Cybersecurity Certification Centre (CCC), which is part of the Cyber Security Agency (CSA) of Singapore.[60] The CSA was formed in 2015 as part of the Prime Minister's Office and is the national government agency with responsibility for protecting 'Singapore's cyberspace'.[61] It offers and supports the use of the CLS to provide assurance to customers that CIoT products have been objectively assessed for cybersecurity by adopting a 'security by-design approach'.[62]

The CLS was launched in October 2020 and is expressly intended to raise overall 'cyber hygiene levels', to 'better secure Singapore's cyberspace' and enable consumers to discern the security levels of IoT devices and on this basis, make more informed purchase decisions.[63] Relatedly, it is intended to incentivise manufacturers to develop more secure products and by doing so, differentiate their products from those of competitors.[64] The scheme was initially confined to Wi-Fi routers and smart home hubs due to the wide usage and importance of these products but has since been extended to apply to all categories of CIoT devices, including IP cameras, smart door locks, smart lights and smart printers.[65]

The CLS incorporates four progressive rating levels, with each higher level being more comprehensive in the assessment that correlates with the star rating on the label. In summary, the four levels are:[66]

- **Level 1:** Meet Baseline Security Requirements
- **Level 2:** Adherence to the Principles of Security-by-Design
- **Level 3:** Absence of Known Common Software Vulnerabilities
- **Level 4:** Resistance against Common Cyber-Attacks

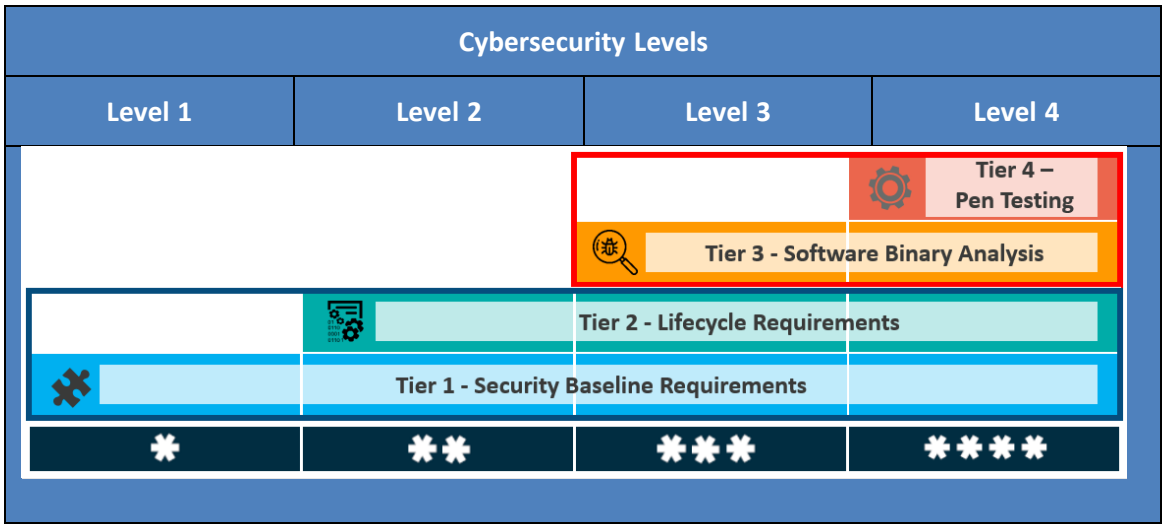
[60] 'Cybersecurity Labelling Scheme (CLS)', *Cyber Security Agency of Singapore* (Web Page, 30 March 2022) <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls>.
[61] See 'Who We Are', *Cyber Security Agency of Singapore* (Web Page, 25 April 2022) <https://www.csa.gov.sg/Who-We-Are/Our-Organisation>.
[62] Cyber Security Agency of Singapore, *Cybersecurity Certification Guide* (Report, 2021) 1 <https://www.csa.gov.sg/-/media/Csa/Documents/CLS/CSA-Cybersecurity-Certification-Guide.pdf>.
[63] Ibid 5.
[64] 'Cybersecurity Labelling Scheme (CLS)' (n 60).
[65] Ibid.
[66] Cyber Security Agency Singapore (n 62) 7.

The details of the CLS scheme are set out in two documents published by the CSA in April 2021:

- *Cybersecurity Labelling Scheme (CLS) Publication No. 1: Overview of the Scheme*
- *Cybersecurity Labelling Scheme (CLS) Publication No. 2: Scheme Specifications*

The four rating levels are set out in the following diagram and explained further immediately below.

Figure 2 Singapore Cybersecurity Labelling Scheme Tiers



3.2.2.1 Assessment Tier #1: Security baseline requirements

The first assessment tier is designed to indicate that the developer has taken steps to mitigate against common basic attacks and CIoT security problems. Accordingly, developers are required to conform to the top three requirements of ETSI standard EN 303 645, namely: having no universal default passwords; implementing a means to manage vulnerability reporting; and keeping device software updated. To qualify for Tier #1, developers are required to complete and submit a conformance checklist (which includes 67 items) and supporting evidence. However, compliance with these requirements depends upon the checklist submitted by the developer and no independent testing is required for this assessment tier.

3.2.2.2 Assessment Tier #2: Lifecycle requirements

Assessment Tier #2 is aimed at ensuring that devices are developed according to a security-by-design framework. These requirements are determined by reference to the lifecycle requirements set out in the *IMDA IoT Security Guide,* published by Singapore's Info-Communications Media Development Authority (IMDA).[67] The Security Guide incorporates the following four IoT security design principles:

[67] Info-Communications Media Development Authority, in consultation with Cyber Security Agency Singapore, *Internet of Things (IoT) Cyber Security Guide* (Guidelines, v 1, March 2020) <https://www.imda.gov.sg/-

secure by default; rigour in defence; accountability; and resiliency. To qualify for Tier #2, developers are required to complete a conformance checklist (indicating compliance with the lifecycle provisions) and submit a declaration of conformance. The CCC reviews the conformance checklist and associated evidence, and must be satisfied that the developer has implemented the required practices and processes. However, as with Tier #1, no independent testing or auditing is required.

3.2.2.3 Assessment Tier #3: Software binary analysis

The objective of Tier #3 is to indicate that the software (namely, the firmware and companion mobile applications) in a CIoT device is protected from: common software errors such as buffer overflows; known vulnerabilities in third party libraries that are used; and known malware. To qualify for Tier #3, the software must be submitted to the developer's testing laboratory of choice, which must analyse the software by binary scanners. The testing results are then submitted to the CCC, which reviews the laboratory's report before deciding whether to grant approval. If vulnerabilities are detected by the laboratory, remediation is required before a device can be approved for a Tier #3 label.

3.2.2.4 Assessment Tier #4: Penetration testing

The objective of Tier #4 assessment is to indicate that a device is resistant to common IoT attacks by 'black box penetration testing'. The testing procedures are set out in the CLS publication *Minimum Test Specifications and Methodology for Tier 4*.[68] Testing is intended to provide basic assurance that the device is resistant to commonly known and straightforward attacks. This can, for example, involve testing for 'password cracking'. The testing laboratory examines sources of information publicly available to identify potential vulnerabilities, including through public search engines. Black box penetration testing for Tier #4 can take up to 15 days and a device is deemed to pass if there are no critical or significant vulnerabilities. Testing laboratories may be required by CCC to perform further testing; otherwise, the product is approved and the developer is permitted to use the Tier #4 label.

Once a device has been approved, it is entitled to bear a label with the relevant star rating. The label includes product registration identification and the date the product was registered. It also includes a link to the CCC website where further information can be obtained, including vulnerability policies (which are required to be published). Developers can affix the label to product packaging, advertisements, promotional material and/or labelled products by the 'developer' applicant. The

/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf>.

[68] Cyber Security Agency Singapore, *Cybersecurity Labelling Scheme (CLS): Minimum Test Specifications and Methodology for Tier 4* (Report, v 1.1, April 2021) <https://www.csa.gov.sg/-/media/csa/documents/cls/pub-cls--minimum-test-specification-v1-1.pdf>.

certified rating is valid for a maximum period of three years, and the CCC provides a list of products rated under the CLS on its website. The following is an example of a CSA-approved label.

Figure 3 Example of Singapore Cybersecurity Label

Once a device has been labelled, the CCC may conduct random audits and testing to ensure that the product complies with the relevant requirements. If a device is non-compliant or there is another breach of the CLS terms, such as a failure to take corrective measures or a misrepresentation, the CCC may revoke a CLS label. Upon revocation, the label must cease to be used and the CCC will remove the product from the list of labelled products.

3.2.3 Finland's Cybersecurity Label (CL)

Finland's Cybersecurity Label (CL) scheme was introduced in 2019 and is intended to indicate that an IoT product or service is designed to meet minimum security standards. The voluntary scheme is administered by the National Cyber Security Centre Finland (NCSC-FI), which is part of the Finnish Transport and Communications Agency, Traficom. Traficom owns the visual trade mark for the CL and grants the right to use it to companies that comply with the application requirements. The evaluative criteria for approval to use the CL are set out in the *Statement of Compliance* application form, which

cross references provisions of ETSI EN 303 645.[69] The Traficom terms and conditions stipulate how the CL can be used, including duration, visibility and monitoring.[70]

The evaluative criteria in the CL scheme are based on ETSI standard EN 303 645, with the *Statement of Compliance* submitted by applicants requiring the following information:

- Comprehensive product description;
- Software security measures that described the software being used and the level of information security;
- Secure access control to confirm only users can access their functions;
- Secure default settings described so that default settings protect the user;
- Security of online services and ecosystem interfaces with a description of how this has been implemented;
- Data protection that describes how and why personal data is collected and who has access to process such data; and
- Secure transfer and storage of data that describes how information security is ensured during the transfer and storage of data.

General information is provided by Traficom to explain the system.[71] The device is sent to a testing body selected by the applicant, which examines compliance of the security features with the requirements in the *Statement of Compliance* in accordance with a testing plan approved by Traficom.[72] The application process takes between five to 20 days. The findings of the inspection are submitted to Traficom, where experts then assess whether or not the evaluative criteria are met. If not, corrective action may be required before permission is granted by Traficom to use the label.[73] Once approved, the label is valid for three years and a fee of 350 Euros is payable with a further annual fee of 350 Euros for each annual review.[74]

The IoT CL consists of an image of a padlock (see below), which confirms that the product is fully compliant with the evaluation criteria. Once approved, the CL may be affixed to approved products

[69] Traficom, *Statement of Compliance for the Cybersecurity Label* (Application Form, 2022) <https://tietoturvamerkki.fi/sites/default/files/media/file/statement-of-compliance-for-the-cybersecurity-label.pdf>.
[70] Traficom, *Terms of Use – Cybersecurity Label for IoT Consumer Devices* (Terms of Use, 1 March 2022) <https://tietoturvamerkki.fi/sites/default/files/media/file/Terms%20of%20Use%20%E2%80%93%20Cybersecurity%20Label%20for%20IoT%20consumer%20devices.pdf> ('*Terms of Use*').**Error! Hyperlink reference not valid.**
[71] Traficom, *Cybersecurity Label – Help your Customers Make Secure Choices* (Report, 2022) <https://tietoturvamerkki.fi/sites/default/files/media/file/cybersecurity-label-infopack-for-companies.pdf> ('*Cybersecurity Label – Help your Customers Make Secure Choices*').
[72] 'Inspection', *Traficom* (Web Page, 25 April 2022) <https://tietoturvamerkki.fi/en/inspection>.
[73] 'Apply for the Label', *Traficom* (Web Page, 9 March 2022) <https://tietoturvamerkki.fi/en/apply-label>.
[74] Traficom, *Cybersecurity Label – Help your Customers Make Secure Choices* (n 71).

and services and used in marketing and communication channels.[75] Approved devices are published on the Traficom website, which includes the product's *Statement of Compliance.* To date, 13 products have been listed, including a contact tracing app, home hubs, intelligent lighting, fitness watches and a smart heating adjuster.[76] The use of the label is monitored primarily by means of spot checks and feedback.[77] Labelled products or services are reviewed annually to take into account possible changes on information security that may have arisen, thereby ensuring continuous security.[78]

Figure 4 Example of Finnish Cybersecurity Label

Under the terms of use of the CL, companies that are licensed to use the trade mark must notify Traficom of any security breaches or other problems that may compromise the security of a product bearing the CL label. After becoming aware of the problem, Traficom and the company must jointly agree on a schedule for corrective action, with problems expected to be rectified within a maximum of 90 days.

3.2.4 Singapore-Finland MoU

A Memorandum of Understanding (MoU) has been signed between Singapore and Finland that mutually recognises the respective cybersecurity labels for CIoT products issued in each country. [79] The MoU is the first bilateral agreement whereby products under either scheme can meet the

[75] Traficom, *The Finnish Cybersecurity Label* (Presentation, 28 August 2020) <https://tietoturvamerkki.fi/sites/default/files/media/file/cybersecurity_label_presentation-280920.pdf>.
[76] 'Products', *Traficom* (Web Page) <https://tietoturvamerkki.fi/en/products>.
[77] Traficom, *Terms of Use* (n 70).
[78] 'Inspection' (n 72).
[79] 'Cybersecurity Labelling Scheme (CLS)' (n 60); David Koh, 'The Memorandum of Understanding (MoU) on Cooperation in the Field of Recognition of Cyber Security Labelling between the Cyber Security Agency of the Republic of Singapore and the Transport and Communications Agency of the Republic of Finland (Traficom)' (Speech, International IoT Security Roundtable, 6 October 2021) <https://www.csa.gov.sg/News/Speeches/speech-by-mr-david-koh-at-the-opening-of-international-iot-security-roundtable-2021>; Gregers Møller, 'Singapore and Finland Sign Agreement to Mutually Recognise IoT Security Labels', *ScandAsia* (online, 9 October 2021) <https://scandasia.com/singapore-and-finland-sign-agreement-to-mutually-recognize-iot-security-labels/>.

requirements of both the Finnish CL and Singapore's CLS with a single application process.[80] Under the MoU,

> *… consumer IoT products that have met the requirements of Finland's Cybersecurity Label are recognised as having met the requirements of Level 3 of Singapore's Cybersecurity Labelling Scheme, and products with CLS Level 3 and above are recognised by Finland to have met their requirements.*[81]

The uniform requirements facilitated by the MoU are intended to allow products or services to be placed on the market in both countries that meet the security criteria of both labels.

3.2.5 Should Australia Introduce a Mandatory Labelling Scheme?

To date, no jurisdiction has introduced a mandatory security labelling scheme for CIoT devices. Moreover, the July 2021 Department of Home Affairs DP on strengthening cyber security did not expressly canvas the introduction of a mandatory regime, confining itself to the options of introducing a voluntary star rating labelling scheme or a mandatory expiry date label. As previously noted, during the 2022 federal election campaign, the outgoing Minister for Home Affairs rejected proposals for a mandatory expiry date label but supported a voluntary labelling scheme to be co-developed by government and industry.

Nevertheless, the DP refers to evidence produced by the UK DDCMS in a 2019 analysis of policy options for enhancing the security of consumer IoT products, which supported mandatory labelling.[82] The UK impact assessment suggested that over a ten-year period, 15 per cent of consumers would switch to more secure devices as a result of mandatory labelling and that there could be a reduction in security breaches of between 10 to 50 per cent. As this section of the Report explains, it seems likely that even if a voluntary scheme were to be introduced, it would need to eventually migrate to a mandatory scheme to ensure its effectiveness. Furthermore, as consumer labelling alone is unlikely to be effective, it must be seen as part of a suite of measures designed to enhance security, including minimum mandatory security standards for CIoT devices and public education. In other words, both consumer labelling and additional regulation, such as mandatory security standards, are required to address the information asymmetries and other market failures that this Report has identified as the

[80] Eileen Yu, 'Singapore Inks Pact with Finland to Mutually Recognise IoT Security Labels', *ZDNet* (online, 7 October 2021) <https://www.zdnet.com/article/singapore-inks-pact-with-finland-to-mutually-recognise-iot-security-labels/>.
[81] 'Cybersecurity Labelling Scheme (CLS)' (n 60).
[82] Department for Digital, Culture, Media and Sport (UK), *Mandating Security Requirements for Consumer 'IoT' Products: Consultation Stage Impact Assessment* (Report, May 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950420/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment_V2.pdf>.

source of inadequate device security. As Warren, Mann and Harkin have observed, in the context of privacy labels, '[i]t is unlikely privacy icons will have significant impact in addressing privacy issues that arise from CIoTs in the absence of substantive legislative reform, enforcement oversight, and industry engagement'.[83] These observations hold equally true for concerns about CIoT device security.

The Department of Home Affairs DP acknowledges that a voluntary labelling scheme is unlikely to have the same effect as a mandatory scheme and may take longer to have an impact.[84] On the other hand, it suggests that if a voluntary labelling scheme became popular, there would be an incentive for other market participants to improve security in order to become competitive.[85] The difficulty with this argument mirrors the problems with arguments against mandatory security standards: providers of devices at the lower end of the market compete mainly on price and not on reputation or security, and therefore have little incentive to improve security or, in this case, to accurately label their products. This would be the case irrespective of the level of uptake of a voluntary scheme. That said, the DP does, at least implicitly, raise the most important objections to a mandatory regime.

The two main objections to a mandatory labelling scheme are cost and practicality. The costs incurred in a labelling regime include testing and auditing costs, administrative costs and marketing costs. However, these costs must be incurred by any labelling scheme, regardless of whether it is mandatory or voluntary. Moreover, as indicated by the experience in Singapore and Finland, establishing an effective voluntary regime requires some degree of government involvement, with associated costs incurred by government. Over and above these costs, a mandatory regime would necessarily include additional regulatory costs for government. Therefore, in relation to this issue, the case for a mandatory scheme resolves to whether the additional costs incurred by government are greater than the benefits, in terms of increased device security and reduced security breaches, arising from a mandatory labelling scheme. While it is admittedly difficult to estimate the benefits of mandatory labelling, the costs of inadequately secured devices are likely to be substantial. Furthermore, the regulatory costs incurred by government could be minimised by leveraging existing government expertise potentially including, as suggested at 3.1.6.4, expertise at the newly-established CISC.

While the 2019 UK policy impact statement, referred to earlier, supported the introduction of a mandatory labelling scheme, the UK Government has not mandated a scheme. In its January 2020 response to a consultation on proposals for regulating CIoT devices, the UK Government explained that requiring a specific label to be mandated would create supply chain management issues that

[83] Warren, Mann and Harkin (n 57).
[84] *Department of Home Affairs Discussion Paper* (n 16) 38.
[85] Ibid.

could result in potential disruption to business.[86] The identified issues included the problems or costs imposed on retailers required to validate the claims of device manufacturers. Similarly, in assessing the option for introducing a mandatory expiry date label, the Department of Home Affairs DP pointed to the challenges of mandating a label for overseas retailers, especially given the difficulties of preventing consumers from importing unlabelled products sourced from outside of Australia.[87] Although the DP suggested that a mandatory label could result in reduced product availability, it considered that the risks of this were low as the costs of a mandatory expiry label would likely be low. Needless to say, the costs imposed on industry by a fully-fledged mandatory labelling scheme would be higher than the costs of a mandatory expiry date label.[88]

While it is true that CIoT devices often have complex supply chains, so do many other consumer products. Moreover, the challenges of determining responsibility for device labels arise regardless of whether labelling is voluntary or mandatory. In addition, Australian consumer law is premised on the principle that liability for products placed on the market in Australia cannot be evaded merely because a product is sourced from outside of Australia. Accordingly, responsibility for complying with a mandatory labelling scheme, much like responsibility for mandatory security standards, needs to be allocated to those entities responsible for placing IoT devices on the market in Australia, which might be importers or retailers. Although this does impose costs on business in determining the security of products, this can be regarded, in the same way as minimum health and safety standards, as a necessary cost of doing business in Australia. These costs could be reduced by ensuring that any Australian scheme is harmonised, to the extent possible, with other relevant national schemes. Furthermore, while difficulties do arise from the extent to which CIoT devices may be directly sourced from outside of Australia, the overall policy objective is not necessarily to ensure that all imported devices are labelled, but to create the greatest possible incentive for devices to be labelled. In addition, as explained in the Department of Home Affairs DP, online marketplaces currently voluntarily remove products that fail to comply with Australian product safety standards, and similar arrangements could be expected to be implemented for unlabelled CIoT devices.

[86] Department for Digital, Culture, Media and Sport (UK), *Government Response to the 'Regulatory Proposals for Consumer Internet of Things (IoT) Security' Consultation* (Command Paper No Cp213, January 2020) 14–15 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/862953/Government_response_to_consultation__Regulatory_proposals_for_consumer_IoT_security.pdf>.
[87] *Department of Home Affairs Discussion Paper* (n 16) 40.
[88] There would be few advantages in confining a scheme to a mandatory expiry date label and some potentially significant disadvantages. As pointed out in the IoTAA submission to the Department of Home Affairs Discussion Paper, consumers viewing a mandatory expiry label might be misled into believing that it guaranteed device security: IoTAA, *Response* (n 34).

The Department of Home Affairs DP posed the question of whether, before deciding upon a labelling scheme, it might be best to await evidence from regimes that have already implemented security labelling, namely Singapore and Finland.[89] This directly raises the issue of the timing of regulatory intervention. Ideally, as mentioned, given the extent to which CIoT devices may be sourced across national boundaries, there should be a degree of cross-border consistency in national approaches to ensuring device security. As the Singapore Government has indicated, the 'CSA intends to engage other like-minded partners for mutual recognition of the CLS with the objective of eliminating duplicated assessments across national boundaries'.[90] In other words, the more countries that adopt a consistent labelling regime, the better for all concerned and, correspondingly, delays in implementing effective national regimes can impose external costs on all jurisdictions. This suggests that Australia should be more active in promoting internationally consistent labelling schemes.

In Australia, the IoTAA (Internet of Things Alliance Australia) has been involved in developing a voluntary industry-led Security Trust Mark since as long ago as 2017. In consultations undertaken as part of this project, it was indicated that the Australian Government was actively considering introducing a voluntary labelling scheme. As this Report has explained, however, given the incentives facing low cost device suppliers, a purely voluntary scheme is unlikely to achieve the objectives of a labelling scheme. Nevertheless, given both the costs of developing and implementing a scheme and uncertainties about the potential impact of a labelling scheme, there is a case for a staged implementation of device labelling, with evidence acquired in the initial stages of implementation being used to refine and improve the scheme. Moreover, while a mandatory labelling scheme would take some time to establish, including the time needed for industry consultation, a voluntary scheme could be established more expeditiously. Therefore, in the absence of a mandatory regime, a voluntary scheme, such as that which has been implemented in Singapore or Finland, should be trialled, at least as an interim measure.

However, as suggested by the experience in Singapore and Finland, any comprehensive voluntary scheme must depend upon the active involvement of government. For example, assuming that the regime includes a star rating scheme, government must have a role in accrediting certifying bodies and in enforcing compliance. Certification is an essential part of any labelling scheme, with a choice between self-certification and certification by independent third parties. In consultations undertaken for this project, it was reported that when the IoTAA conducted an informal draft certification scheme

[89] Ibid 41.
[90] Cyber Security Agency Singapore, *Cybersecurity Labelling Scheme (CLS) Publication No. 1: Overview of the Scheme* (Report, v 1.1, April 2021) 2 <https://www.csa.gov.sg/-/media/csa/documents/cls/pub-cls-pub-1---overview-of-cls-v1-1.pdf>.

for security labelling, more than half of the applicants failed at the application stage, meaning that they did not qualify to submit an application. This was attributed to insufficient understanding of device security, which strongly suggests that self-certification is unlikely to be successful.

To assist with enforcement, if a voluntary regime were to be introduced, it could be supported by an obligation to provide a statement of compliance, such as that required under the UK PSTI Bill, which would mean that any misrepresentations would amount to misleading or deceptive conduct under the *Australian Consumer Law* (*ACL*).[91] In addition, as is the case under the schemes implemented in Singapore and Finland, a voluntary regime would need to be accompanied by an authoritative white list of labelled products, with misrepresentations resulting in removal of a device from the list.

To be effective, any labelling scheme must be accompanied by other measures notably consumer education. In consultations undertaken for this project, it appeared that the Australian Government had received evidence of some consumer confusion about Singapore's star rating system. While consumers in Singapore generally understood that more stars are better, they did not necessarily know what this meant for their particular device. This reinforces the need for any labelling scheme to be accompanied by an effective public education campaign. In addition, it raises the important issue of whether a one-size-fits-all labelling scheme is suitable for all CIoT products: for example, the desirable level of security for a baby monitor clearly differs from that required for a connected kettle. This consideration suggests that any general labelling scheme will need to focus on minimum standards. Moreover, it is important for education about the scheme to make it clear that the security labels are not a guarantee that a device is absolutely secure. Such guarantees cannot be given, especially as device security depends upon the entire IoT ecosystem, including network security and security of any server a device is connected to. These considerations further emphasise the need, as explained in the Introduction and returned to in the Conclusion to this Report, for greater efforts to be made in relation to public education about CIoT security.

Recommendation 8

Over time, a mandatory security labelling scheme should be introduced as part of a comprehensive CIoT security regulatory regime. The labelling scheme must be properly resourced to ensure satisfactory testing, certification and enforcement. The scheme should be consistent, to the extent possible, with other relevant national labelling schemes.

[91] See *ACL* s 18.

Recommendation 9

Prior to the introduction of a mandatory labelling scheme, a voluntary scheme with government backing, similar to Singapore's CLS, should be introduced and properly resourced. The government's role in supporting the scheme should extend to accrediting certification bodies and enforcement. The scheme should incorporate arrangements for certification by independent third parties and should not be based on self-certification.

Recommendation 10

In conjunction with the introduction of a labelling scheme, government should fund a public education campaign to increase consumer awareness of both the scheme and security issues relating to CIoT devices.

4 Consumer Protection and CIoT Devices

Introduction

This Part of the Report introduces recommendations for reform of Australian consumer protection law aimed at improving the protection of consumers who purchase CIoT devices for the home. The analysis undertaken in this part supports recommendations for reforms to the provisions of the *Australian Consumer Law* (*ACL*) that relate to consumer guarantees, disclosure of pre-contractual information, the regulation of unfair contract terms and product liability.

The first section of this Part introduces the *ACL* and its main objectives. Following this, the consumer guarantees, which effectively give Australian consumers certain rights that cannot be contracted out of, are introduced and the challenges of applying the guarantees to CIoT devices explained. While this section of the Report supports current proposals for strengthening the enforcement of the consumer guarantees, it recommends more fundamental reforms, including introducing a new category of digital products that would be distinct from the existing categories of 'goods' and 'services', and new guarantees that are specifically designed to protect consumers of digital products. Given the considerable difficulties encountered in research undertaken for this project in locating and interpreting the complex terms and conditions for CIoT devices, the next section of the Report recommends introducing new obligations in the *ACL* mandating pre-contractual information disclosure, including making all terms and conditions readily available on publicly accessible websites. This section also supports the development of new consumer-facing technology tools to support the identification and analysis of contractual terms and conditions and to facilitate the comparison of terms and conditions offered by different suppliers.

The following section of this Part investigates measures for improving the 'unfair contracts' safeguards in the *ACL*. First, it supports proposals for introducing a new general prohibition of 'unfair trading' practices, which could assist in addressing predatory and manipulative practices associated with data-driven business models, including those relating to CIoT devices. Second, while welcoming measures for enhancing the enforcement of the unfair contract terms law, this Report does not consider that these go far enough. The Report therefore recommends that consideration be given to introducing more prescriptive lists of unfair terms, such as a black list of prohibited terms and/or a grey list of

presumptively unfair terms. This reform would add clarity and assist enforcement. Third, this section advocates the development and use of new technology tools, such as machine learning tools, to assist regulators in proactively identifying unfair or potentially unfair terms in consumer contracts.

The final section in this part of the Report examines the application of the product liability regime in the *ACL* to CIoT devices. After identifying the difficulties in determining when there may be a 'safety defect' in a CIoT devices, this section recommends the development of more consumer guidance, including on when security vulnerabilities may amount to a 'safety defect'. Particular difficulties arise in the application of some defences in the product liability regime to CIoT device, specifically the defence that confines liability to defects that exist at the time of supply and the regime that applies to liability for component parts of complex products. This section of the Report therefore makes recommendations for reforming these provisions to better protect purchasers of CIoT devices. This section of the Report also includes recommendations for extending the product liability and product recall provisions of the *ACL* so that they apply to intangible harms, such as data loss or privacy breaches, which may arise from defective CIoT devices.

4.1 The *Australian Consumer Law* (*ACL*)

The centre-piece of Australian consumer protection law is the *ACL*, which commenced on 1 January 2011. The *ACL* is a single national uniform consumer law, which provides for consumer protection and fair trading rules across all sectors of the Australian economy. While there are a range of national, state and territory sector-specific laws aimed at protecting consumers, this Report focuses on the application of the *ACL* to CIoT devices.

The objectives of Australian consumer protection law and policy are set out in the 2009 *Intergovernmental Agreement for the Australian Consumer Law* (*IGA*), which underpins the *ACL* and the national consumer policy framework. The objectives spelt out in the *IGA* were drawn from a 2008 report of the Productivity Commission, which formed the basis for reforms resulting in the *ACL*.[1]

The *IGA* provides that the main objectives of the *ACL* are to:

- improve consumer wellbeing through consumer empowerment and protection;
- foster effective competition; and

[1] Productivity Commission, *Review of Australia's Consumer Policy Framework* (Inquiry Report No 45, 30 April 2008) v1, 12–13 <https://www.pc.gov.au/inquiries/completed/consumer-policy/report/consumer1.pdf > ('*Consumer Policy Framework Review Report*').

- enable the confident participation of consumers in markets in which both consumers and suppliers trade fairly.

These general objectives are supported by the following six operational objectives:

- to ensure that consumers are sufficiently well-informed to benefit from and stimulate effective competition;
- to reduce the supply of unsafe goods and related services in the Australian market and ensure they are fit for the purpose for which they are sold;
- to prevent practices that are unfair;
- to meet the needs of those consumers who are most vulnerable or are at the greatest disadvantage;
- to facilitate accessible and timely redress where consumer detriment has occurred; and
- to promote proportionate, risk based enforcement.

The above objectives are promoted through the substantive provisions of the *ACL*, which include:

- a national unfair contract terms law covering standard form consumer and small business contracts;
- a national law guaranteeing consumer rights when buying goods and services;
- a national product safety law and enforcement system;
- a national law for unsolicited consumer agreements covering door-to-door sales and telephone sales;
- simple national rules for lay-by agreements; and
- penalties, enforcement powers and consumer redress options.

This Report focuses on: (a) the consumer guarantees, which provide consumers with rights in relation to goods or services that they acquire; (b) a proposed obligation for pre-contractual disclosure of product information; (c) the safeguards against unfair contracts; and (d) the product safety provisions, which regulate unsafe products and product-related services.

4.2 Consumer Guarantees

Division 1 of Part 3.2 of the *ACL* sets out statutory consumer guarantees that apply to the supply of goods or services to consumers. The consumer guarantees provide certain rights to consumers regardless of any warranties provided to consumers by suppliers or manufacturers. The guarantees

generally apply where a consumer purchases goods and services ordinarily acquired for personal, domestic or household use.[2]

Of the statutory guarantees established under the *ACL*, the following are the most relevant to the supply of CIoT devices:

- suppliers and manufacturers guarantee that goods are of acceptable quality when sold to a consumer;
- a supplier guarantees that goods will be reasonably fit for any purpose the consumer or supplier specified; and
- manufacturers or importers guarantee they will take reasonable action to provide spare parts and repair facilities for a reasonable time after purchase.

The consumer guarantees, which essentially impose statutory duties on suppliers and/or manufacturers, are mandatory and cannot be contracted out of. As the following case study illustrates, the way that product information is presented to consumers can create uncertainty or confusion about the application of the guarantees.

CASE STUDY: VTech SmartWatch

For the VTech DX SmartWatch, consumers may not understand that the relevant Australian consumer guarantees apply to all Australian purchases. The Australian VTech website recognises the application of Australian consumer guarantees to goods and services supplied by VTech Electronics (Australia) Pty Ltd. However, the website states that its warranty is limited to goods sold by authorised retailers and the warranty cannot be transferred, explicitly excluding outlets such as Ebay.com.au. This statement is part of a sub-section of the web page entitled Consumer Guarantees and does not clearly distinguish between the warranty and the consumer guarantees. Consumers may interpret this as a representation that the consumer guarantees described on that web page do not apply where the product is purchased from non-authorised retailers.

In accordance with the 2009 IGA, the consumer protection regime must be subject to ongoing review. In 2015, Australian ministers for consumer affairs commissioned Consumer Affairs Australia and New Zealand (CAANZ) to undertake a broad ranging review which, in 2017, delivered its Final Report (*ACL*

[2] *Australian Consumer Law* (sch 2 of the *Competition and Consumer Act 2010* (Cth)) s 3 (definition of 'consumer' (1)(b)) ('*ACL*').

Review Report).[3] The *ACL Review Report* noted that in relation to the consumer guarantees, digital products are

> *… challenging traditional concepts of consumers and traders, the traditional distinction between goods and services, ownership rights, the remedies that are expected by consumers and what 'fit-for-purpose' means in this context.*[4]

While acknowledging that UK consumer law expressly addresses the unique characteristics of digital content – such as software, e-books and other content – the *ACL Review Report* did not make any specific recommendations about this, but observed that there was 'merit in further exploring whether the *ACL* consumer guarantee provisions should be specifically tailored for digital content'.[5]

The following sections of this Report recommend changes to the Consumer Guarantee Law (CGL) in order to take into account the distinctive features of CIoT devices (and other digital products). In doing so, the Report reviews and assesses relevant recommendations relating to the consumer guarantees made by the Productivity Commission (PC) in its final report on the *Right to Repair,* which was released in October 2021.[6]

4.3 Enhancing Enforcement of Consumer Guarantees

Current proposals for reforming the CGL are focussed on measures for enhancing enforcement of the existing consumer guarantees, which were stimulated by recommendations made in the PC's *Right to Repair Report*. In its report, the PC generally accepted arguments made in some submissions that the certainty and effectiveness of the existing consumer guarantees would be best improved by enhanced enforcement. As the *Right to Repair Report* put it: 'A well-functioning consumer redress system is essential for the effective operation of the consumer guarantees'.[7] In consultations undertaken for this project, some stakeholders also emphasised that enhancing the enforcement regime has the most potential for improving the effectiveness of the consumer guarantees. This Report therefore addresses proposals for reforming enforcement before examining whether these alone are sufficient to redress gaps or deficiencies in the CGL.

[3] Consumer Affairs Australia and New Zealand (CAANZ), *Australian Consumer Law Review* (Final Report, March 2017) <https://consumer.gov.au/sites/consumer/files/2017/04/ACL_Review_Final_Report.pdf> ('*ACL Review Report*').
[4] Ibid 96.
[5] Ibid.
[6] Productivity Commission, *Right to Repair* (Inquiry Report No 97, 29 October 2021) <https://www.pc.gov.au/inquiries/completed/repair/report/repair.pdf> ('*Right to Repair Report*').
[7] Ibid 102.

Overall, the *Right to Repair Report* concluded that the costs and inconvenience of bringing actions to enforce the consumer guarantees mean that consumers are often denied redress for breaches. To address this shortcoming, the PC made the following three recommendations:

- The Australian Government should, in consultation with State and Territory Governments, amend the *ACL* to make it a contravention for suppliers and manufacturers to fail to provide a remedy to consumers when legally obliged to do so under the consumer guarantees.[8]
- The State and Territory Governments should work together to identify opportunities to enhance alternative dispute resolution options in each jurisdiction to better resolve complaints about the consumer guarantees.[9]
- The Australian Government should enable designated consumer groups to lodge 'super complaints' on systemic issues associated with access to consumer guarantees, with the complaints to be fast tracked and responded to by the ACCC.[10]

The ACCC is currently unable to take legal action against suppliers or manufacturers that refuse to provide a remedy for breach of a consumer guarantee. Following the PC *Right to Repair Report*, in December 2021, Treasury commenced a consultation on options for improving the effectiveness of the consumer guarantees.[11] The consultation canvassed the option of introducing a prohibition on suppliers failing to provide a remedy for a breach of a consumer guarantee which, in the event of a 'major failure', would be enforced by a court imposing a civil pecuniary penalty or injunction, or the ACCC issuing a civil penalty notice. As the consultation pointed out:

> *To the extent litigation is undertaken, any resulting precedents would enable greater certainty about how the law applies in specific circumstances, which would be reflected in regulator guidance, and could be followed by businesses, courts and tribunals in considering future claims.*[12]

A consumer protection regime is clearly only as effective as its enforcement. The introduction of a prohibition on failing to provide a remedy for breach of a consumer guarantee and empowering the ACCC to enforce the prohibition, would address a weakness in the enforcement regime, enhance deterrence and as the consultation document suggested, potentially improve the certainty of the

[8] Ibid Recommendation 3.4, 110.
[9] Ibid Recommendation 3.3, 107.
[10] Ibid Recommendation 3.2, 101.
[11] Department of the Treasury on behalf of Consumer Senior Officials, *Improving the Effectiveness of the Consumer Guarantee and Supplier Indemnification Provisions under the Australian Consumer Law* (Consultation Regulation Impact Statement, December 2021) <https://treasury.gov.au/sites/default/files/2021-12/c2021-224294-cgsicris_2.pdf>.
[12] Ibid 45.

existing law. Given the resource constraints facing the ACCC, there is also a case for empowering affected consumers to bring actions for enforcing a prohibition on providing a consumer guarantee remedy.

Recommendation 11

The *ACL* should be amended to introduce a prohibition *on suppliers and manufacturers failing to provide a remedy to consumers when legally obliged to do so under the consumer guarantees which, in the event of a major failure, would be enforced by the ACCC issuing a civil penalty notice, and a civil penalty or injunction issued by a court. Consideration should be given to providing consumers with the ability to initiate actions to enforce the prohibition.*

Given the limitations of the court system, the PC recommendation for enhancing alternatives to courts as a means for resolving disputes about failure to comply with the consumer guarantees has considerable potential for assisting consumers. As suggested by the PC *Right to Repair Report*, however, further investigation is needed about how best to implement this recommendation. A number of submissions to the PC inquiry raised the potential advantages of a consumer ombudsman scheme in particular industry sectors.[13] Given the complex and novel consumer issues raised by CIoT devices identified in this Report, an alternative dispute resolution scheme, such as an ombudsman scheme, has the potential to assist with resolving such complaints, especially as the Telecommunications Industry Ombudsman (TIO) does not deal with complaints about smart devices unless they are bundled with a telecommunications service provided by a carrier or internet service provider (ISP).[14]

Recommendation 12

Further consideration should be given to how enforcement of the consumer guarantees could be improved by the introduction of alternative dispute resolution schemes, such as ombudsman schemes.

4.4 Is Enhanced Enforcement Sufficient?

Although improving the enforcement regime has the potential to enhance deterrence and improve the certainty of the existing consumer guarantees, this begs the question as to whether this alone is sufficient to address the challenges of applying the existing law to CIoT devices. The mirror of the

[13] Ibid 104–105.
[14] See Telecommunications Industry Ombudsman (TIO), *Terms of Reference* (12 November 2019) <https://www.tio.com.au/sites/default/files/2020-03/TIO%20TERMS%20OF%20REFERENCE_FINAL%2012%20November%202019.pdf>.

principle that regulation is only as effective as its enforcement is that enforcement (and compliance) can only possibly be effective if the substantive law is both clear and properly targeted: no amount of enforcement can redress failings, such as gaps or imprecision, in the substantive law. In short, it is impossible to enforce a law that does not exist and to the extent that the substantive law is unclear, enforcement will be compromised. While reform of the substantive and procedural law can be complementary, it is arguable that defining the objectives of a law and ensuring that the substantive law sufficiently reflects these objectives are first order priorities. Moreover, substantive law reform, such as determining whether existing consumer guarantees should be amended or new guarantees introduced, involves policy decisions that the legislature, and not the courts, is best placed to make. Therefore, the current proposed reforms to the regime for enforcing the CGL should not proceed in isolation from analysis of the adequacy or otherwise of the consumer guarantees. The following sections of the Report therefore examine the adequacy of the CGL.

4.5 Is There a Case for a New Category of 'Digital Products'?

The guarantees that apply to the supply of a product under the CGL depend upon whether the product is characterised as a 'good' or a 'service', with nine guarantees applying to goods and three different guarantees to services. However, threshold difficulties can arise in characterising a product as a good or a service and accordingly, determining which guarantees apply.[15]

This section of the Report analyses the case for introducing a new sui generis category for 'digital products'. First, it identifies difficulties in categorising products as either goods or services under the *ACL*. Second, it explains the introduction of a distinct category of 'digital content' under UK consumer protection law. Third, it introduces the way in which digital products are dealt with under EU consumer law. This section concludes by explaining the case for introducing a new category of 'digital products' under the *ACL*.

4.5.1 'Goods' and 'Services' under the *ACL*

There has been long-standing uncertainty about whether the supply of software amounts to the supply of 'goods'.[16] At common law, and under state and territory Sale of Goods Acts, supply of

[15] Benjamin Hayward, 'What's in a Name? Software, Digital Products and Sale of Goods' (2016) 38 *Sydney Law Review* 441 ('What's in a Name?'). Similar issues have arisen under international trade law: Sam Fleuter, 'The Role of Digital Products under the WTO: A New Framework for GATT and GATS Classification' (2016) 17 *Chicago Journal of International Law* 153.
[16] See eg Sarah Green and Djakhongir Saidov, 'Software as Goods' [2007] (March) *Journal of Business Law* 161.

software embodied in a tangible medium has been regarded as the supply of goods.[17] On the other hand, the supply of software not embodied in a tangible medium, such as software downloaded from the internet, has been held not to amount to the supply of goods.[18] The *ACL* deals with this issue by defining 'goods' as including 'computer software'.[19] This means that the guarantees that apply to goods apply to the provision of software, as part of the supply of a CIoT device. For example, in *ACCC v Apple (No 4)*,[20] the Federal Court assumed that the consumer guarantees for goods applied to a software fault in iPhones and iPads. However, some CIoT devices effectively bundle goods with services, such as support or security services or with the supply of data, and this can give rise to complex issues of classification.

Some problems in determining whether a complex digital product is a good or service arose in *Australian Competition and Consumer Commission v Valve Corporation (No 3)* (*Valve (No 3)*).[21] In this case, Valve, a US-based corporation, operated an online game distribution network, which included an online support assistance service. The ACCC alleged that Valve had made misrepresentations about the guarantee of acceptable quality, which applies to goods but not services. In response, Valve claimed that it supplied a service and not a good and was therefore not subject to the acceptable quality guarantee. In addressing this argument, Edelman J, at first instance, considered the relationship between the definitions of 'goods' and 'services' in the *ACL*.

As Edelman J pointed out, the relationship between the definitions is dealt with in the definition of 'services', which includes:

> *… any rights (including rights in relation to, and interests in, real or personal property), benefits, privileges or facilities that are, or are to be, provided, granted or conferred in trade or commerce.*[22]

However, as the definition specifically excludes 'rights or benefits being the supply of goods or the performance of work under a contract', a transaction must first be characterised to determine if it is a supply of 'goods'.[23] Moreover, once a transaction has been characterised as a supply of 'goods', the effect of the exception to the definition of 'services' is that the transaction as a whole will not involve

[17] See generally Jeanie Marie Paterson, *Corones' Australian Consumer Law* (Thomson Reuters, 4th ed, 2019) 356, citing *St Albans City and District Council v International Computers Ltd* [1996] 4 All ER 481 ('*St Albans v International Computers*').
[18] *Gammasonics Institute of Medical Research Pty Ltd v Comrad Medical Systems Pty Ltd* [2010] NSWSC 267.
[19] *ACL* (n 2) s 2 (definition of 'goods').
[20] *Australian Competition and Consumer Commission v Apple Pty Ltd (No 4)* [2018] FCA 953.
[21] *Australian Competition and Consumer Commission v Valve Corporation (No 3)* [2016] FCA 196 ('*Valve (No 3)*').
[22] *ACL* (n 2) s 2 (definition of 'services' (a)).
[23] *Valve (No 3)* (n 21) [131].

the supply of a service.[24] The conclusion reached by Edelman J is reinforced by Wilson J's judgment in *Castlemaine Tooheys Ltd v Williams & Hodgson Transport Pty Ltd*, in relation to the equivalent definitions under the previous *Trade Practices Act 1974* (Cth), which held that:

> *The Act clearly contemplates that services may accompany the supply of goods in such a way as to constitute a single transaction properly described as a supply of goods. It follows that an act or series of acts, once characterised for the purposes of the Act as a supply of goods, cannot also be a supply of services …* [25]

Applying this analysis to the product supplied by Valve, Edelman J held that, as the transaction with consumers involved the supply of software, this amounted to the supply of goods and not services. In reaching this conclusion, Valve's argument that there was no 'supply' of the software, as it was provided subject to a licence, was rejected, with Edelman J pointing out that the definition of 'supply' in the *ACL* includes:

> *(a) in relation to goods – supply (including re-supply) by way of sale, exchange, lease, hire or hire-purchase.*[26]

Therefore, although the supply of online games might include the supply of services, as the 'core' of the transaction was the supply of computer games by means of software, the transaction as a whole was characterised as the supply of goods and was therefore subject to the guarantee of acceptable quality.[27] This conclusion was not challenged in an appeal to the Full Federal Court, which was dismissed in December 2017.[28]

In most cases, therefore, the supply of a CIoT device will amount to a supply of 'goods', even if the product also includes a mixed supply of software and associated services. That said, there is residual uncertainty where goods are incidentally supplied as part of the supply of a service, such as antibiotics supplied as part of the supply of medical services. While transactions such as these were characterised as the supply of services under the *Trade Practices Act 1974* (Cth), in *Valve (No 3)*, Edelman J questioned whether, given the exception in the definition of 'services' in the *ACL*, any 'incidental' supply of goods whatsoever might properly be described as the supply of goods.[29] Potentially more importantly, Edelman J acknowledged that not everything supplied by Valve might amount to the

[24] Ibid [132].
[25] *Castlemaine Tooheys Ltd v Williams & Hodgson Transport Pty Ltd* (1986) 162 CLR 395, 402.
[26] *ACL* (n 2) s 2 (definition of 'supply' (a)).
[27] *Valve (No 3)* (n 21) [157].
[28] *Valve Corporation v Australian Competition and Consumer Commission* [2017] FCAFC 224.
[29] *Valve (No 3)* (n 21) [134].

supply of a good, specifically pointing out that non-executable data and 'non-game' services, such as security protection, might not be goods.[30]

This analysis leaves ambiguities and potential gaps in consumer protection law.[31] First, as Hayward has pointed out, it is not clear whether digital content, such as digital music and e-books, is sufficiently integrated with any software, such as software used in its supply, to amount to a good.[32] Secondly, in relation to CIoT devices, there is uncertainty about whether services that are not necessarily connected to the operation of the product would be categorised as goods or as distinct services. For example, hardware might be provided by one supplier but a linked service, such as cloud storage of data that is necessary for a device to function, provided by another supplier. In that case, the transaction might be characterised as both a supply of goods and a separate supply of services, with different guarantees applying to different elements of the product. While Hayward has suggested that these issues could be addressed by extending the definition of 'goods' to include digital products as well as software,[33] they have to some extent been addressed under UK and EU law by the introduction of a new category of 'digital content'.

4.5.2 The *Consumer Rights Act 2015* (UK)

While uncertainty about whether software is a good or service is resolved by the definition of 'goods' in the *ACL*, the problem of categorisation arose again when intangible digital content, such as music, films and e-books, became accessible for downloading without being embodied in a tangible medium. Recognising these difficulties, in 2009, the UK Department for Business, Innovation and Skills commissioned Professor Bradgate to produce a report on consumer rights in digital products. The report, known as the *Bradgate Report,* was released in 2010.[34] Citing the UK Court of Appeal decision in *St Albans City and District Council v International Computers Ltd*,[35] which held that software was classified as a good when it was supplied in a physical medium but that otherwise it was not a good, the *Bradgate Report* observed that 'the case law seems to draw illogical distinctions between equivalent transactions so that like claims are not treated alike'.[36] Concluding that digital products do

[30] Ibid [156]–[157].
[31] Hayward, 'What's in a Name?' (n 21); Benjamin Hayward, 'E-books and Other Digital Products: Why Australia's Consumer Laws are Lacking' (2018) 44 *Law Society Journal* 28 ('E-books and Other Digital Products').
[32] Hayward, 'What's in a Name?' (n 15) 461.
[33] Hayward, 'E-books and Other Digital Products' (n 31) 29.
[34] Robert Bradgate, *Consumer Rights in Digital Products: A Research Report prepared for the UK Department for Business, Innovation and Skills* (Report, Institute for Commercial Law Studies, University of Sheffield, September 2010) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/31837/10-1125-consumer-rights-in-digital-products.pdf> ('*Bradgate Report*').
[35] *St Albans v International Computers* (n 17),
[36] *Bradgate Report* (n 34) 4.

not fit comfortably within the categories of 'goods' or 'services', the *Bradgate Report* recommended that contracts for their supply should be regarded as sui generis and that consumers of digital products should be afforded the same rights as purchasers of goods.[37] This approach was reflected in the *Consumer Rights Act 2015* (*CRA*), which applies a single set of rules (replacing the previous fragmented consumer protection regime) to all contracts between traders and consumers.[38] As with previous UK consumer protection laws, and similar to the former *Trade Practices Act 1974* (Cth), the 'rights' are implemented as terms implied into consumer contracts.

Chapter 3 of the *CRA* establishes rights (or implied terms) for consumers in relation to the sui generis category of 'digital content', which is distinct from both 'goods' and 'services', with section 33(1) providing that chapter 3 'applies to a contract for a trader to a consumer, if it is supplied or to be supplied for a price paid by the consumer'. The chapter 3 rights, therefore, generally apply only where digital content is supplied in accordance with a contract backed by consideration. They do not apply where the content is made available free of charge, although the rights will also apply where digital content is available for free but supplied together with paid for goods, services or other digital content.[39] Under section 2(9) of the *CRA*, 'digital content' is defined to mean 'data which are produced and supplied in digital form'. As McConnell points out, the *CRA* takes a 'holistic approach', in that it applies to digital content that is supplied in both tangible and intangible formats.[40] Moreover, chapter 3 applies to 'mixed contracts', which include both 'goods' and 'digital content', or 'services' and 'digital content'.[41] As the chapters applying to goods and services may also apply, however, and as the consumer protection rules differ depending upon the category of product, clearly this can give rise to inconsistency.[42]

As recommended by the *Bradgate Report,* the *CRA* generally applies the same rules to the supply of digital content as apply to the supply of goods. Accordingly, digital content must be of satisfactory quality,[43] reasonably fit for purpose[44] and must be as described by a trader.[45] There are, however,

[37] Ibid 62, 64.
[38] See Paula Giliker, 'The Consumer Rights Act 2015 – A Bastion of European Consumer Rights' (2017) 37 *Legal Studies* 78.
[39] *Consumer Rights Act 2015* (UK) s 33(2) ('*CRA*').
[40] Siobhan McConnell, 'Contractual Liability for Defective Internet of Things (IoT) Products – What can the UK Learn from the EU Approach?' (2020) 3 *European Journal of Consumer Law* 481, 489.
[41] *CRA* ss 1(4), (5).
[42] Christianne Wendehorst, 'Sale of Goods and Supply of Digital Content – Two Worlds Apart? Why the Law on Sale of Goods Needs to Respond Better to the Challenges of the Digital Age' (Research Paper No PE556.928, European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, 2016) 12 <https://www.europarl.europa.eu/cmsdata/98774/pe%20556%20928%20EN_final.pdf>.
[43] *CRA* s 34.
[44] Ibid s 35.
[45] Ibid s 36.

some implied terms that are specific to contracts to supply digital content. These specific obligations are introduced here, and returned to later in the Report in the section (4.6) dealing with the case for introducing specific consumer obligations for CIoT devices.

First, recognising that digital content is supplied not only in the form of a tangible medium but also by downloading or streaming, the *CRA* provides that the trader's obligations relating to supply, such as the obligation that the digital content is of satisfactory quality, extend only to where the content is supplied to the consumer's device or to a communications intermediary, such as an ISP.[46] This means that the trader is not liable for faults or problems attributable to a consumer's device or to the services of a communications intermediary. In addition, the *CRA* implies a term into consumer contracts that a processing facility, namely a facility operated by the trader for transmitting and receiving digital content, must be available to the consumer for a reasonable time, unless a time is otherwise specified in the contract.[47] For example, this means that if a consumer pays for access to an online game for a certain period, he or she should continue to have access to that game for that period.

Secondly, the *CRA* acknowledges that traders (or third parties) can modify digital content after supply but where a trader does so, the modified content must remain of satisfactory quality, be fit for purpose and be as described by the trader.[48] Where content has been modified, the new or improved features will not be in breach of the obligation to comply with a trader's description, provided the content continues to match the original description and certain other information provided by the trader.[49]

While the introduction of a specific category for digital content addresses the gap in consumer protection law for intangible content that is downloaded or streamed, it does not address the uncertainties relating to complex, hybrid CIoT devices. The issue of extending the sui generis category to products beyond digital content arose in debates relating to two EU directives, which are introduced immediately below.

4.5.3 The EU Directives

The treatment of CIoT devices under the *CRA* was not a significant issue at the time of the passage of that legislation, as such devices were not as commonplace as they have since become.[50] The classification of IoT products for the purpose of consumer protection laws did, however, become a

[46] Ibid s 39(2).
[47] Ibid s 39(5).
[48] Ibid s 40(1).
[49] Ibid ss 40(2), 36(3).
[50] McConnell (n 40) 482.

matter of contention during debates about updating EU consumer law to deal with digital content. The process for updating EU law, which was influenced by the adoption of the *CRA* in the UK, began in December 2015, when the European Commission proposed a *Digital Content Directive* (*DCD*), which was one of a number of instruments aimed at promoting a Digital Single Market.[51]

Under the first draft of the *DCD*, the directive would not have applied to:

> *… digital content integrated in goods such as household appliances or toys where the digital content is embedded in such a way that its functions are subordinate to the main functionalities of the goods and it operates as an integral part of the goods.*[52]

This meant that most CIoT devices would be dealt with as 'goods' and not 'digital content' and, accordingly, would fall under the outdated 1999 *Consumer Sales Directive* (*CSD*), which gave less rights to consumers than the proposed *DCD*.[53] The exclusion from the *DCD* gave rise to considerable criticism, including criticism of the difficult interpretative problems in determining when the functions of the content might be 'subordinate', as opposed to operating as 'an integral part' of a device.[54] As a result, the EU Parliament opposed the exclusion and subsequently, the European Commission proposed repealing the 1999 *CSD* and replacing it with a new *Sale of Goods Directive* (*SGD*), which would apply to sale of goods contracts, including goods with digital elements. The two consumer protection directives, the *DCD* and the *SGD*, were introduced in May 2019,[55] with member states having until 1 July 2021 to transpose the directives into national laws and with the directives coming into effect on 1 January 2022.

Determining how EU-level consumer protection law applies to CIoT devices depends upon an understanding of the complex relationship between the *DCD* and the *SGD*. The *DCD* applies to consumer contracts where the trader supplies or undertakes to supply digital content or a digital

[51] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*, COM(2015) 634 final 2015/0287, 2. See also European Commission, *Commission Staff Working Document: A Digital Single Market Strategy for Europe – Analysis and Evidence*, COM(2015) 192 final.
[52] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Online and Other Distance Sales of Goods*, COM(2015) 635 final 2015/0288, Recital 13.
[53] *Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on Certain Aspects of the Sale of Consumer Goods and Associated Guarantees* [1999] OJ L 171/12 ('*CSD*').
[54] McConnell (n 40) 487; Karin Sein, 'What Rules Should Apply to Smart Consumer Goods? Goods with Embedded Digital Content in the Borderland between the Digital Content Directive and "Normal" Contract Law' (2017) 8(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* 96, 98.
[55] *Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services* [2019] OJ L 136/1 ('*DCD*'); *Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Sale of Goods* [2019] OJ L 136/28 ('*SGD*').

service in return for payment or where payment is made in the form of personal data.[56] For the purpose of the directive, 'digital content' is defined consistently with the *CRA* to mean 'data which are produced and supplied in digital form'.[57] The *DCD* also includes a definition of 'goods with digital elements', which are defined as:

> *[A]ny tangible movable items that incorporate, or are inter-connected with, digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions.*[58]

Under article 3(4), the directive does not apply to digital content or services which are incorporated or inter-connected as 'goods with digital elements' and which are provided with goods under a sale of goods contract. In that case, the contract is dealt with as a sale of goods and consequently, falls under the *SGD*. The decision to include goods with a digital element within the *SGD* followed extensive debate during the EU trilogue negotiations.[59]

The relationship between the two directives is expanded upon by Recital (21) to the *DCD*, which provides, in relevant part:

> *Whether the supply of the incorporated or inter-connected digital content or digital service forms part of the sales contract with the seller should depend on the content of this contract. This should include incorporated or inter-connected digital content or digital services the supply of which is explicitly required by the contract. It should also include those sales contracts which can be understood as covering the supply of specific digital content or a specific digital service because they are normal for goods of the same type and the consumer could reasonably expect them given the nature of the goods and taking into account any public statement made by or on behalf of the seller or other persons in previous links of the chain of transactions, including the producer. If, for example, a smart TV were advertised as including a particular video application, that video application would be considered to be part of the sales contract. This should apply regardless of whether the digital content or digital service is pre-installed in the good itself or has to be downloaded subsequently on another device and is only inter-connected to the good.*

[56] *DCD* (n 55) art 3(1).
[57] Ibid art 2(1).
[58] Ibid art 2(3).
[59] Jozefien Vanherpe, 'White Smoke, but Smoke Nonetheless: Some (Burning) Questions Regarding the Directives on Sale of Goods and Supply of Digital Content' (2020) 2 *European Review of Private Law* 251, 254.

The Recital cites smart phones with pre-installed alarm or camera applications and smart watches with pre-installed applications as examples of 'goods with digital elements' that will fall under the *SGD*. Conversely, Recital (22) to the Directive provides that:

> *… if the absence of the incorporated or inter-connected digital content or digital service does not prevent the goods from performing their functions, or if the consumer concludes a contract for the supply of digital content or a digital service which does not form part of a sales contract concerning goods with digital elements, that contract should be considered to be separate from the contract for the sale of the goods, even if the seller acts as an intermediary of that second contract with the third-party supplier, and could fall within the scope of this Directive.*

In this event, the Recital gives the example of a game application downloaded to a smart phone from an app store, in which case, the sales contract for the smart phone will fall under the *SGD* while the contract for the game application will fall under the *DCD*.

Although the *SGD* does not apply to contracts for the sale of digital content or services, it applies to digital content or services that are incorporated or inter-connected with goods 'in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions (goods with digital elements)'.[60] Therefore, the *SGD* will apply to most CIoT devices but the *DCD* could still apply to digital content that is not necessary for the functioning of a device. Although McConnell claims that there may be limited practical implications as to whether the *DCD* or *SGD* applies,[61] as Vanherpe argues, there are differences between the directives, sometimes subtle, which can result in inconsistencies.[62]

The two directives include consumer warranties that are specifically designed to apply to digital content or services (under the *DCD*) or 'goods with digital elements' (under the *SGD*). As McConnell points out, compared with the *CRA*, the directives provide protections that 'are much more tailored to IoT products and which are much more explicit'.[63] This Report returns to the issue of whether or not there is a need to provide specific consumer rights for digital products after analysis of the merits of introducing a new category of consumer product distinct from goods and services.

[60] *SGD* (n 55) arts 3(3), 2(5)(b).
[61] McConnell (n 40) 489.
[62] Vanherpe (n 59) 255.
[63] McConnell (n 40) 494.

4.5.4 The Case for Introducing a New Category of 'Digital Products'

There are evident gaps in the *ACL*; non-executable digital content does not clearly fit within the categories of goods or services, and there are uncertainties in applying the distinction to hybrid CIoT products. UK and EU law have addressed this gap by introducing a new category of 'digital content', while EU law deals with the uncertainties relating to other digital products by means of the concept of 'goods with digital elements'. These reforms were introduced in response to the uncertainties in applying the distinction between goods and services to digital products and to include consumer obligations specifically tailored for digital products. Nevertheless, as illustrated by the *CRA* and the two EU directives, a new category of consumer products inevitably introduces complexities, both in defining the legal boundaries of categories and in fitting a given product within a category. For example, under EU law, determining whether the *DCD* or *SGD* applies to a digital product depends upon whether it falls within the definition of 'goods with digital elements', which can give rise to considerable interpretative difficulties, such as whether the absence of content or a service would prevent a device from performing its functions.

Arguably, uncertainties in applying the existing categories to digital products would be best dealt with by developing case law. For example, applying the 'likeness principle', it could be argued that as the supply of digital products, such as digital content and CIoT devices, shares many features with the supply of goods, the same rules should apply.[64] However, there are limits to how far the definitions of goods and services in the *ACL* can be pushed; in any case, it seems clear that the current definitions fail to apply to the supply of intangible digital content. Therefore, at the least, there is a case for remedying this, either by extending the definition of 'goods' beyond software to include non-executable digital content or by introducing a new legislative category. On either approach, a legislative definition of digital content would be required. Ultimately, the choice between the two options must depend upon the extent to which the consumer guarantees that apply to goods are equally applicable to digital content or whether, as recognised by UK and EU law, the distinctive features of the supply of digital content require specifically designed consumer protections.

If specific provision were to be made for digital content, this raises the question of whether other digital products, specifically CIoT devices, merit similar distinctive treatment. As explained in Part 1 of this Report, CIoT devices share significant features that set them apart from tangible consumer products. As also explained above, while there are uncertainties, the exception in the *ACL* definition of services makes it likely that most CIoT devices will be categorised as goods. Given the extent to

[64] On the 'likeness principle' in the context of international trade law, see Fleuter (n 15); Stewart A Baker et al, 'E-Products and the WTO' (2001) 35(1) *International Lawyer* 5.

which any categorisation of digital products necessarily raises definitional uncertainties, whether CIoT devices should be included in a new legislative category also depends upon whether there is a case for introducing consumer guarantees over and above those that currently apply to goods or services, which is dealt with in the next section of this Report. This section of the Report therefore defers further consideration of the introduction of a new category of products until after reviewing the need for new consumer guarantees.

4.6 Is There a Case for New Consumer Guarantees?

This section of the Report analyses the case for introducing consumer guarantees that are designed specifically to apply to digital products, such as CIoT devices. First, it explains the application of the most relevant current consumer guarantees to CIoT devices. It then introduces the warranties that apply specifically to digital products under EU consumer law. Drawing from this analysis, this section makes the case for at least three new categories of consumer guarantees that would apply specifically to digital products, including CIoT devices.

As indicated previously, the three most relevant consumer guarantees are as follows:

- suppliers and manufacturers guarantee that goods are of *acceptable quality* when sold to a consumer;
- a supplier guarantees that goods will be *reasonably fit for any purpose* the consumer or supplier specified; and
- manufacturers or importers guarantee they will take reasonable action to provide *spare parts and repair facilities* for a reasonable time after purchase.

The next sections of the Report analyse each of these guarantees in turn.

4.6.1 Guarantee of Acceptable Quality

The guarantee that goods must be of 'acceptable quality' replaced the implied condition of 'merchantable quality' in the *Trade Practices Act 1974* (Cth) (*TPA*).[65] To add certainty, the *ACL* introduced a definition of 'acceptable quality' that is more expansive than the definition of 'merchantable quality' under the *TPA*. Under section 54(2) of the *ACL*, goods are of 'acceptable quality' if they are:

(a) fit for all the purposes for which goods of that kind are commonly supplied;

[65] *Trade Practices Act 1974* (Cth) s 71.

(b) acceptable in appearance and finish;

(c) free from defects;

(d) safe; and

(e) durable.

The definition is subject to the 'reasonable consumer' test so that goods will meet the standard if a reasonable consumer, who is fully acquainted with the state and condition of the goods (including any hidden defects), would regard the goods as acceptable having regard to a list of statutory matters. The statutory matters required to be taken into account are:

(a) the nature of the goods;

(b) the price of the goods (if relevant);

(c) any statements made about the goods on any packaging or label on the goods;

(d) any representation made about the goods by the supplier or manufacturer of the goods; and

(e) any other relevant circumstances relating to the supply of the goods.[66]

The 'reasonable consumer' test ensures that the guarantee of acceptable quality is not an absolute guarantee that goods will be free from any defect, completely safe or of unlimited durability. In doing so, it establishes a pragmatic balance between protecting consumers without imposing unrealistic standards on suppliers.[67] However, there are particular difficulties in applying the test to CIoT devices. As noted in Part 1 of this Report, CIoT devices may be relatively opaque to consumers: the functions and nature of a device may change due to software updates, and the hybrid mix of hardware, software, data and services may make it particularly difficult for consumers to understand how a device works. Arising from these features, CIoT devices raise novel issues for the application of the guarantee of acceptable quality.

Security vulnerabilities in CIoT devices may create risks of the devices being used to cause harm, not only to the consumer but to remote third parties, such as through Distributed Denial of Service (DDoS) attacks.[68] This gives rise to questions about whether potential harms to remote parties should be taken into account in determining whether a device is reasonably 'safe' but also to broader questions about the relationship between data security and consumer protection law. What does it mean, for example, to be 'fully acquainted' with the level of security (and therefore 'safety') of a CIoT device?

[66] *ACL* (n 2) s 54(3).
[67] Paterson (n 17) 371.
[68] Mikko Hypponen and Linus Nyman, 'The Internet of (Vulnerable) Things: On Hyponnen's Law, Security Engineering and IoT Legislation' (2017) 7(4) *Technology Innovation Management Review* 5.

Moreover, the extent to which CIoT devices may be subject to fundamental change due to software updates poses challenges to elements of the current consumer protection framework, which are based on the assumption that a supplier has no power to alter a product after the point of sale. For example, the time at which goods are to be assessed as of acceptable quality is the time at which the goods are supplied to the consumer.[69] This raises questions about the application of the 'reasonable consumer' test where defects or other flaws result from updates to devices, which may be difficult or impossible for a consumer to be aware of or to predict.

The 2017 *ACL Review Report* recommended that to improve the certainty and clarity of the consumer guarantees, stakeholders should collaborate on providing guidance on when goods may not be of acceptable quality due to not being reasonably safe or not being reasonably durable.[70] In relation to guidance about product safety, the *ACL Review Report* specifically recommended guidance to clarify how the guarantee should apply where a safety issue may not eventuate for some time or render the good, as a whole, unsafe.[71] In relation to reasonable durability, the *ACL Review Report* noted consumer uncertainty about how durable a good should be, and recommended that guidance be provided for specific circumstances and goods, including where 'the good is a "smart" or hybrid product that combines different functions or blurs traditional product categories'.[72] Following from these recommendations, specific guidance on how the consumer guarantee of acceptable quality applies to the safety and durability of goods was produced by relevant stakeholders, including state and territory consumer affairs and fair trading offices.[73] However, the examples given in the published guidance are mainly confined to traditional consumer products. It therefore provides little or no assistance in addressing the novel issues posed by complex CIoT products. For example, although *the ACL Review Report* specifically identified the extent to which digital products may be 'fit-for-purpose' as an issue meriting further exploration, [74] the published guidance does not mention this issue.

Like the *ACL Review Report*, the PC's *Right to Repair Report* identified uncertainties in determining what amounts to 'reasonable durability' and considered proposals for addressing these uncertainties by introducing additional regulatory guidance.[75] While acknowledging that there might be benefits in providing guidance, on balance, the PC concluded that the potential disadvantages outweighed any

[69] See, for example, *Freestone Auto Sales Pty Ltd v Musulin* [2015] NSW CA 100.
[70] *ACL Review Report* (n 3) 14.
[71] Ibid 18.
[72] Ibid 23.
[73] Australian Consumer Law, *Guidance on the Consumer Guarantee as to Acceptable Quality and 'Safe'* (Report, December 2017) <https://consumer.gov.au/sites/consumer/files/inline-files/ACL-guidance-safe.pdf>; Australian Consumer Law, *Guidance on the Consumer Guarantee as to Acceptable Quality and 'Durability'* (Report, September 2019) <https://consumer.gov.au/sites/consumer/files/inline-files/ACL-guidance-durability_0.pdf>.
[74] *ACL Review Report* (n 3) 96.
[75] Ibid 87–91.

benefits. Instead, as explained at 4.3, the *Right to Repair Report* supported proposals for enhancing the enforcement of existing guarantees.

4.6.2 Guarantees that Goods are Fit for a Disclosed Purpose or Correspond with Description

While the extent to which goods are fit for the purposes for which goods of that kind are commonly supplied is a criterion for determining whether the goods are of acceptable quality, under sections 55 and 56 of the *ACL*, suppliers of goods guarantee that they are reasonably fit for purposes disclosed by or to the consumer. Under section 55 of the *ACL*, the supplier of goods guarantees that the goods will be reasonably fit for any purpose that is disclosed by the consumer. The scheme of the *ACL* is that the general suitability of goods is dealt with by the guarantee of acceptable quality, while section 55 deals with the suitability of goods where one or more purposes are disclosed by the consumer to the supplier, to someone involved in the negotiation process or to the manufacturer.[76] The duty imposed on suppliers by the section 55 guarantee is to supply goods that are 'reasonably' fit for the disclosed purpose, not 'absolutely' fit. However, as the Explanatory Memorandum to the *ACL* pointed out, the guarantee 'will ordinarily require a higher standard of quality than the guarantee of acceptable quality'.[77] This seems to necessarily follow from the requirement to meet the standard in accordance with the purpose disclosed by a consumer.

Under section 56 of the *ACL*, suppliers and manufacturers guarantee that their description of goods, such as in a catalogue or advertisement, is accurate. The objective of section 56 is to broadly hold suppliers and manufacturers to the 'representations' they make about their goods, however those representations are communicated.

The main difficulty posed by CIoT devices for the guarantees in sections 55 and 56 relates to the extent to which IoT products and their operation may change over time as a result of software updates or downloads. This means that a device may be fit for a purpose disclosed by a consumer at the point-of-sale, but subsequently cease to be suitable for that purpose. Similarly, a CIoT device may correspond to the description of the device at the time of sale but cease to do so after the device has been modified by changes to the software. Apart from this, given the complexity of many CIoT devices, there are questions in relation to the section 55 guarantee about when a device might be 'reasonably' fit for a disclosed purpose.

[76] Paterson (n 17) 391.
[77] Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth), [7.43].

4.6.3 Guarantee of Spare Parts and Repair Facilities

Under section 58 of the *ACL*, manufacturers guarantee they will take reasonable steps to provide spare parts and repair facilities for a reasonable time after purchase. Like other consumer guarantees, the section 58 guarantee is not an absolute guarantee to provide spare parts and repair facilities but depends upon whether or not doing so is 'reasonable' in all of the circumstances.

The increasing complexity of consumer products, especially arising from the incorporation of software into products such as CIoT devices, has given rise to economy-wide concerns about the increasing difficulties facing consumers in repairing products, which formed part of the background to the PC's *Right to Repair* inquiry. Although, as previously explained, the PC concluded that the consumer guarantees in the *ACL* are 'reasonably comprehensive and generally work well',[78] it found that it was unclear whether the guarantees, and especially the guarantee of spare parts and repair, impose an obligation to provide updates for embedded software. The *Right to Repair Report* therefore recommended that the *ACL* be amended to include 'a new consumer guarantee for manufacturers to provide reasonable software updates for a reasonable time period after the product has been purchased, with no option to limit or exclude that guarantee'.[79]

In making the recommendation, the PC explained the purpose of the proposed new guarantee was to 'clarify that consumers are guaranteed access to software updates that are *critical* to maintaining the quality (functionality, security and safety) of software-enabled products, for a reasonable time'.[80] While the report phrased its recommendation in general terms, it proposed that the 'exact nature and scope of the amendment to the *ACL* should be subject to regulatory impact analysis and stakeholder input'.[81]

In making this recommendation, the PC considered the rationale for 'opt out' clauses for the provision of spare parts and repair facilities. Under section 58(2) of the *ACL*, the repair and spare parts guarantee does not apply where the manufacturer or importer takes 'reasonable action' to ensure that the consumer, at or before the 'point-of-sale', is given written notice that spare parts will not be available or will only be available for a specified time. While the PC did not recommend removing or amending section 58(2), in supporting the proposed new guarantee it recommended that it not be subject to a similar 'opt out' clause. The reason given for this distinction was that:

[78] Productivity Commission, *Right to Repair Report* (n 6) 79.
[79] Ibid 98.
[80] Ibid (emphasis in original).
[81] Ibid.

> *… whereas the 'need' to access spare parts may only affect a small proportion of the consumer base (such as where a part has broken), the need for software updates is likely to be one that affects the functionality or operation of an entire product line.*[82]

The PC's analysis of the case for introducing a new guarantee for reasonable software updates acknowledges one respect in which the guarantee of spare parts and repair facilities falls short in protecting purchasers of hybrid products, such as CIoT devices. However, given the limits of the terms of reference for the PC inquiry, it begs the question of whether there is a need for additional guarantees. Therefore, the next section of this Report introduces the specific obligations imposed on the supply of digital products under the two relevant EU directives to examine the extent to which they support a case for additional guarantees under *ACL*.

4.6.4 Warranties for Digital Products under EU Consumer Law

As noted at 4.5.3, the *SGD* and *DCD* impose obligations on suppliers that are specifically tailored to digital products. This section of the Report explains the obligations imposed on the supply of digital products by the directives. To understand the obligations, it is important to first appreciate how the directives distinguish between subjective requirements for conformity with the consumer obligations and objective requirements. While subjective requirements are those agreed to in the consumer contract, objective requirements refer to the general expectations that consumers should be able to have for a consumer product.

In relation to subjective requirements for conformity, the *SGD* provides that goods (which include 'goods with digital elements') must:

- be of the description, type, quantity, and possess the functionality, compatibility, interoperability and other features, as required by the sales contract;
- be delivered with all accessories and instructions, including on installation, as stipulated by the sales contract; and
- be supplied with updates as stipulated by the sales contract.[83]

In addition to the subjective requirements, the objective requirements for conformity include that goods must:

[82] Ibid.
[83] *SGD* (n 55) art 6(a), (c), (d).

- be fit for the purposes for which goods of the same type would normally be used, taking into account, where applicable, any existing Union and national law, technical standards or, in the absence of such technical standards, applicable sector-specific industry codes of conduct;
- where applicable, be delivered along with such accessories, including packaging, installation instructions or other instructions, as the consumer may reasonably expect to receive; and
- be of the quantity and possess the qualities and other features, including in relation to durability, functionality, compatibility and security normal for goods of the same type and which the consumer may reasonably expect given the nature of the goods and taking into account any public statement made by or on behalf of the seller, or other persons in previous links of the chain of transactions, including the producer, particularly in advertising or on labelling.[84]

In addition, in relation to 'goods with digital elements', the *SGD* specifically provides that 'the seller shall ensure that the consumer is informed of and supplied with updates, including security updates, that are necessary to keep those goods in conformity' for a certain period of time.[85] The applicable period of time is either, where the sales contract provides for a single act of supply, the time the consumer may reasonably expect or, where the sales contract provides for a continuous supply, either two years from the original supply of goods or a longer period of time specified in the contract.[86]

The conformity requirements for digital content or digital services under the *DCD* are similar to those for goods with digital elements under the *SGD* but with some potentially important differences. For example, in relation to subjective conformity, the *DCD* includes the obligation that digital content or a digital service 'be updated as stipulated by the contract'.[87] In relation to objective conformity, the *DCD* provides that digital content or a digital service must 'comply with any trial version or preview of the digital content or digital service, made available by the trader before the conclusion of the contract'.[88] In addition, the directive provides that unless the parties have agreed otherwise, 'digital content or a digital service shall be supplied in the most recent version available at the time of the conclusion of the contract'.[89] Finally, the *DCD* specifically provides that a lack of conformity resulting from incorrect integration of content or a service into the consumer's digital environment will be a

[84] Ibid art 7.1(a), (c), (d).
[85] Ibid art 7.3.
[86] Ibid art 10(2).
[87] *DCD* (n 55) art 7(d).
[88] Ibid art 8.1(d).
[89] Ibid art 8.6.

breach of a trader's obligations, where either the trader was responsible for the integration or the incorrect integration was due to shortcomings in instructions provided by the trader.[90]

Therefore, the directives distinguish between the consumer warranties that apply to the supply of digital content on the one hand, and 'goods with digital elements' on the other. First, under the *DCD*, acknowledging that digital material may be subject to modification, there is a requirement that unless the parties agree otherwise, the most recent version of digital content or a digital service must be supplied at the time of contract.[91] However, as this obligation is not included in the *SGD*, it does not apply to 'goods with digital elements', meaning most CIoT devices, despite such devices being subject to modification. Secondly, recognising that digital material may need to be updated, the *DCD* includes an obligation to ensure consumers are informed of and supplied with updates, including security updates, where either the consumer contract provides for continuous supply for a period of time or the consumer would reasonably expect updates.[92] In similar terms, the *SGD* includes an obligation to inform consumers of and supply updates for goods with digital elements.[93] However, there is a difference between the two directives in relation to liability for a failure to provide updates: while under the *DCD*, updates must be provided throughout the period of supply, under the *SGD*, there is a capped two year liability period for goods with digital elements, unless the contract provides otherwise.[94]

The general obligations relating to the quality of consumer goods or services under the two directives also include modifications designed to take into account the specific features of digital products but which again differ. For example, under the *DCD*, the requirement that digital content complies with its description is extended by the express requirement that digital content or a digital service complies with any trial version or preview.[95] This is not matched for goods with digital elements under the *SGD*; but under both directives, technical standards or applicable industry codes of conduct are to be taken into account in determining whether a product is fit for the purposes it would normally be used for.[96]

The differences between the warranties that apply to digital content and goods with digital elements, despite the extent to which the warranties are designed to address features shared by these digital products, exposes the artificiality of distinguishing these two categories of product. As explained in the next section of this Report, however, the specific warranties imposed by the EU directives illustrate

[90] Ibid art 9.
[91] Ibid art 8(6).
[92] Ibid art 8(2).
[93] *SGD* (n 55) art 7(3).
[94] Ibid art 10(2).
[95] *DCD* (n 55) art 8(1)(d).
[96] Ibid art 8(1)(a); *SGD* (n 55) art 7(1)(a).

at least three areas where the distinctive features of digital products explained in this article presents challenges for the existing consumer guarantees and may justify new specific guarantees: software updates, security and integration of elements of devices.

4.6.5 The Case for New Consumer Guarantees

Consumers should be entitled to expect an equivalent level of protection for products, such as CIoT devices, to that which applies to other consumer products. In relation to digital products, these expectations include that: any software, including security software, should be up to date and regularly updated; the devices should be reasonably secure from intrusions; and the elements of a hybrid device – including software, hardware, data and associated services – should be properly integrated. The extent to which these legitimate expectations are met by the current consumer guarantees is, at best, unclear.

As explained in the PC's *Right to Repair Report*, for any products that incorporate software elements, software updates may be necessary to correct faults, address security vulnerabilities, maintain functionality and add new features or improvements.[97] In other words, software updates are commonly essential for the continued viability and operation of digital products. Yet as the PC found, the existing guarantees in the *CGL* fail to clearly incorporate a guarantee of software updates. For example, it is unclear whether a failure to provide a guarantee of software updates would mean that a CIoT device is not fit for the purpose for which it was supplied, especially given that the time for goods to be assessed as of acceptable quality is the time they are supplied. Unsurprisingly, under EU law, both the *DCD* and *SGD* include obligations requiring software updates for digital products. Any debate about an obligation to provide software updates is therefore not about whether the existing guarantees should be clarified or extended – that much seems generally accepted – but about the elements of a new guarantee, including the duration of the obligation.

From the point of view of consumers, the most significant safety issues facing purchasers of connected products, such as CIoT devices, concern security vulnerabilities. The importance of security for purchasers of CIoT products is illustrated by the Ring Doorbell case study detailed below. In considering the relationship between the recommendation to introduce a guarantee relating to software updates and more general security obligations in its *Right to Repair Report*, the PC acknowledged that 'to fully achieve broader cyber security objectives additional measures may be needed beyond the Commission's recommended consumer policy changes'.[98] However, the report did

[97] Productivity Commission, *Right to Repair Report* (n 6) 96.
[98] Ibid 98.

not engage in systematic analysis of the application of the existing guarantees to the security of connected products, including the guarantee of acceptable quality. As previously indicated, the guidance produced by the ACCC on the guarantee of reasonable 'safety' as part of the guarantee of acceptable quality does not raise issues relating to the cyber security of connected devices. The extent to which the guarantee of reasonable safety includes a guarantee of reasonable security is therefore unclear. While in order to satisfactorily protect legitimate consumer expectations, this might suggest the need for a new guarantee of reasonable security for connected products, it does raise issues of regulatory competence: consumer regulators, such as the ACCC, are not necessarily best placed to evaluate device security. Conversely, as security is likely the single most important issue facing consumers of connected devices, it is arguable that to remain credible, consumer regulators must address consumer security concerns, including by upskilling. This suggests that there is a good case for introducing a new guarantee of reasonable security as part of any reforms aimed at ensuring that the consumer guarantees remain relevant to the most important issues facing consumers.

As this Report has explained, the complexity of CIoT devices can create difficulties in integrating elements of a hybrid product, leading to defects or deficiencies in the performance of a product. Failure of elements of a complex device to be properly integrated could amount to the device not being fit for the purpose for which it was supplied, nor reasonably free from defects, and therefore failing to comply with the guarantee of acceptable quality, but this is untested. Moreover, as the time for assessing compliance with the obligation of acceptable quality is the time of supply, the guarantee does not apply to integration problems arising from software updates following purchase. The EU *DCD* incorporates a broader integration obligation in that it requires integration of digital content or a digital service with the consumer's 'hardware or software environment', meaning the hardware, software or network connection used to access or make use of the content or service.[99] In relation to at least some CIoT devices, their operation will depend upon interoperability with a broader digital ecosystem; yet it is doubtful whether a failure of a device to integrate with other devices or services would breach the current guarantee of acceptable quality. Consequently, there seems a good case for introducing a new guarantee requiring digital products to be properly integrated that would extend, where necessary, to reasonable integration with a broader digital ecosystem.

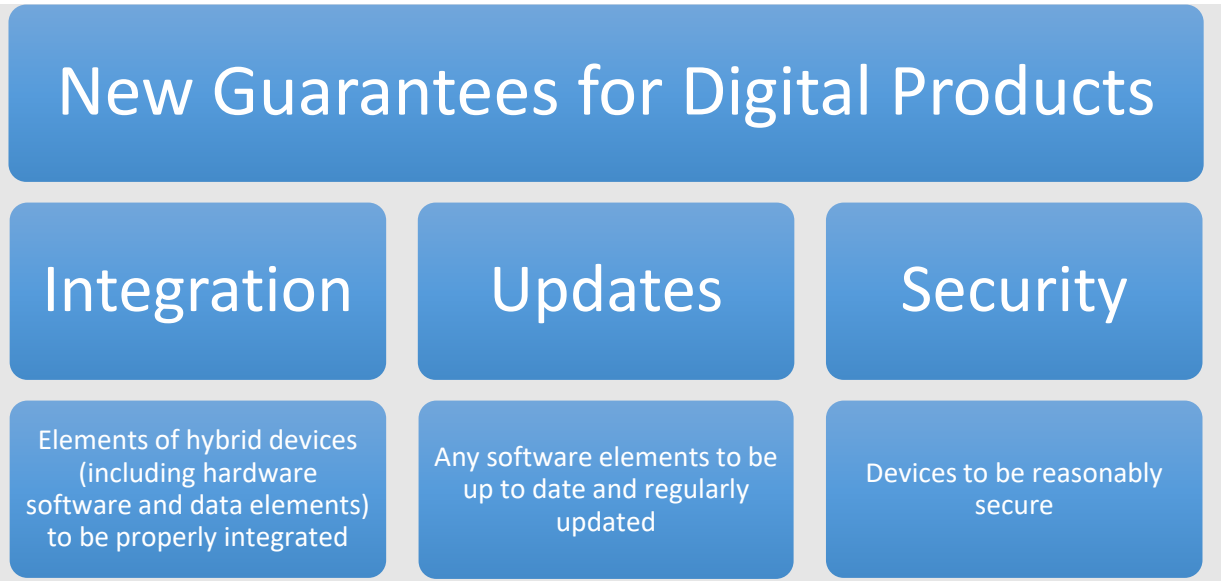
Whether digital products require amendments to the existing consumer guarantees or new guarantees depends upon an assessment of the extent to which they differ from traditional, tangible consumer products. After all, many consumer products – from cars to toys to coffee machines – have long included software elements, which poses challenges for consumer protection. However, CIoT

[99] *DCD* (n 55) art 2(9).

devices are characterised by features that have never existed in other consumer products: they are always connected, they may be remotely modified following purchase and they are more complex than other products. As this Report has explained, these features can exacerbate existing consumer harms, such as harms arising from product complexity, but can also create potential new harms, such as harms arising from inadequate device security. Taken together, the distinctive features of CIoT products and the associated potential harms suggest the need for new consumer guarantees that are designed to address these harms.

The proposed new guarantees are set out in the following diagram.

Figure 5 Elements of New Guarantees for Digital Products: Integration, Updates and Security



CASE STUDY: Ring Doorbell

Compliance with industry standards or relevant codes of practice may assist in securing consumer protections by ensuring that CIoT devices conform to industry security standards. Ring characterises its approach to privacy and security as 'defense-in-depth' – ensuring that protections are layered in a way that no one failure compromises the security of a system.[100] *However, there are a number of examples where Ring services have been compromised resulting in unauthorised access to home cameras. For example, in 2019-2020 numerous complaints were raised regarding the ability of hackers to access various Ring products, and monitor who entered and left a house and even speak to occupants via security cameras.*[101] *Hackers have also been able to intercept WiFi passwords due to insecure transmission of details during device configuration.*[102] *A number of these cases have proceeded to litigation in the US.*

The vulnerability of Ring devices, as shown by these cases, have been variously attributed to a failure by consumers to use two factor authentication and poor encryption protocols on the part of Ring. Prior to February 2020, users were not required to use two factor authentication to secure their accounts and this was simply available as an option. From 18 February 2020, two step verification of accounts became mandatory. From January 2021, end-to-end encryption was also available as an option for users seeking additional security. This is provided as an option because the use of end-to-end encryption limits some user features, and therefore requires a trade-off between security and product features.[103] *Videos that are end-to-end encrypted are automatically excluded from any requests made by law enforcement.*[104]

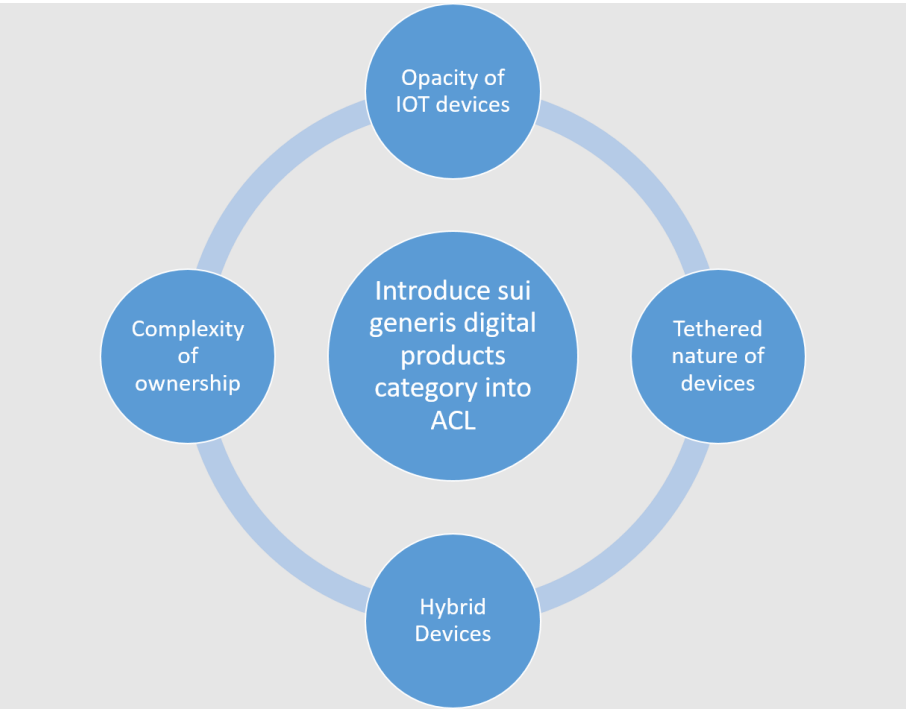
The use of two factor authentication and end-to-end encryption is consistent with industry standards for CIoT devices. However, the fact that the use of end-to-end encryption is optional due to a lack of functionality that may arise as a result demonstrates the need for security by design principles to inform product development. It seems unlikely that a failure to provide end-to-end encryption would breach the guarantee of acceptable quality. Depending upon industry practices, however, it might breach a guarantee of reasonable security.

[100] Ring, *End-to-End Encryption* (White Paper, January 2021) 3, n 2 <https://assets.ctfassets.net/a3peezndovsu/7bwgu7ybi1XoyH61pDraYT/94e4bab9347d4abe07f8d843fdfd4bd4/Ring_Encryption_Whitepaper_FINAL.pdf> ('*Ring White Paper*').
[101] ABC News, 'New Security Warning for In-Home Smart Cameras' (You Tube, 13 December 2019) <https://www.youtube.com/watch?v=GnIIEQt_QFo&t=155s>; Paul Black, 'Ring Hacked: Doorbell and Camera Security Issues' *NordVPN* (Blog Post, 4 June 2020) <https://nordvpn.com/blog/ring-doorbell-hack/>.
[102] Zack Whittaker, 'Amazon Ring Doorbells Exposed Home Wi-Fi Passwords to Hackers' *Tech Crunch* (Web Page, 8 November 2019) <https://techcrunch.com/2019/11/07/amazon-ring-doorbells-wifi-hackers/>.
[103] *Ring White Paper* (n 100).
[104] Ibid 12.

4.7 Recommendations for Reform of the Consumer Guarantees Law (CGL)

As explained at 4.5.4, any attempt to classify products, especially complex products, will give rise to definitional uncertainties. As further explained, however, there is currently a gap in the law, at least inasmuch as the *ACL* does not apply to non-executable digital content. Moreover, as explained at 4.6.5, the uncertainties in the application of the current consumer guarantees to CIoT products, as well as the distinctive features of those products, support the case for introducing new consumer guarantees designed specifically for these products. The features of CIoT devices that, taken together, challenge the distinction between goods and services are set out in the following diagram, while the difficulties in applying the distinction between goods and services to CIoT devices are illustrated by the Ring Doorbell case study.

Figure 6 Elements of Proposed Sui Generis Category of Digital Products



CASE STUDY: Ring Doorbell

The language in the Ring Doorbell Terms of Service (ToS) demonstrates some of the difficulties in applying the distinction between goods and services to CIoT devices. In this case, the supply of the goods (that is, the doorbell) is inextricably linked with services (the application, the web service, etc). Without use of the services, the good will not function properly. While the ToS defines the Ring software as a 'service', it is a 'good' for the purpose of the ACL. Therefore, taking into account the transaction as a whole, the consumer guarantees applicable to 'goods' will apply to both the 'products' (as they are defined in the Ring ToS) and the software. But, applying the reasoning in Valve (No 3), there may potentially be service elements that will not be characterised as goods. Furthermore, in the event of security being compromised, there are uncertainties about whether this would breach the guarantee that goods must be of acceptable quality.

From the perspective of consumers, it is preferable for a uniform set of consumer guarantees to apply to a single product, even if that product is a complex hybrid of hardware, software and associated services, and regardless of whether different elements of the product are subject to different contracts. Moreover, consumer guarantees should be tailored to the characteristics of the product, as much as possible. The combination of the uncertainties in applying the distinction between goods and services to CIoT devices and the desirability of introducing bespoke consumer guarantees presents a good case for introducing a new sui generis category of digital products.

While this Report supports the introduction of a new sui generis category of digital products, the definitions and distinctions drawn by current UK and EU laws provide little practical assistance. For example, the similarities between digital content and CIoT devices suggest that they should both fall within the single category of 'digital products'. That said, there are complexities. For example, the introduction of a new category of digital products would necessarily have to be accompanied by a means for determining whether elements of a complex product are sufficiently integrated into the product so that they are part of that product, and when they are not linked in a way that means they are a separate product. The latter might, for instance, be the case with at least some apps that are separately downloaded to a CIoT device.

This Report therefore makes the following recommendations for reform of the CGL.

Recommendation 13

A new sui generis category for digital products, distinct from 'goods' and 'services', should be introduced to the ACL. The new category should include both digital content and CIoT devices. A new category is justified because digital products are sufficiently different from traditional consumer products to merit new, specifically tailored consumer guarantees. A new category would also reduce current uncertainties in determining whether elements of a CIoT device are 'goods' or 'services'. In introducing a new legislative category, care is needed in defining the category; especially in determining when elements of a complex product are sufficiently integrated so as to form part of that product.

Recommendation 14

In association with the introduction of a new category of digital products, a set of consumer obligations should be developed for these products. The obligations should at least include the following: any software elements, including security software, should be up to date and regularly updated; the devices should be reasonably secure from intrusions; and the elements of a hybrid device – including software, hardware, data and associated services – should be properly integrated.

4.8 Pre-Contractual Information Disclosure

This project has found that the limited availability of consumer information regarding CIoT devices is a significant issue for consumers (and the organisations who represent their interests), as well as for more meaningful regulation by consumer protection authorities. As illustrated by the case studies in this section of the Report, research undertaken for this project indicates that there are serious problems with the accessibility and interpretability of terms and conditions for CIoT devices, which are associated with the complex 'nest' of contracts facing consumers. While acknowledging that consumers are faced with information overload and usually do not consult terms and conditions, there are clear advantages in requiring better practices in the disclosure of terms and conditions by suppliers. The advantages include greater transparency and, for consumers that consult terms and conditions, more information for determining whether or not to enter a contract.[105] As more information is not necessarily better information, the position is more complex than simply providing consumers with all information. As Noto La Diego and Walden argue, while transparency is generally

[105] Geriaint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking EU Law* (Routledge, 2018) 96–97.

integral to contractual fairness, the need for transparency within a contract ultimately depends upon the nature of the product and the particular contractual provision.[106] Above all, however, transparency and accessibility of terms and conditions is important for detecting terms that are potentially unfair, which is dealt with in the next section of the Report.

Although there are requirements for mandatory pre-contractual disclosure of certain terms in other jurisdictions,[107] the *ACL* does not currently require pre-contractual disclosure of key terms. However, for many of the case studies, it was difficult or not possible to locate contractual information relevant to consumers prior to purchase. Currently, the only way to obtain warranty information about many CIoT products is actually to purchase the product. Often following purchase, consumers must download linked software that contains additional terms and conditions of use, which is not accessible prior to purchase. The difficulties in accessing potentially problematic terms prior to purchase are illustrated by the Tapo Smart Light Bulb case study.

CASE STUDY: Tapo Smart Light Bulb

The Tapo Smart Light Bulb is available both online and in store. The device was purchased in-store in a shrink-wrapped package that stated that the light bulb has a two-year warranty and directs consumers to a website for 'support and warranty' information. However, that page does not provide details of the warranty terms. These are supplied inside the packaging. The terms provide a limited warranty for 'manifest defects in material or workmanship' but also provide further information not disclosed at purchase, including that claimants are responsible for 'shipping charges, insurance and other transportation-related expenses' in claiming the warranty. Given the relatively low cost of the product (under $20), it is not clear if making a warranty claim would be more expensive than purchasing a new product.

In multiple case studies, consumers were first required to accept both terms of use and privacy policies if they wished to use the relevant CIoT products. Consumers were then asked to accept further user agreements and privacy policies containing additional provisions that reflected privacy obligations of

[106] Guido Noto La Diega and Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 7(2) *European Journal of Law and Technology* 1, 19. Noto La Diega and Walden argue that where IoT applications are 'more intimate' to a user's well-being 'a higher standard of transparency could be imposed on providers under unfair contract terms rules': at 19.

[107] European Union directives mandate pre-purchase provision of certain information: see *Council Directive 2011/83/EU on Consumer Rights* [2011] OJ L 304/64; *Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services* [2019] OJ L 136/1; *Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Sale of Goods, Amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC* [2019] OJ L 136/28.

international jurisdictions (such as the GDPR), before they were able to use the apps that permitted access to key features associated with the device. Suppliers commonly do not make warranty information readily available before purchase for devices supplied through online purchase agreements, including terms of return. In some cases, such as the August Smart Lock Pro, warranty information is available online only in relation to jurisdictions such as the US or Europe, but not for Australia. The difficulties facing consumers are illustrated by the VTech Smartwatch and August Smart Lock Pro case studies immediately below.

CASE STUDY: VTech Smartwatch

For the DX Smartwatch, Australian warranty information is provided within the packaging on purchase of all VTech products. However, it is not readily available on the VTech Australia website or on the websites of authorised suppliers of VTech products in Australia. There are no specific return provisions if users do not accept an additional privacy policy (based on the GDPR) and the terms of use for the Learning Lodge app. The Learning Lodge app permits consumers to access all the features of the DX smartwatch. The additional terms include a requirement that children using the app must be supervised by parents during use.

CASE STUDY: August Smart Lock

For the August Smart Lock, the only available warranty information is in relation to the US and Canada. When the device is imported to Australia through Amazon US, there is no warranty provided for Australian purchasers. Although users who refuse to accept the end user agreement are given three months to return the product for a refund, this applies only to American and Canadian purchasers.

4.8.1 Pre-Contractual Disclosure under the *Fair Trading Act* (NSW)

A pre-purchase requirement for disclosure of key terms has recently been introduced into the New South Wales *Fair Trading Act 1987* (NSW).[108] The primary obligations provide that:

> *[A] supplier must, before supplying a consumer with goods or services, take reasonable steps to ensure the consumer is aware of the substance and effect of any term or condition relating to the supply of the goods or services that may substantially prejudice the interests of the consumer.*[109]

[108] *Fair Trading Legislation Amendment (Reform) Act 2018* (NSW).
[109] *Fair Trading Act 1987* (NSW) s47A(1).

The examples given are non-exhaustive and include those related to exclusion of liability, exit fees and balloon payments, customer liability for delivered goods that are damaged, and terms that permit suppliers to provide data about or from a consumer to a third party.[110] The regulations can then provide further guidance regarding reasonable steps for suppliers to ensure consumer awareness of the substance and effect of terms and conditions, the type of terms that may or do not substantially prejudice consumer interests, other requirements and exemptions.[111]

The regulations also provide information standards for the supply of goods and services with specific details about the information that needs to be supplied and there are penalties for non-compliance with the standards. These information standards have been applied to specific industries. The *Fair Trading Regulation 2019* (NSW) contains information standards for funeral goods and services and fuel price signs at service stations, as well as a code of conduct for motor vehicle insurers and repairers. For funeral goods and services, the relevant standard specifies information that needs to be prominently displayed at the place of business and on a public website, as well as specific individualised cost information that needs to be provided before agreements are entered into.[112]

At the time of writing this Report, it is too soon to comment on compliance with the new obligations as they were introduced in July 2020, with the grace period having expired only at the beginning of 2021.

4.9 Recommendations for Requiring Pre-Contractual Information Disclosure

This Report recommends that in order to promote greater transparency and accessibility to terms and conditions, a disclosure requirement modelled on the New South Wales mechanism should be introduced to the *ACL*. This should include a general disclosure obligation for critical terms and conditions in a form that can be understood by consumers prior to purchase, as well as an obligation to notify consumers of changes to these terms after purchase.[113] Bearing in mind that some terms are more important to consumers than others, the information standards could give further specific guidance about the type of terms that suppliers should provide clear information about to consumers. The standards should take the form of regulations so they can be readily revised in response to the changing digital environment.

[110] Ibid s 47A(2).
[111] Ibid s 47A(3).
[112] *Fair Trading Regulation 2019* (NSW) pt 2 div 2.
[113] See below discussion that a term allowing unilateral amendments without notice should be regarded as unfair.

These reforms are especially important for consumers of digital products, including CIoT devices. In part, this is due to the difficulties in accessing and understanding the terms arising from the complexities of interrelated or nested agreements.[114] If a separate information standard were to be developed in relation to digital products (including CIoT devices), the law could require disclosure of those terms that are most relevant to the problems faced by consumers, as identified in this Report. To address the problem of terms and conditions being accessible only after purchase, clear explanations of the substance of any prescribed terms should be made available to consumers before purchase. In addition, at least in relation to digital products, there should be transparent disclosure of the full contractual terms and conditions on a publicly available website.[115] This obligation should not be onerous for suppliers of digital products, who will have an online presence.

While obligations for greater disclosure of terms and conditions are not a panacea and, as explained below, must be linked to measures aimed at promoting accessibility, there are clear benefits to the approach outlined in this section of the Report. First, as mentioned above, a mandatory disclosure requirement could help redress the power imbalance between suppliers and consumers, at least for those consumers that consult the terms and conditions. Second, it could assist with the regulatory activities of consumer protection authorities, including the ACCC, as it would permit them to more easily detect contractual terms that are unfair or unconscionable. Third, mandatory disclosure of warranties – as well as of consumer, privacy and security protections – would reinforce other recommendations in this Report, such as those relating to unfair contract safeguards. Fourth, it would also assist consumer organisations to identify problematic features of digital product contracts and warn consumers. As explained below, this could be one component of a more general shift to a proactive approach to protecting consumers. Fifth, increased transparency could also complement consumer education measures. Educating consumers about the consequences of problematic clauses, such as those permitting unilateral changes to material terms without sufficient notice, can assist in redressing the power imbalance between suppliers and consumers – but this is impossible unless consumers have adequate access to terms and conditions.

Pre-contractual disclosure obligations are only effective if terms and conditions are both understandable and accessible by consumers. In relation to comprehensibility, there are considerable developments in applying design principles to contracts, including the incorporation of visual

[114] Noto La Diega and Walden (n 106) criticise the absence of transparency that results for the 'average consumer' in circumstance where there are 'complex dependencies and interaction between the product, service and software agreements': at 19.
[115] This approach is consistent with the current obligations for disclosure of privacy policies found in Australian Privacy Principle 1 in the Australian privacy regime: *Privacy Act 1988* (Cth) sch 1.

elements.[116] These advances could be reinforced by regulatory obligations, possibly included in regulations, such as requirements to include summaries of particular problematic types of terms, or even check-boxes linked to prescribed information that a consumer must acknowledge. In relation to accessibility, any disclosure requirements must be accompanied by measures to assist accessibility. This project considered the potential for establishing a centralised online repository of terms and conditions for CIoT devices. The motivation for this was the inordinate difficulty experienced in accessing the complex nest of terms and conditions for CIoT devices. An alternative approach would be to encourage the development of consumer-centred tools for locating and analysing terms and conditions.

To date, RegTech – the use of technology such as data analytics and AI for the purposes of regulation – has been used mainly to assist business and regulators with compliance. However, there is untapped potential for RegTech tools to be used to empower consumers. As Paterson has pointed out:

> *The growth in the standards of digital design and AI systems should be able to help customers to navigate their contracts; identifying key terms and providing reminders of critical time periods are exactly the kind of tasks these new technologies are being used for at the top end of the corporate market. There is clearly scope for dynamic, creative and innovative ways for this technology to be applied in the consumer market as well.*[117]

On the basis that it is better to prevent consumer harms than to attempt to rectify them after the fact, the use of appropriate RegTech tools could assist consumers in both locating relevant terms and conditions and interpreting them, including in interpreting complex, interconnected contracts. For example, in conjunction with regulatory obligations mandating greater disclosure, applications could be developed to search and return relevant terms and conditions. This could assist in addressing problems of disclosure without accessibility. As accessibility is of limited assistance if contracts remain difficult for consumers to understand, accessibility tools would need to be complemented by tools that identify the most important terms and translate them into comprehensible language. In short, there is potential for RegTech tools to be used by both consumers and regulators as part of a more proactive approach to consumer protection aimed at identifying problems – or in this case, problematic terms and conditions – at source. Further tools could be developed that facilitate comparisons between terms and conditions for similar digital products. This could strengthen competition between suppliers in the terms and conditions offered to consumers, consistent with the

[116] See, generally, Margaret Hagen, *Law by Design* (online, 2020) <https://lawbydesign.co/>.
[117] Jeannie Paterson, 'RegTech and the Future of Customer Protection', *Pursuit* (online, University of Melbourne, 8 September 2017) <https://pursuit.unimelb.edu.au/articles/regtech-and-the-future-of-customer-protection>.

ACL objectives of ensuring that consumers are sufficiently well-informed to benefit from effective competition. While these tools are not yet available, the building blocks are being developed. Legal obligations for pre-contractual disclosure of terms and conditions should therefore be seen as part of a potential emerging ecosystem in which technological tools could eventually be used to empower consumers, and overcome the current problems of relatively inaccessible contractual information and opaque terms and conditions.

Recommendation 15

Suppliers of digital products, including CIoT devices, should be required to ensure that clear explanations of prescribed contractual terms, including warranties, are made available to consumers before purchase. Full contractual terms and conditions should also be publicly available on supplier websites. The conditions for complying with these obligations should be specified in regulations.

Recommendation 16

Additional measures should be investigated for improving access to, and understandability of, terms and conditions for CIoT devices. Such measures could include tools to assist in locating consumer contracts that, under Recommendation 15, would be legally required to be disclosed before purchase. In addition, measures should be investigated to assist consumers in identifying and interpreting key contractual terms, including terms in complex, interconnected contracts for CIoT devices and market comparisons between supplier terms and conditions.

4.10 'Unfair Contract' Safeguards

The *ACL* includes two general safety nets that set flexible standards, as opposed to prescriptive rules, that can be applied to protect consumers against unfair contracts and associated practices:

- a statutory prohibition on unconscionable conduct; and
- the 'unfair contract terms law', which can render void unfair terms in standard form consumer contracts.

While the prohibition on unconscionable conduct mainly addresses procedural unfairness, which means a lack of fairness in the process of contractual formation, the unfair contracts law mainly addresses substantive unfairness, which means unfairness in the terms themselves.[118]

As this Report has explained, the complexity and hybrid nature of CIoT devices presents considerable challenges for consumer protection law. This complexity can result in a 'nest' of contracts and potentially multiple contracts with multiple parties involved in the IoT supply chain. As illustrated by the case studies in Part 2 of this Report, this is often exacerbated by the way in which suppliers present terms and conditions to consumers. In addition, the supply of CIoT devices is rarely a simple 'one-off' supply of a product. Rather, the dependence of most devices upon software updates places consumers and suppliers in an ongoing relationship. As circumstances change, this raises questions about how the terms and conditions of a consumer contract may be amended, and especially whether terms and conditions should be able to be unilaterally amended without the agreement of consumers, and what steps should be taken to notify consumers of changes to the terms and conditions.

4.11 Statutory Unconscionability

Section 21 of the *ACL* prohibits conduct in trade or commerce that is, in all the circumstances, unconscionable. The prohibition applies to conduct in the supply or acquisition of goods or services, and therefore applies to contracts for the supply of CIoT devices.

Statutory unconscionability under the *ACL* establishes a broad standard of commercial conduct, which requires the court to determine whether the apparent autonomy of parties to enter into a contract should be over-ruled. Giving meaning to, and applying, a broad standard such as statutory unconscionability can be contentious and poses considerable challenges.[119] This project considered proposals for improving certainty about how the broad standard applies by, for example, introducing statutory presumptions. However, in response to feedback on the practicality of these proposals, this Report focusses on the potential advantages of introducing a new prohibition on 'unfair trading' practices.

[118] Jeannie Paterson, 'The Australian Unfair Contract Terms Law: The Rise of Substantive Unfairness as a Ground for Review of Standard Form Consumer Contracts' (2009) 33(3) *Melbourne University Law Review* 934.
[119] Jeannie Paterson, 'Unconscionable Bargains in Equity and Under Statute' (2015) 9 *Journal of Equity* 188.

4.12 Prohibition of 'Unfair Trading' Practices

As a 2008 PC report pointed out, statutory unconscionability not only lacks clarity but it is costly and slow to use.[120] Therefore, consideration needs to be given to whether there is conduct outside of the scope of statutory unconscionability that should be prohibited, or whether there are alternatives that could assist in dealing with potential procedural unfairness in CIoT contracts.

In its *DPI* (*Digital Platforms Inquiry*), the ACCC identified a range of practices of platforms that are potentially detrimental to consumers but which do not fit neatly under existing consumer protection law.[121] The practices are driven mainly by the data-driven business model of collecting large amounts of consumer data, analysing the data and targeting the consumer with behavioural advertising. Given the extent to which CIoT providers apply versions of the data-driven business model, the ACCC's analysis is as applicable to the provision of CIoT devices as it is to the practices of digital platforms. As the ACCC pointed out, 'these areas of concern exist, not just in the context of digital platforms, but across all businesses that are involved in data-driven industries'.[122]

The concerning practices identified by the ACCC included:

- Changing terms on which products or services are provided without reasonable notice or the ability to consider the new terms, including in relation to products with subscriptions or contracts that automatically renew.
- Adopting business practices to dissuade a consumer from exercising their contractual or other legal rights, including requiring the provision of unnecessary information in order to access benefits.
- Inducing consent or agreement by very long contracts, or providing insufficient time to consider them, or all or nothing 'click wrap' consents.

To address these practices, the ACCC recommended introducing a prohibition on unfair trading practices in the *ACL*, which would draw on experience with similar prohibitions in the EU and the US.[123] However, in making this recommendation, the ACCC noted that the 'scope of such a prohibition should

[120] Productivity Commission, *Consumer Policy Framework Review Report* (n 1) v 1, 34.
[121] Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry* (Final Report, June 2019) 498–499 <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf> ('*Digital Platforms Inquiry Report*').
[122] Ibid 499.
[123] Ibid 498.

be carefully developed so that it is sufficiently defined and targeted, with appropriate legal safeguards and guidance'.[124]

In its submission to the PC's *Right to Repair* inquiry, the ACCC argued that a general prohibition on unfair trading could address concerns relating to the 'durability' of products, including:

- undisclosed planned obsolescence that relies on high switching costs to force consumers to regularly purchase additional or replacement products;
- businesses not disclosing that, as a result of internal decisions on future support, a product will be obsolete in an unreasonably short period of time; and
- a business not providing security updates for smart products for a reasonable amount of time, thereby putting sensitive consumer information at risk.[125]

These concerns are clearly particularly relevant to CIoT devices.

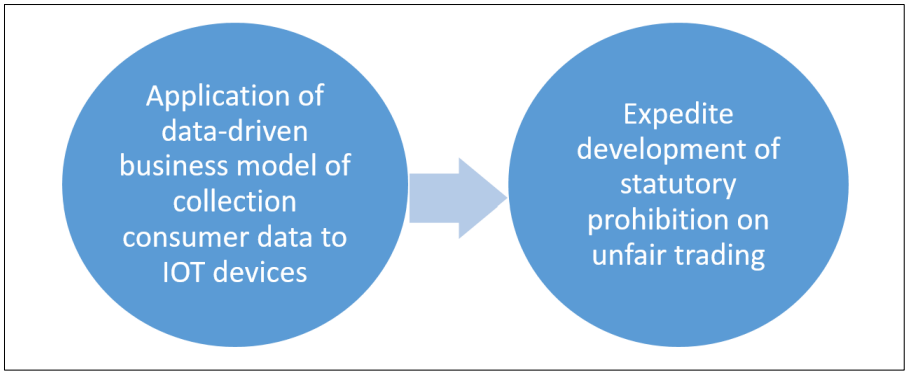
The Commonwealth Government's response to the *DPI* noted that CAANZ was undertaking work exploring how an unfair trading prohibition could be adopted in Australia and indicated that a decision on policy options for introducing such a prohibition would be developed in 2020.[126] However, in its *Right to Repair Report*, the PC concluded that it was impossible, without further research, to determine whether a general prohibition on unfair trading practices could address potential harms with planned obsolescence.[127] Given its terms of reference, the PC could not reach a conclusion on the general merits of such a proposal. At the time of writing this Report, policy options for addressing the ACCC's recommendation from the *DPI* had not been produced.

As Paterson and Bant have pointed out, the case for introducing a prohibition on unfair trading, although initially based on concerns about the limitations of statutory unconscionability in addressing systematic targeting of vulnerable consumers with unsuitable products, is reinforced by the extent to which data-driven business models enable businesses to manipulate consumer preferences, especially those of vulnerable consumers, by means of fine-grained targeting.[128] While the authors explain the

[124] Ibid.
[125] Productivity Commission, *Right to Repair Report* (n 6) 227.
[126] Department of the Treasury (Cth), *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Report, 12 December 2019) <https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf> ('*Regulating in the Digital Age*').
[127] Productivity Commission, *Right to Repair Report* (n 6) 228.
[128] Jeannie Marie Paterson and Elise Bant, 'Should Australia Introduce a Prohibition on Unfair Trading? Responding to Exploitative Business Systems in Person and Online' (2021) 44 *Journal of Consumer Policy* 1. See also Kayleen Manwaring, 'Will Emerging Information Technologies Outpace Consumer Protection Law? – The Case of Digital Consumer Manipulation' (2018) 26 *Competition and Consumer Law Journal* 141; Jeannie Marie Paterson and Gerard Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) 38 *Journal of Consumer Policy* 331.

benefits of a calibrated prohibition of unfair trading, they also acknowledge that it is not a 'magic bullet' but must be part of a multi-layered regulatory regime, which includes bright-line rules as well as broad standards such as a 'safety net' prohibition on unfair trading.[129] This conclusion is supported by a 2020 study by the Consumer Policy Research Centre (CPRC), which emphasised the ACCC's observations that it is important to establish appropriate boundaries on any general prohibition of unfair trading to ensure that it is proportionate and does not result in an overly broad interpretation of 'unfairness'.[130]

Figure 7 Data-Driven Business Model Reinforces Need for Statutory Prohibition on Unfair Trading



To address the gaps and deficiencies in the *ACL* in addressing unfair practices, including contractual practices relating to CIoT devices, this Report supports proposals for introducing a new prohibition on unfair trading practices. However, this prohibition must be seen as just one part of a 'layered' or 'holistic' approach to regulating problematic contractual practices relating to CIoT devices, including recommendations relating to the unfair contract terms law, dealt with in the next section of this Report.

[129] Jeannie Marie Paterson and Elise Bant, 'Should Australia Introduce a Prohibition on Unfair Trading? Responding to Exploitative Business Systems in Person and Online' (2021) 44 *Journal of Consumer Policy* 1, 14.
[130] Consumer Policy Research Centre (CPRC), *Unfair Trading Practices in Digital Markets – Evidence and Regulatory Gaps* (Research and Policy Briefing, December 2020) 17 <https://cprc.org.au/wp-content/uploads/2021/11/Unfair-Trading-Practices-in-Digital-Markets.pdf>.

Recommendation 17

As proposed by the ACCC, a statutory prohibition of unfair trading should be introduced. The prohibition should extend to prohibiting certain predatory and manipulative conduct associated with data-driven business models. The boundaries of any prohibition must be carefully calibrated, so that it is proportionate and does not extend to legitimate business practices. Like statutory unconscionability and the unfair contract terms law, the prohibition should be regarded as a general 'safety net' that forms one part of a layered regulatory regime.

4.13 Unfair Contracts

Part 2-3 of the *ACL* contains the 'unfair contract terms law', which can result in terms in standard form consumer and small business contracts being held to be void. The main operative provision in Part 2-3 is section 23, which renders a term in a consumer or small business standard form contract void if it is 'unfair'. Section 23(3) defines a 'consumer contract' as a contract for the supply of goods or services or a sale or grant of an interest in land 'to an individual whose acquisition of the goods, services or interests is wholly or predominantly for personal, domestic or household use or consumption'. The requirement that goods or services be acquired 'wholly or predominantly for personal, domestic or household use or consumption' means that a person may be a consumer for the purpose of the consumer guarantees but the unfair contract terms law does not apply as the products were not acquired for a specified purpose. The unfair contract terms provisions of the *ACL* do not exhaustively define a 'standard form contract' but in section 27(2), set out a number of factors that must be taken into account in determining whether a contract is a standard form contract. In effect, the factors point to whether a contract is, first, prepared by one party only and, second, offered on a 'take-it-or-leave-it' basis to the other party.

The test for determining whether a term is 'fair' is set out in section 24(1) of the *ACL* and consists of three elements, which must each be satisfied. The three elements provide that a term will be 'unfair' if:

- it would cause a significant imbalance in the parties' rights and obligations under the contract;
- it is not reasonably necessary to protect the legitimate interest of the party who would be advantaged by the term; and
- it would cause detriment to a party if it were to be applied or relied on.

Section 25 of the *ACL* provides a list of examples of terms that may be unfair. The examples are intended to provide guidance only, are not prohibited and do not create a statutory presumption that the term is unfair. Like the similar indicative list in the UK law, the examples of unfair terms can be regarded as a 'grey list'.[131] In practice, the indicative list tends to operate as a de facto presumption that the terms are unfair.[132]

The examples of unfair terms set out in section 25 are as follows:

- A term that effectively permits one party (but not another party) to avoid or limit performance of the contract;
- A term that allows one party (but not another party) to terminate the contract;
- A term that penalises one party (but not another party) for a breach or termination of the contract;
- A term that allows one party (but not another party) to vary the terms of the contract;
- A term that allows one party (but not another party) to renew or not renew the contract;
- A term that allows one party to vary the upfront price payable under the contract without the right of another party to terminate the contract;
- A term that allows one party unilaterally to vary the characteristics of the goods or services to be supplied, or the interest in land to be sold or granted, or the financial goods or services to be supplied under the contract;
- A term that allows one party unilaterally to determine whether the contract has been breached or to interpret its meaning;
- A term that limits one party's vicarious liability for its agents;
- A term that allows one party to assign the contract to the detriment of another party without that other party's consent;
- A term that limits one party's right to sue another party;
- A term that limits the evidence one party can present if taking legal action; and
- A term that imposes the burden of proof on one party.

As the following case study illustrates, CIoT devices commonly include terms, such as terms permitting unilateral variations to a contract, that are included in the statutory list of examples of potentially unfair terms.

[131] Paterson (n 17) 234.
[132] As a matter of law, however, it is clear that the indicative list does not create a presumption that particular terms are unfair: see Explanatory Memorandum (n 77) [5.44].

CASE STUDY: Unilateral Change of Terms

A number of agreements reviewed in the case studies allowed for unilateral change of terms and conditions. Users may not be directly notified of such changes, instead they may be required to monitor websites for changes or updates.

Ring Doorbell: *The Ring Doorbell Terms of Service provide that the terms and conditions may be updated by Ring from time to time, with only material changes (as determined by Ring) notified to the user through publication on the website, through the Service, email, or by some other means. Ring encourages users to check the website for updates from time to time. The Terms of Service provide that continued use of the Product or Services constitutes acceptance of the revised terms and conditions.*

Roomba: *The iRobot Terms of Service state that iRobot may update the terms from time to time and that continued use of the Service constitutes acceptance of the new terms. According to section 18.2, the changes to the iRobot Terms of Service 'will usually occur because of new features being added to the Service, changes to the law or where we need to clarify our position on something'. iRobot will provide notice of changes 'where possible and reasonable', either through the Service (such as the mobile application) or via email; however, urgent changes may be made without notice. Although the iRobot Terms of Service provide a URL that is intended to contain the current version of the Terms of Service, the current URL directs the user to a blank page.*

4.13.1 Enhancing Enforcement of the Unfair Contracts Law

In its *DPI,* the ACCC recommended amending the unfair contract terms law so that unfair terms are prohibited and not merely voidable, and that civil penalties apply to the incorporation of an unfair term in a consumer or small business standard form contract.[133] In its response to the report, the government indicated that it was consulting on policy options for strengthening protection against unfair contracts for small business, and that this would extend to include whether unfair terms should be illegal.[134] In December 2019, the Treasury released for public consultation a Regulation Impact Statement (RIS) on Enhancements to Unfair Contract Term Protections. As a result of the consultation, in November 2020, Commonwealth and state and territory consumer affairs ministers announced they had agreed to amend the unfair contract terms law by:

[133] ACCC, *Digital Platforms Inquiry Report* (n 121) 497.
[134] Department of the Treasury, *Regulating in the Digital Age* (n 126) 5.

- making unfair contract terms unlawful and giving courts the power to impose a civil penalty;
- increasing eligibility for the protections by expanding the definition of small business and removing the requirement for a contract to be below a certain threshold; and
- improving clarity on when the protections apply, including on what is a 'standard form contract'.[135]

In August 2021, the Commonwealth released exposure draft legislation aimed at implementing this agreement by strengthening and clarifying the unfair contract terms law.[136] Then in February 2022, the Government introduced the Treasury Laws Amendment (Enhancing Tax Integrity and Supporting Business Investment) Bill 2022, which included a chapter based on the exposure draft legislation. The Bill was intended to strengthen the remedies and enforcement of the unfair contract terms law by:

- prohibiting the proposal of, use of, application of, or reliance on, unfair contract terms in a standard form consumer or small business contract;
- creating new civil penalty provisions for breaches of the prohibitions;
- clarifying the powers of a court to make orders to void, vary or refuse to enforce part or all of a contract;
- making clear a court's power to make orders that apply to any existing consumer or small business standard form contract that contains an unfair contract term that is the same or substantially similar to a term the court has declared to be an unfair contract term; and
- making clear a court's power to issue injunctions against a respondent with respect to existing or future consumer or small business standard form contracts containing a term that is the same or is substantially the same as a term the court has declared to be an unfair contract term.

The Bill included a number of further amendments, including expanding the class of contracts covered by the unfair contract terms law. The main variation from the exposure draft bill was the removal of a proposed rebuttable presumption that terms found to be unfair that are subsequently included in contracts in similar circumstances would also be presumed unfair. The amending Bill lapsed before the 2022 federal election.

The proposals for enhancing the enforcement of the unfair contract terms law, which arose from a relatively lengthy reform process, have the potential to improve the position of consumers faced with

[135] 'Enhancements to Unfair Contract Term Protections', *Department of the Treasury (Cth)* (Web Page, November 2020) <https://consult.treasury.gov.au/consumer-and-corporations-policy-division/enhancements-to-unfair-contract-term-protections/>.
[136] Treasury Law Amendment (Measures for a Later Sitting) Bill 2021: Unfair Contract Terms Reform (Cth).

unfair terms. However, as explained in the next section of this Report, if the main objective of the law is to reduce the incidence of unfair contract terms, more fundamental reforms may be necessary. Therefore, if legislation such as the lapsed Bill were to be reintroduced, this Report recommends revisiting the desirability of including a rebuttable presumption that terms found by a court to be unfair will be presumed unfair if included in similar contracts. However, if the more fundamental reforms recommended in the next section of the Report were adopted, there would be no need for this.

Recommendation 18

Legislation aimed at strengthening the remedies and enforcement of the unfair contract terms law should be reintroduced. In reintroducing the legislation, consideration should be given to including a rebuttable presumption that terms found by a court to be unfair will be presumed unfair if included in a similar contract.

4.13.2 The Case for Reforms to the Unfair Contracts Law

While the reforms in the lapsed Bill would strengthen the existing regime, there are more fundamental questions about the extent to which the current law may be adequately equipped to deal with the challenges posed by contracts for CIoT devices, which are a sub-set of broader challenges posed by data-driven business models. This gives rise to two sets of issues: first, whether there is scope for improving the substantive unfair contract terms law; and second, whether there are additional regulatory measures that might be considered as part of a desirable 'layered' approach to regulation.

The prevalence of potentially unfair terms in standard form contracts offered as part of data-driven business models is posing challenges for laws regulating unfair terms across jurisdictions. The EU *Unfair Contract Terms Directive* (UCTD),[137] which was adopted in 1993, was an important influence on the introduction of the unfair contract terms law in the *ACL*.[138] Apart from a 2019 amendment to provide for increasing the effectiveness of penalties and enforcement,[139] the UCTD has not been updated since it was introduced. However, an independent study produced for the European Parliament's Committee on Legal Affairs (the JURI Committee), which was specifically aimed at

[137] *Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts* [1993] OJ L 095/29.
[138] Paterson (n 17) 200.
[139] *Council Directive 2019/2161 of 27 November 2019 on Better Enforcement and Modernisation of Union Consumer Protection Rules* [2019] OJ L 328/7.

proposing measures for increasing the effectiveness of the UCTD in the regulation of digital services, was released in February 2021.[140]

The major recommendations of the study were that the UCTD should be amended to create a 'black list' of contractual terms that would be prohibited, as well as a 'grey list' of terms that should be presumed to be unfair unless the service provider gives valid reasons for including the term. The debate about whether to incorporate black and/or grey lists of unfair terms, which in the EU is associated with the imperative for harmonisation of national consumer laws, has a long history.[141]

The proposed black list of terms, which includes terms that are so obviously unfair that there can be no justification for their inclusion in a standard form consumer contract, included the following:

- Misleading consumers as to the nature of the contract and statutory rights following from it.
- Recognising tacit consent as a valid method of contract formation.
- Creating the impression that the consumer protection framework does not apply.
- Creating the impression that digital services are provided for free, where consumers are paying for the service with their personal data, time or attention.
- Creating the impression that digital services are provided "as is".
- Exempting the service provider from liability for consumers' damage caused intentionally or through gross negligence.
- Allowing service providers to unilaterally modify terms where: the contract does not provide a valid reason for the change of terms; or the service provider did not inform consumers of the change with reasonable notice before the change was applied; or the consumer has not been informed about the option to and was not given a reasonable time to terminate the contract after having been informed of the change.
- Hindering the consumers' use of the right of withdrawal.
- Providing service providers with a unilateral right to suspend the performance or terminate a contract, when the consumer's behaviour does not objectively justify this.
- Requiring consumers to go to arbitration or suggesting that arbitration is the only method available for dispute resolution.

[140] Marco Loos and Joasia Luzak, *Update the Unfair Contract Terms Directive for Digital Services* (Report No PE 676.006, Study requested by the European Parliament's Committee on Legal Affairs (JURI), February 2021) <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf>.
[141] See, for example, Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council on Consumer Rights*, COM(2008) 614 final.

- Misinforming consumers as to their right to rely on the mandatory consumer protection of the country where they live.

On the other hand, the grey list proposed by the study include the following terms:

- Discriminating against consumers as a result of the personalisation of terms.
- Limiting or excluding the access to digital services, if consumers do not give an explicit consent to the sharing of personal data in the scope exceeding what is needed for the provision of a digital service.
- A no-survivorship clause (which would prevent consumer rights to products passing on death, sometimes known as 'digital inheritance').

A similar proposal, drawing on previous research commissioned by the EU, was made by Malbon in a submission to the 2019 Treasury consultation.[142]

The introduction of a black list of prohibited terms, or a grey list of presumptively unfair terms, or a combination of both, would be a fundamental shift in the unfair contract terms law. In particular, it would move more towards *ex ante* regulation rather than the current *ex post* regulation of unfair terms. Nevertheless, the prevalence of problematic terms in the CIoT contracts in the case studies introduced in this Report suggests that the current approach, which is confined to an indicative list of potentially unfair terms, is not achieving the objectives set for the unfair contract terms law and, in particular, the objective of reducing the overall incidence of unfair terms. This conclusion is reinforced by the 2020 Regulatory Impact Statement produced by Treasury, which recommended enhancing enforcement but which also observed that:

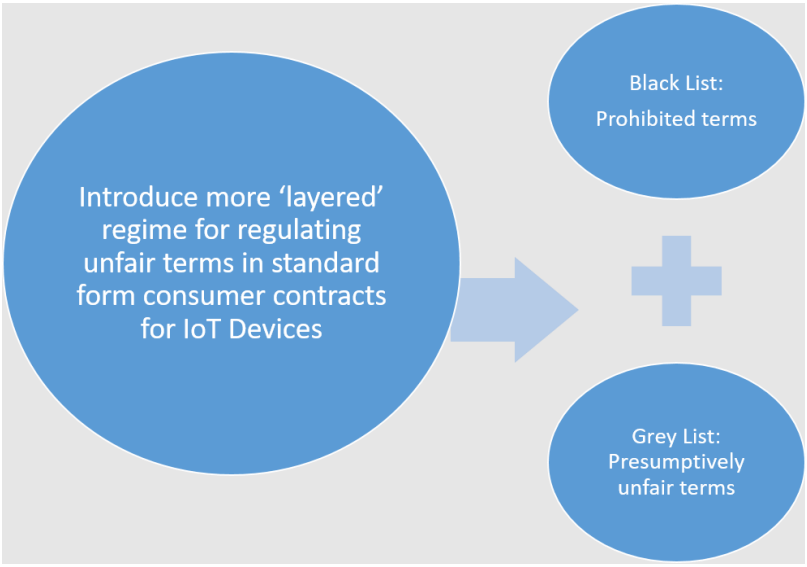
> *More than ten years after the introduction of the UCT protections for consumers and nearly four years since their extension to small business, UCTs are still prevalent in standard form contracts. Stakeholders advise that the current approach (involving voiding UCTs) is ineffective and that contract-issuing parties are able to capitalise on the typically weaker bargaining position of consumers and small businesses by including UCTs in their contracts.*[143]

The main argument against the introduction of prescriptive lists is that determining whether or not a contractual term is unfair is properly a decision for the courts, taking into account all of the relevant

[142] Justin Malbon, Submission to the Department of the Treasury, *Consultation on Enhancements to Unfair Contract Terms Protection – Regulation Impact Statement* (December 2019) <https://treasury.gov.au/sites/default/files/2020-11/c2019-5386_dr_justin_malbon.pdf>.
[143] Department of the Treasury (Cth), *Enhancements to Unfair Contract Term Protections: Regulation Impact Statement for Decision* (Report, September 2020) <https://treasury.gov.au/sites/default/files/2020-11/p2020-125938-ris.pdf>.

circumstances, and therefore should not be relegated to the mechanistic application of an inflexible list of prescribed terms. Moreover, even if a list-based approach were to be adopted, this would raise sometimes complex issues of interpretation, including whether a particular contractual term falls within one of the prescribed terms. Against this, prescribed lists would provide greater guidance and certainty to business and consumers alike and could reduce the costs of enforcing the unfair contract terms law. In addition, the inclusion of terms on a prescribed list would send an important signal to business that such terms are disfavoured. Above all, the adoption of bright line rules – in the form of a list-based approach – holds a greater prospect of reducing the prevalence of problematic contractual terms than the current ex post approach which, in practice, is not proving to be effective. This Report therefore recommends revisiting the issue of reforming the unfair contract terms law by introducing a black list of prohibited terns, a grey list of presumptively unfair terms or, preferably, a combination of both.

Figure 8 Layered Regime for Regulating Unfair Terms: Black and Grey Lists



Recommendation 19

Consideration should be given to reforming the unfair contract terms law by introducing a black list of prohibited terms, a grey list of presumptively unfair terms or, preferably, a combination of both.

4.13.3 Additional Measures

The complexity of standard form contracts, together with the complex nest of contracts that characterise the provision of CIoT devices, make it difficult to identify potentially unfair terms. Furthermore, most consumers rationally fail to read or understand complex standard form contracts.[144] In addition, even where a consumer may attempt to read contractual terms, problematic terms are sometimes buried in long, complex contracts. Consequently, there is a need for a more effective means of identifying unfair terms, or potentially unfair terms, in complex standard form consumer contracts.

There is an increasing use of artificial intelligence, specifically machine learning and natural language processing (NLP), to assist in the analysis of legal documents.[145] A group of European researchers has been developing a machine learning system, known as CLAUDETTE, to assist in identifying terms in consumer contracts that are potentially unfair under the UCTD.[146] In published reports, it appears that with a limited data set the system has shown promise in both identifying potentially unfair terms and in categorising (using multi-label classification) potentially unfair terms. Given the considerable costs in identifying unfair terms, or potentially unfair terms, in complex standard form contracts, this Report considers there is considerable merit in the investment of resources to assist regulators, such as the ACCC, with developing tools for identifying such terms. Internal use of RegTech tools such as this could assist in transitioning to more proactive forms of regulatory intervention, which is increasingly required for rapidly evolving technologies, such as CIoT devices.[147]

This Report has previously recommended (Recommendation 18) that RegTech tools should be investigated for assisting consumers in accessing contractual terms and conditions, the interpretation of terms and conditions, and the comparison of contractual terms offered by suppliers. Similarly, RegTech tools hold out some potential for assisting consumers to identify potentially unfair terms. As with the potential use of RegTech tools by regulators, the operation of consumer tools for identifying problematic terms could be facilitated by the introduction of prescribed lists of prohibited or presumptively unfair terms.

---

[144] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2018) 23(1) *Information, Communication & Society* 128.
[145] Michael Legg and Felicity Bell, *Artificial Intelligence and the Legal Profession* (Hart Publishing, 2020).
[146] Marco Lippi et al, 'CLAUDETTE: An Automated Detector of Potentially Unfair Clauses in Online Terms of Service' (2019) 27 *Artificial Intelligence and Law* 117.
[147] See, for example, World Economic Forum, *Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators* (Report, December 2020) <https://www3.weforum.org/docs/WEF_Agile_Regulation_for_the_Fourth_Industrial_Revolution_2020.pdf>.

Recommendation 20

Consideration should be given to resourcing regulators, such as the ACCC, to investigate and potentially design machine learning tools to assist in the identification of unfair terms in standard form consumer contracts. If, as recommended in this Report, the unfair contract terms law were to be amended to include prescriptive lists, such tools could enhance enforcement of the law.

4.14 Product Liability

Under Part 3-5 of the *ACL*, a manufacturer will be liable to compensate an individual if the manufacturer supplies goods that have a safety defect and the individual suffers injuries because of the safety defect,[148] or where other goods, land, buildings or fixtures are destroyed or damaged because of the safety defect.[149] The manufacturer's liability will also extend to loss or damage suffered by a person other than an injured individual where the loss or damage does not arise as a result of a business or professional relationship.[150]

Product liability laws should operate to ensure that the burden of costs arising from safety defects is appropriately allocated to the party most able to bear them: manufacturers, suppliers or their consumers. In general, manufacturers or suppliers of goods should be liable for harm caused by their goods. Manufacturers and suppliers have the requisite knowledge to minimise risks, especially when compared to consumers who must 'take the goods on trust'.[151] This is particularly true when it comes to CIoT devices where information asymmetries mean that consumers do not have a good understanding of how the goods function or the security vulnerabilities that may arise. Even where a consumer does have the requisite knowledge,

> *… there is no reason to shift the burden. The best incentive for manufacturers and suppliers, who do have the relevant information, to price the goods properly is certainty that they will be legally responsible to compensate for losses their goods cause.*[152]

As discussed in this Report, there is uncertainty as to how the *ACL* applies to CIoT devices where harm arises as a consequence of security vulnerabilities. This section of the Report will consider the issues

[148] *ACL* (n 2) s 138(1).
[149] Ibid s 140(1), s 141(1).
[150] *ACL* (n 2) s 139.
[151] Law Reform Commission, *Product Liability* (Report No 51, 1 June 1989) 16 <https://www.alrc.gov.au/publication/product-liability-alrc-report-51/>.
[152] Ibid.

that arise when applying the existing product liability regime to CIoT devices including the following important questions:

1. Are security vulnerabilities a 'safety defect' under section 9 of the *ACL*?
2. Is the existing product liability regime fit for purpose where safety defects may be introduced by the manufacturer by way of updates at a time after the product has been supplied?
3. Should manufacturers have a continuing duty to monitor security vulnerabilities and provide updates for CIoT devices? In such case, could failure to release security updates be considered a 'safety defect'?
4. Should damage to intangible property such as data be covered by the product liability regime?

The Report will then make recommendations to ensure that the existing product liability regime under the *ACL* is responsive to emerging disruptive technologies, such as digital products, and protects consumers who may suffer harm as a consequence of security vulnerabilities associated with CIoT devices.

4.15 Safety Defects Under the *ACL*

According to section 9 of the *ACL*, goods will have a safety defect 'if their safety is not such as persons are generally entitled to expect'.[153] In making a determination as to the safety of goods under the *ACL*, section 9(2) provides that the following must be taken into account: the manner in, and purpose for which, the goods have been marketed; any packaging; the use of any mark in relation to the goods; any instructions or warning provided; what might reasonably be expected to be done with or in relation to the goods; and the time when the goods were supplied by the manufacturer. It is worth setting out section 9 in full.

> ***9 Meaning of safety defect in relation to goods***
>
> *1) For the purposes of this Schedule, goods have a **safety defect** if their safety is not such as persons generally are entitled to expect.*
>
> *2) In determining the extent of the safety of goods, regard is to be given to all relevant circumstances, including:*
>
> *(a) the manner in which, and the purposes for which, they have been marketed; and*
>
> *(b) their packaging; and*
>
> *(c) the use of any mark in relation to them; and*

[153] *ACL* (n 2) s 9.

(d) any instructions for, or warnings with respect to, doing, or refraining from doing, anything with or in relation to them; and

(e) what might reasonably be expected to be done with or in relation to them; and

(f) the time when they were supplied by their manufacturer.

3) An inference that goods have a safety defect is not to be made only because of the fact that, after they were supplied by their manufacturer, safer goods of the same kind were supplied.

4) An inference that goods have a safety defect is not to be made only because:

(a) there was compliance with a Commonwealth mandatory standard for them; and

(b) that standard was not the safest possible standard having regard to the latest state of scientific or technical knowledge when they were supplied by their manufacturer.

When considering CIoT devices, potential security issues could result in harm to consumers. However, there is uncertainty whether security vulnerabilities would fall under the definition of 'safety defect' for the purpose of the *ACL*.

The definition of 'safety defect' is particularly problematic in relation to CIoT devices. As previously discussed in this Report, there exist information asymmetries between producers or suppliers and consumers. Consumers are often unaware of the security risks posed by CIoT devices and are unable to make informed choices regarding security. It is therefore unclear what the 'reasonable expectations' of the community might be in relation to the security of CIoT devices.

As observed by Butler:

> *The consumer expectations test is likely the most difficult to apply to insecure software defect claims because the test is poorly suited to address defects in complex systems. Consumers, especially those purchasing IoT devices, do not typically have an understanding of how their devices function, their role in the internet ecosystem, or the significance of any security vulnerabilities embedded in those systems. A purchaser of a DVR (or a webcam, or a "smart" refrigerator) likely does not have any expectations about how the software in that device will function. So long as the device carries out the tasks that the user expects, the user is not likely to think about what software is embedded in the device or how the software was developed. If a device has been hacked and is simultaneously being used as part of a botnet to attack*

servers of a major news site or gaming company, the user may not even be aware of that fact.[154]

The complexity of CIoT devices also makes it difficult to define what may be considered a 'defect' for the purposes of the product liability regime. While in recent years there is a greater understanding of the potential for and the impact of software vulnerabilities, not all vulnerabilities may be exploited.[155] Furthermore, if there is a reasonable expectation as to the presence of certain security features, what particular security features would be considered so critical that their absence would constitute a safety defect?[156] Reference may be made to a Code of Practice or other industry standards to determine essential security features, or to the sort of legally mandated security standards referred to in Part 3 of this Report. Particular difficulties arise in determining whether failure to release software updates or engage in continuous monitoring of security vulnerabilities post marketing would constitute a safety defect for the purpose of the *ACL*. In principle, the continuing relationship between the consumer and the supplier or manufacturer should be sufficient to impose a post-sale duty upon the manufacturer to release updates, as well as monitor and rectify security vulnerabilities.[157]

While the difficulties in applying the concept of a 'safety defect' to CIoT devices may be resolved by case law over time, there are considerable uncertainties and, accordingly, an immediate need for greater clarity. This Report therefore recommends that stakeholders, including consumer protection authorities, should provide guidance on what might be regarded as safety defects in CIoT devices.

Recommendation 21

Relevant stakeholders should provide consumer guidance on what may constitute a 'safety defect' with respect to CIoT devices (or digital products more generally), including guidance on the 'reasonable expectations' of the community in relation to product security.

4.15.1'No Defect at Time of Supply' Defence

A claim for defective goods must relate to a safety defect that existed 'at the time when the goods were supplied by their actual manufacturer', and it is a defence to a product liability claim under the *ACL* if the defect arose after the product was put into circulation. As section 142(a) provides:

[154] Alan Butler, 'Products Liability and the Internet of (Insecure) Things: Should Manufacturer's Be Liable for Damage Caused by Hacked Devices?' (2017) 50 University of Michigan Journal of Law Reform 913, 927.
[155] Benjamin C Dean, *Strict Product Liability and the Internet of Things* (Report, Center for Democracy and Technology, 16 April 2018) 20 <https://cdt.org/insights/report-strict-product-liability-and-the-internet-of-things/>.
[156] Ibid.
[157] Butler (n 154) 928.

In a defective goods action, it is a defence if it is established that:

(a) the safety defect in the goods that is alleged to have caused the loss or damage did not exist:

(i) in the case of electricity – at the time at which the electricity was generated, being a time before it was transmitted or distributed; or

(ii) in any other case – at the time when the goods were supplied by their actual manufacturer.

There is uncertainty whether, and if so how, such a provision would limit the ability of consumers to make claims for safety defects that arise in relation to CIoT devices.

One of the less problematic examples is where a security breach in relation to a smart lock results in unauthorised access to and damage of private property. Consumers are generally entitled to expect that a smart lock functions to secure property, and provided the security vulnerability is present at the time of sale, manufacturers should be liable for unauthorised access that results in damage to physical property. However, what if the security vulnerability arises after the date of supply by the actual manufacturer? Consider where a CIoT device is made insecure as a consequence of a security flaw in a software update that was distributed by the manufacturer after the goods were originally supplied. Would the software update itself be considered a 'good' separate to the device and therefore covered by the safety defect regime? Or, would action by a consumer be prevented due to the fact that the defect arose after the time that the goods were supplied by the manufacturer, albeit as a consequence of the actions of the manufacturer? Given the control that manufacturers have over the development and distribution of software updates, and that in some cases updates are installed automatically, the responsibility of the manufacturer should, in principle, extend to cover safety defects that arise as a consequence.

There is similar uncertainty in the EU in relation to the *Directive on Liability for Defective Products* (*Product Liability Directive*).[158] The *Product Liability Directive* is a useful comparator as it forms the basis for the product liability regime established under the *ACL*.[159] The *Product Liability Directive* provides that a producer will not be liable for a defective product where 'it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterward'.[160] A recent impact assessment by the European

[158] *Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products* [1985] OJ L 210/29 ('*Product Liability Directive*').
[159] Paterson (n 17) 498.
[160] *Product Liability Directive* (n 158) art 7(b).

Commission stated that the *Product Liability Directive* was 'unclear about who should be liable for defects resulting from changes to products after they are put into circulation'.[161] While the impact assessment suggested that further research on the extent of the problem is required, the report did set out a potential option for reform to extend strict liability rules to address 'defects resulting from changes to products after they have been put into circulation (eg, software updates or circular economy activities like product refurbishments)'.[162] Given that the *ACL* suffers from the same problem, a similar approach should be considered in Australia to extend the product liability regime to cover safety defects that arise as a consequence of changes made to goods after they have been supplied by the manufacturer, such as software updates released by the manufacturer or related parties.

Recommendation 22

The defence set out in section 142(a) of the ACL should be amended such that the ACL covers defects that may be introduced by the manufacturer at a point after the original supply, for example, through software updates. Such an amendment could be enacted by introducing a new sub-section under section 142(a), such as: 'in the case of digital products – at the time at which the digital products were supplied or subsequently modified or updated by their actual manufacturer.' This drafting is contingent upon the introduction of a category of 'digital products' being introduced into the ACL, as recommended in this Report.

4.15.2 Component Defence

Under section 142(d) of the *ACL*, it is a defence to a defective goods action if it is established that

> *… if the goods that had the safety defect were comprised in other goods – that safety defect is attributable only to:*
>
> *(i) the design of the other goods; or*
>
> *(ii) the markings on or accompanying the other goods; or*
>
> *(iii) the instructions or warnings given by the manufacturer of the other goods.'*

This means that a component manufacturer is generally liable for defective goods where a defective component is included in a finished product. However, the component defence effectively excuses

[161] European Commission, *Inception Impact Assessment: Adapting Liability Rules to the Digital Age and Circular Economy* (Report No Ref Ares(2021)4266516, 30 June 2021) 2 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en>.
[162] Ibid 4.

liability where a finished product is defective due to an act or omission of the manufacturer of the finished product – such as careless assembly, using an unsuitable component or incorrect instructions. In that case, it is the manufacturer of the finished product that should be liable.

Liability for safety defects under the *ACL* rests with the actual or deemed manufacturer[163] of the good. As discussed in this Report, CIoT devices are complex products combining hardware, software, data and associated services. As observed by Dean, 'complex supply chains for the design, manufacture, assemblage, shipping, and sale of these technologies'[164] may complicate the issue of determining and assigning responsibility for defective products. The consumer is therefore unlikely to be aware of, or unable to easily determine, which party in a complex supply chain should be liable for a safety defect; it is unreasonable to place such a burden on a consumer.

Consistent with the principles of good product liability regulation, it is a more cost effective and appropriate balancing of rights and responsibilities to require the manufacturer, supplier and distributor to identify and apportion liability for defective products, or components thereof, rather than the consumer. This Report therefore recommends that a consumer should be able to bring an action against the ultimate supplier or manufacturer and not bear the burden of determining who is responsible for defects in relation to parts of complex products, such as CIoT devices.

Recommendation 23

In the event that a product liability claim involves a CIoT device with components, the consumer should be able to bring an action against the ultimate supplier or manufacturer, with the burden resting with the supplier or manufacturer to reach a determination as to liability between the providers of the component parts.

4.16 Liability for Safety Defects and Available Remedies

A manufacturer will be liable to compensate an individual if the manufacturer supplies goods that have a safety defect and the individual suffers injuries because of the safety defect; or whether other goods, land, buildings or fixtures are destroyed or damaged because of the safety defect.[165] The manufacturer's liability will also extend to loss or damage suffered by a person other than an injured

[163] *ACL* (n 2) s 7.
[164] Dean (n 155) 12–13.
[165] *ACL* (n 2) ss 138-141.

individual, such as an innocent bystander, where the loss or damage does not arise as a result of a business or professional relationship.[166]

Under section 138(2) of the *ACL*, an individual may recover 'the amount of the loss or damage suffered by the individual'. The loss or damage envisaged under Part 3-5 of the *ACL* is physical – that is, loss arising as a consequence of injuries to an individual or damage to physical property, such as other goods,[167] buildings or land. The nature of digital products, however, means that loss or damage may not be restricted to such categories. In fact, the most common form of harm that is likely to arise as a result of a safety defect with respect to CIoT devices is loss of data as a consequence of a data breach or other non-physical harms, such as distress arising as a result of an invasion of privacy. The potential harm may also extend to future, unknown harms where hackers or third parties may use information obtained through a security vulnerability to cause harm in the future (such as financial harm). This can be illustrated by the Ring Doorbell case study.

CASE STUDY: Ring Doorbell

There have been several cases in the US dealing with data breaches and IoT devices, including class action complaints against Ring. These cases involve situations where Ring products were hacked with parties obtaining access to security cameras and doorbells and in some cases communicating with occupants.[168] In one case, the plaintiff's outdoor camera was hacked with the hacker speaking to the plaintiff's children.[169] In another case, hackers obtained access to a camera in a child's room and began speaking to her.[170] Both complaints contain numerous other examples of hacking, including threats and demands for ransoms to be paid in Bitcoin. The class action complaints allege that Ring has failed to implement basic security measures, such as two factor authentication[171] and strong passwords and, as a result, Ring products are vulnerable to security breaches.

The complaints allege that, in addition to no longer being able to use the Ring products as intended, the plaintiffs have suffered emotional distress and have been exposed to increased risk of theft or

[166] Ibid s 139(1)(e).
[167] The term 'other goods' is defined with reference to the definition of 'goods' in s 2 of the *ACL*. The term 'goods' includes: '(a) ships, aircraft and other vehicles; and (b) animals, including fish; and (c) minerals, trees and crops, whether on, under or attached to the land or not; and (d) gas and electricity; and (e) computer software; and (f) second-hand goods; and (g) any component part of, or accessory to, goods'.
[168] See *John Baker Orange on Behalf of Himself and All Others Similarly Situated v Ring LLC and Amazon.com Inc* (CD Cal, Case No 2:19-cv-10899, 26 December 2019) ('*Orange v Ring LLC and Amazon.com*'); *Ashley LeMay, Dylan Blakely, Tania Amador and Todd Craig v Ring LLC* (CD Cal, Case No 2:20-cv-00074, 3 January 2020) ('*LeMay et al v Ring LLC*').
[169] *Orange v Ring LLC and Amazon.com* (n 168).
[170] *LeMay et al v Ring LLC* (n 168).
[171] Note that two factor authentication has been mandatory for Ring products since 2020.

fraud.[172] *Such loss or damage, however, would not be covered under existing provisions dealing with liability of manufacturers for safety defects.*

The right to bring a defective goods action is not limited to the person who suffered the loss or damage (or their estate). Under section 149(1) of the *ACL*, the regulator may, 'by application, commence a defective goods action on behalf of one or more persons identified in the application who have suffered the loss or damage in relation to which the action is commenced'. The exercise of this power by the regulator may only occur with the written consent of the person on whose behalf the application is made. The exercise of this power may be appropriate to safeguard the rights of consumers, particularly where the safety defect arises in relation to a CIoT device manufactured by a company who is not present in Australia, or where there is a power imbalance between the manufacturer and the consumer.

Given the importance of the non-physical harms that may arise from safety defects in digital products, this Report recommends that the product liability regime should be amended to provide for compensation for such harms, such as harms resulting from data loss. While there may be complexities in quantifying compensation for such harms, guidance can be sought from other regimes where compensation may be awarded for intangible harms.

Recommendation 24

The liability of manufacturers under Part 3-5 of the ACL should be expanded to cover liability for all loss or damage suffered by a person because of the safety defect, regardless of whether the loss or damage is tangible or intangible, and should extend to including compensation for data loss.

4.17 Product Recalls

In addition to the defective goods provisions outlined above, Part 3-3 of the *ACL* also provides for the banning or recall of consumer goods[173] and the application of mandatory safety standards. Consumer goods may be recalled either voluntarily by the supplier, or upon order of the Minister, on the following grounds:

- The consumer goods will or may cause injury to a person;

[172] *LeMay et al v Ring LLC* (n 168) [89], [94].
[173] 'Consumer goods' are defined in s 2 of the *ACL* as follows: 'means goods that are intended to be used, or are of a kind likely to be used, for personal, domestic or household use or consumption, and includes any such goods that have become fixtures since the time they were supplied if: (a) a recall notice for the goods has been issued; or (b) a person has voluntarily taken action to recall the goods'.

- A reasonably foreseeable use (including misuse) of the consumer goods will or may cause injury;
- Non-compliance with a relevant safety standard for the consumer goods; or
- A ban on the consumer goods is in force.[174]

Where the Minister initiates a recall, the Minister must be satisfied that 'one or more suppliers of such goods have not taken satisfactory action to prevent those goods causing injury to any person'.[175]

There are a number of recall notices in place in relation to IoT devices (which are referred to as 'interconnected devices' by the ACCC).[176] These recall notices cover a range of products including location trackers, fitness trackers, medical devices and home assistant devices for vulnerable people. The most common reasons for product recalls in this category include risks of batteries overheating, improperly secured button batteries posing a risk of choking or injury upon ingestion, failure of the device to function due to network failure, and short circuits due to incorrect installation.[177] In relation to medical devices, safety issues may interfere with the proper operation of the IoT device, including incorrect administration of medicine. While clearly important, specific regulatory issues arising in relation to medical IoT devices fall outside the scope of this Report.

The scope of the product recall provisions are limited to where the safety issue is such that the goods will or may cause injury to a person. As discussed above, however, the potential harms caused by CIoT devices include other loss or damage, such as loss of data or non-physical harms including distress arising as a result of invasion of privacy. Expanding the recall provisions to encompass situations where consumer goods may cause loss or damage (other than physical injury) would allow product safety laws under the *ACL* to be responsive to the specific harms that are most relevant to CIoT devices. This Report therefore recommends that the product recall provisions be amended to allow for recall where a product causes, or is likely to cause, significant non-physical harms.

[174] *ACL* (n 2) ss 122, 128.
[175] Ibid s 122(1)(c).
[176] 'Interconnected Devices', *ACCC Product Safety Australia* (Web Page) <https://www.productsafety.gov.au/products/electronics-technology/interconnected-devices>.
[177] 'Browse All Recalls – Smart Devices', *ACCC Product Safety Australia* (Web Page, last updated 14 April 2022) <https://www.productsafety.gov.au/recalls/browse-all-recalls?f%5B0%5D=field_psa_product_category%3A4803>.

Recommendation 25

The recall provisions under Part 3-3 of the ACL should be expanded to allow for recall (both voluntary and compulsory) of consumer goods where such goods will or may cause injury to any person, or otherwise cause loss or damage, regardless of whether such loss or damage is tangible or intangible. Products should be able to be recalled where they cause, or are likely to cause, significant intangible harms, such as data loss or invasion of privacy.

4.18 Information Standard

Under section 134(1) of the *ACL*, the Minister may publish a mandatory information standard applicable to specific goods or services that sets out certain information that should be made available to consumers. The objective of the mandatory information standards regime under Part 3-3 of the *ACL* was explained in the Explanatory Memorandum to the Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010:

> *Information standards are an example of regulatory intervention to address market failure associated with information asymmetry. Lack of information on which to base purchasing decisions can lead consumers to make decisions which are not in their best interests … Information standards … are proactive, requiring a positive standard of information disclosure that the market, on its own, has not provided.*[178]

There are a number of information standards currently in place covering a diverse range of products, including button batteries, cosmetics, clothes, free-range eggs and tobacco products.[179] These information standards address existing information asymmetries and support consumers in making informed purchasing decisions. For example, children have died or been seriously injured after swallowing button batteries. The provision of information on button batteries in accordance with the information standard ensures that consumers have the information to make informed decisions regarding the purchase and use of products containing button batteries and encourages consumers to take steps to secure their products.

As explained in this Report, the increasing prevalence of CIoT devices poses significant risks to consumers, especially security risks. An information standard specifically for CIoT devices could

[178] Explanatory Memorandum (n 77) [23.180]–[23.181].
[179] See eg Australian Consumer Law (Free Range Egg Labelling) Information Standard 2017; Consumer Goods (Button/Coin Batteries) Information Standard 2020; Consumer Goods (Products Containing Button/Coin Batteries) Information Standard 2020; Consumer Goods (Cosmetics) Information Standard 2020; Competition and Consumer (Tobacco) Information Standard 2011.

provide information on the security and safety of devices, the associated privacy risks, the availability of software updates, and the steps or actions that can be taken to secure devices. Furthermore, mandatory information standards could be used in support of mandatory security standards, and a mandatory security labelling scheme for CIoT devices, as discussed in Part 3 of this Report.

While other elements of the *ACL* that regulate consumer information, such as the prohibition on misleading and deceptive conduct, are reactive, information standards are proactive, requiring disclosure of information that would not otherwise be provided. As part of the package of proposals for reforming the *ACL* proposed in this Report, which together are intended to support a more proactive approach to consumer protection regulation, especially in relation to device security, we therefore recommend the introduction of a new mandatory information standard specifically for CIoT devices.

Recommendation 26

A mandatory information standard for CIoT devices should be established under Part 3-3 of the ACL. The information standard should contain information to be provided to consumers that extends to the security and privacy risks associated with consumer IoT devices, the availability of software updates and the measures consumers may adopt to secure their devices.

5 Privacy Law and CIoT Devices

Introduction

CIoT devices pose significant challenges for data privacy law. As the Office of the Victorian Information Commissioner (OVIC) pointed out in an Issues Paper on the *Internet of Things and Privacy* released in 2020:

> *Traditional methods used to protect privacy and better inform individuals about how their personal information is collected, used and disclosed are largely incompatible or insufficient for IoT devices. New and innovative solutions that can work with devices and services that essentially form infrastructure may be needed.*[1]

Some of the challenges are illustrated by the following case study of an incident involving the VTech Smartwatch.

CASE STUDY: VTech Smartwatch

In November 2015, data gathered using the VTech Learning Lodge app was hacked, exposing data from millions of customers (including name, email address, secret question and answer for password retrieval, IP address, mailing address, download history, history of device purchases and password) and children with Learning Lodge profiles (including names, gender and birthdates).[2] *Thousands of Australian consumers, including children, were impacted and the Learning Lodge app was taken offline by VTech, revised and eventually re-released in January 2016.*

This Part of the Report analyses the application of Australian data privacy law to CIoT devices, explains the main weaknesses of the current law and sets out recommendations for improving the law. First, it introduces Australian data privacy law, outlining the main elements of the *Privacy Act 1988* (Cth) (*Privacy Act*). Next, this Part of the Report explains the current fundamental review of the *Privacy Act* being undertaken by the Commonwealth Attorney-General's Department, emphasising those aspects of the review that are most relevant to CIoT devices. After that, it explains how CIoT devices are part

[1] Office of the Victorian Information Commissioner (OVIC), *The Internet of Things and Privacy: Issues and Challenges* (Issues Paper, February 2020) 11 <https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/>.
[2] 'FAQ about Cyber Attack on VTech Learning Lodge', *VTech* (Web Page, last updated 9 January 2018) <https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/#!#18>.

of a constellation of technologies and business practices, involving the collection, processing and analysis of data at scale, which requires a new regulatory paradigm. Important elements of this paradigm include the principles of privacy by design and by default, and risk-based regulation. Following this, this Part of the Report analyses two fundamental elements of the *Privacy Act* that are particularly relevant for ensuring that the privacy of consumers of CIoT devices is properly protected, namely: the definition of 'personal information', which establishes the scope of data regulated by the law; and the 'notice and consent' regime, which underpins the approach to privacy protection adopted by the *Privacy Act*. This Part then turns to the case for additional protections to be introduced to the *Privacy Act*, including a proposed new general obligation for the collection, use or disclosure of personal information to be fair and reasonable, and a specific safeguard for CIoT devices requiring certain defaults to be set to 'off'. Finally, this Part of the Report supports proposals for improving the clarity of the data security principle in APP 11, and points to the importance of ensuring that this principle is consistent with other areas of the law regulating the security of CIoT devices.

5.1 Australian Data Privacy Law

Australian data privacy laws regulate the collection, use and disclosure of personal information. The main Act is the Commonwealth *Privacy Act*, which regulates the collection and processing of personal information by federal government agencies and private sector organisations. Although other areas of the law are relevant to privacy threats posed by CIoT devices, including state and territory surveillance devices and listening devices laws,[3] and telecommunications interception legislation,[4] this Part of the Report focusses solely on the federal *Privacy Act*, which is the single most important regulatory regime. Moreover, given that the *Privacy Act* is currently subject to fundamental review, as explained below, this Part of the Report is principally concerned with how CIoT devices challenge the fundamental principles underpinning the *Privacy Act*.

The *Privacy Act* regulates interferences with the privacy of an individual, which includes an act or practice of an APP entity which breaches an Australian Privacy Principle (APP) in relation to personal information. The scope of the *Privacy Act*, in general terms, is confined to: 'APP entities'; 'acts or practices' of an APP entity that breach an APP; and breaches involving 'personal information'.

An 'APP entity' is a public sector 'agency', such as a Commonwealth government department or a private sector 'organisation'. Although the *Privacy Act* applies to private businesses, it does not generally apply to small business operators, meaning that it applies to businesses that have an annual

[3] See, for example, *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 2007* (NSW).
[4] See *Telecommunications (Interception and Access) Act 1979* (Cth).

turnover of more than $3 million.[5] Under the *Privacy Act*, an APP entity must not engage in an act or practice that breaches an APP.[6] The APPS are 13 principles that regulate the collection, storage, use and disclosure of personal information.[7] For example, the APPs impose requirements to maintain a privacy policy about the management of personal information,[8] not to collect personal information unless it is reasonably necessary[9] and not to disclose personal information for direct marketing purposes (unless an exception applies).[10] The *Privacy Act* also incorporates important exceptions to the operation of the APPs. For example, under section 16, the APPs do not apply to personal information that is held by an individual for the purposes of personal, family or household affairs.

The *Privacy Act* is confined to interferences with privacy that consist of acts or practices that involve 'personal information'. Under section 6, 'personal information' is defined to mean:

> *… information or an opinion about an identified individual, or an individual that is reasonably identifiable:*
>
> *(a) whether the information is true or not; and*
>
> *(b) whether the information or opinion is recorded in a material form or not.*

The interpretation of 'personal information' by the courts has given rise to some difficulties, especially in the context of contemporary data processing practices.

5.2 Current Review of the *Privacy Act*

In its *Digital Platforms Inquiry* (*DPI*) report, released in June 2019, the ACCC made it clear that Australian data privacy law has not kept pace with the data practices of digital platforms, such as Google and Facebook, and made substantial recommendations for addressing deficiencies in the law.[11] The recommendations have implications that go beyond the practices of digital platforms and are especially relevant to the regulation of the data collection and processing practices of CIoT device service providers. The *DPI* report included specific recommendations to strengthen the protections available under the *Privacy Act*, as well as issues that it recommended should be subject to further review.

[5] *Privacy Act 1988* (Cth) ss 6, 6C, 6D, 6DA.
[6] Ibid s 15.
[7] Ibid sch 1.
[8] Ibid sch 1, APP 1.3-1.6.
[9] Ibid sch 1, APP 3.
[10] Ibid sch 1, APP 7.
[11] Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry* (Final Report, June 2019) <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report> ('*Digital Platforms Inquiry Report*').

The six specific recommendations made for strengthening the *Privacy Act* were as follows:

1. Amending the definition of personal information 'to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual'.[12]
2. Strengthening the notification obligations of APP entities to ensure that notices of data collection and processing practices are 'concise, transparent, intelligible and easily accessible'.[13]
3. Strengthening the consent requirements for processing personal information by expanding the circumstances in which consent is required, and by increasing the thresholds for valid consent and for consents from children.[14]
4. Introducing a right to have personal information erased on request, unless retention is necessary for performing a contract, required by law or otherwise necessary in the public interest.[15]
5. Introducing a right to bring individual and class actions, which currently does not exist, against APP entities for interferences with privacy under the *Privacy Act*.[16]
6. Increasing maximum penalties under the *Privacy Act* to mirror the penalties under the *ACL*.[17]

Recognising the need for consultation on the implications of broader reforms of data privacy law, the *DPI* report identified the following seven issues to be taken into account in reforming the *Privacy Act*, to ensure that it remains 'fit for purpose':[18]

1. Reconsider the objectives of the *Privacy Act* to ensure that consumer privacy is properly protected, including a reconsideration of the balance between protecting privacy and the commercial interests of businesses in processing personal information.
2. Establish higher levels of protection, such as an obligation limiting use and disclosure of personal information to lawful and fair uses and disclosures, in order to shift some of the onus from consumers to APP entities.
3. Review the scope of the *Privacy Act*, especially the exceptions for small businesses, employee records and registered political parties.

[12] Ibid Recommendation 16(a), 458.
[13] Ibid Recommendation 16(b), 461.
[14] Ibid Recommendation 16(c), 464.
[15] Ibid Recommendation 16(d), 470.
[16] Ibid Recommendation 16(e), 473.
[17] Ibid Recommendation 16(f), 475.
[18] Ibid Recommendation 17, 476.

4. Review whether the *Privacy Act* should be extended to protect 'inferred information', particularly where this includes sensitive information, such as information about an individual's health, religious beliefs or political affiliations.
5. Consider the need for new protections or standards to safeguard against increased risks of re-identification of de-identified data.
6. Given the importance of cross-border data flows, consider measures to ensure that Australian data privacy law affords an 'adequate level of protection' for the purpose of article 45 of the GDPR.
7. Consider the introduction of a certification scheme, where an independent third party would certify that an APP entity's practices are privacy compliant.

The Commonwealth Government's response to the *DPI* report, released in December 2019, announced support for a fundamental review of the *Privacy Act*.[19]

In October 2020, the Commonwealth Attorney-General's Department released an Issues Paper seeking public submissions on 68 questions relating to fundamental reforms of Australian privacy law.[20] Recognising the extent to which IoT devices may collect personal information without individuals being aware that the information is being collected, and without the consent of those individuals, the Issues Paper sought specific feedback on the following question:

> *How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?*[21]

In October 2021, the Attorney-General's Department released a Discussion Paper (AGDP) which took into account feedback on the Issues Paper and proposed reforms for addressing issues identified with the operation of the *Privacy Act*.[22] At the time of writing, it was expected that a final report would be released in mid-2022.

Given the extensive scope of the issues raised by the AGDP, this Report focusses on only those issues that this project has identified as particularly relevant to CIoT devices.

[19] Department of the Treasury (Cth), *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Report, 12 December 2019) <https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf>.
[20] Attorney-General's Department (Cth), *Privacy Act Review* (Issues Paper, October 2020) <https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf> ('*Privacy Act Review Issues Paper*').
[21] Ibid Question 34, 49.
[22] Attorney-General's Department, *Privacy Act Review* (Discussion Paper, October 2021) <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf> ('*Privacy Act Review Discussion Paper*').

5.3 A New Regulatory Paradigm?

Data privacy law has always been linked to technological developments in data processing, and this has resulted in generations of paradigms for the regulation of data privacy.[23] CIoT devices are part of a constellation of technologies, practices and processes that demand a new regulatory paradigm. The technologies and practices are based upon the collection, analysis and use of data at scale. They also include business practices that use data to profile and target individuals to extract value, including potentially manipulative practices.[24] In the face of these transformative technologies and practices, the *Privacy Act* – which is largely based on a model of siloed processing of data by entities and which attempts, in part, to enhance the control of individual data subjects over data practices – is no longer fit for purpose. While the EU GDPR is a more up-to-date attempt to adapt data privacy regulation to apply to contemporary data processing practices, it too has been overtaken by events. The first step in reforming the law so that it is adequately adapted to existing practices is therefore to review the regulatory paradigm underpinning the *Privacy Act*. In this, it is possible to learn lessons from other regulatory initiatives that attempt to meaningfully grapple with the challenges posed by contemporary data practices.

In April 2021, the European Commission released its proposal for a Regulation on Artificial Intelligence,[25] which clearly built on experience with measures introduced as part of the GDPR to address 'big data' practices. When taken together, it is possible to see some measures in the GDPR, which has clearly influenced data privacy laws and practices internationally, and in the proposed AI Regulation, as part of an embryonic, new regulatory paradigm that attempts to address the challenges of regulating near-ubiquitous data collection and processing. The new paradigm moves away from (but does not completely abandon) the regulation of particular practices – such as the collection, storage, use and disclosure of personal information – towards a more holistic approach to regulating complex socio-technical systems as a whole, including regulating technology design.

The emerging new paradigm includes a combination of *ex ante* and *ex post* regulatory measures. *Ex ante* measures include impact assessments in the form of privacy impact assessments or, as

[23] Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford University Press, 2014); Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis' (2022) 44 *Computer & Security Law Review* 1. The first generation of laws have their genesis in the 1980 OECD Guidelines and the Council of Europe Convention 108 of 1981. The second generation of laws commenced with the EU Data Protection Directive of 1995 and includes the 2001 Amending Protocol to Convention 108. Finally, the third generation refers to the EU GDPR and potentially Convention 108+ of 2018.

[24] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).

[25] European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*, COM(2021) 206 final, 21 April 2021.

recommended in relation to AI systems by the Australian Human Rights Commission (AHRC) in its report on *Human Rights and Technology*,[26] broad-reaching human rights impact assessments. Such assessments should be applied to processing systems that are determined to be high risk. *Ex ante* regulation also incorporates the important principles of data protection by design and by default (DPbDD), a version of which is enacted in article 25 of the GDPR. Article 25(1) of the GDPR provides as follows:

> *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

The operation of the principles are expanded upon in Recital (78) to the GDPR in the following terms:

> *In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.*

More is said about the principles of DPbDD in the section of this Report immediately following this.

[26] Australian Human Rights Commission, *Human Rights and Technology* (Final Report, June 2021) <https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf>.

Ex ante regulatory measures should be designed, as much as possible, to ensure that privacy protection is embodied in the technologies themselves. This is as relevant to CIoT devices as it is to digital platforms. However, as software-based technologies, such as AI systems and CIoT devices, are subject to fundamental change over time, it is important to also apply *ex post* regulatory measures. The potential for CIoT devices to be modified without notice to consumers is illustrated by the Tapo Smart Light Bulb case study.

CASE STUDY: Tapo Smart Light Bulb

The Tapo User Agreement includes broad powers to unilaterally change terms of service without notification. The agreement provides that TP-Link 'may temporarily or permanently modify, suspend, discontinue, or restrict access to all or part of the Services and/or any related software, facilities, and services, with or without notice and/or to establish general guidelines and limitations on their use'. This means that consumers may find that the availability of Tapo Services changes without notice or any recourse and the device potentially becomes inoperable as a result. The Tapo Terms of Use further provide that termination of Tapo Services may occur without advance notice 'for any reason, but usually because it would be impractical, illegal, not in the interest of someone's safety or security, or otherwise harmful to the rights or property of TP-Link'.

The most important *ex post* measures are ongoing monitoring and the ability to conduct audits of products in order to ensure regulatory compliance. Appropriately targeted system auditing is essential to transparency and accountability for CIoT devices.[27] These forms of *ex post* regulation should be supplemented by appropriate obligations imposed on device manufacturers and suppliers to maintain accurate and up-to-date documentation, which could be imposed as part of the mandatory security standards proposed in Part 3 of this Report. Moreover, both *ex ante* and *ex post* regulatory measures must be supported by appropriate regulatory powers of investigation and enforcement, including the availability of sanctions.[28]

Given the scale of contemporary data practices, it is unfeasible for all socio-technical systems, such as all AI systems or all IoT devices, to be subject to *ex ante* and *ex post* regulation: regulators have limited resources. The new regulatory paradigm, as embodied in initiatives such as the European

[27] See Thomas Pasquier et al, 'Data provenance to audit compliance with privacy policy in the Internet of Things' (2018) 22 *Personal Ubiquitous Computing* 333.
[28] For a similar approach in the context of the regulation of AI systems, see Karen Yeung, Andrew Howes and Ganna Progebna, 'AI Governance by Human-Rights Centred Design, Deliberation and Oversight: An End to Ethics Washing' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (Oxford University Press, 2019).

Commission's proposal to regulate AI systems and the AHRC's report on *Human Rights and Technology,* is to apply a 'risk-based' approach to regulation. Under this approach, regulation – and regulatory resources – are targeted at technologies that pose the greatest risks.[29] For example, the European Commission's proposed AI Regulation would draw a distinction between AI systems that pose an unacceptable risk, high risk systems, and systems with low or minimal risk. While systems with an unacceptable risk would be prohibited, regulatory measures would target high risk systems, with low risk systems subject to minimal regulation. The Attorney-General's DP identified options for applying greater regulation to 'high risk' practices, also referred to as 'restricted' practices, which are dealt with in more detail below.

While acknowledging that any regulation of complex, near-ubiquitous systems must prioritise regulatory interventions, it is important to understand the limitations of risk-based approaches to regulation. The limitations of, and problems with, risk-based approaches to privacy regulation are discussed more fully at 5.3.3 below.

Recommendation 27

Australian data privacy law should be reformed to better reflect a new paradigm for regulating ubiquitous collection and processing of data that has been emerging from instruments such as the EU's GDPR and the European Commission's proposal for a Regulation on Artificial Intelligence. Recognising the difficulties of regulating at scale, measures should be introduced that better calibrate regulation to reflect the risks of near-ubiquitous data processing practices, while allowing for more effective regulatory oversight. Such measures could include targeted privacy impact statements, data protection by default and by design, and targeted monitoring and auditing.

5.3.1 'Privacy by Design'

As mentioned above, the principles of DPbDD are important elements of the shift towards *ex ante* regulation. Although article 25 of the GDPR purports to incorporate the principle of 'data protection by design', it is formulated at a very high level of generality. Unsurprisingly, there have been disagreements about what the article means and difficulties in translating the principles into practice. Indeed, Waldman has gone so far as to claim that article 25 is 'so devoid of meaning that it can hardly be considered to reflect privacy by design at all'.[30] Moreover, as Waldman also claims, on a literal reading of article 25(1), it can be interpreted to be little more than a catch-all provision, requiring only

[29] See, for example, Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 *International Data Privacy Law* 3.
[30] Ari Ezra Waldman, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53(1) *Cornell International Law Journal* 147, 149.

compliance with other substantive provisions of the GDPR.[31] Even apart from the vague language used in the GDPR, there are a number of competing conceptions of 'privacy by design'.[32]

That said, on a proper understanding of 'privacy by design', the principle is potentially one of the most significant regulatory tools for protecting data privacy by ensuring that it is fully taken into account at all stages of the production and supply of products incorporating significant data processing elements, such as CIoT devices.

The AGDP addresses the principle of 'privacy by design' in chapter 10, which deals with 'Organisational Accountability'. Referring to the Explanatory Memorandum to the 2012 Privacy Amendment Bill,[33] the AGDP explained that APP 1 – which deals with open and transparent management of personal information – was intended 'to keep the Privacy Act up-to-date with international trends that promote a 'privacy by design' approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception'.[34]

Most relevantly, APP 1.2 imposes an obligation on APP entities to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs, and is able to deal with related inquiries and complaints. From this, it is clear that APP 1 suffers from a similar defect to article 25 of the GDPR in that it does no more than impose an obligation to comply with the APPs. 'Privacy by design', however, goes beyond mere compliance with existing data privacy principles. It is also broader than merely organisational accountability. It requires privacy to be taken into account at all stages of the process of designing a new product or service, which extends to implementing appropriate organisational arrangements, training and record-keeping; it also requires a comprehensive privacy management program which, where appropriate, could require Privacy Impact Assessments (PIAs) by independent third parties.

Therefore, while this Report supports the statutory recognition of a distinct 'privacy by design' principle in the *Privacy Act*, there are lessons to be learned from experience with the poorly drafted article 25 of the GDPR. In particular, a more precise understanding of the concept of 'privacy by design' is required so that it can be properly reflected in legislative form. In addition, as suggested in a 2018 ENISA policy paper, further work by policy makers and the research community is needed on the

[31] Ibid 167. This also seems to be the interpretation adopted by the European Data Protection Board in its guidelines on article 25: European Data Protection Board, *Guidelines 4/2019 on Article 25: Data Protection by Design and by Default* (v 2.0, adopted on 20 October 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>.
[32] Ibid 149–151.
[33] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth).
[34] Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 150.

relationship between the principles of DPbDD, on the one hand, and the associated principles of 'security by design and by default', on the other.[35]

Recommendation 28

The principle of privacy by design is an essential element of the new regulatory paradigm and should be codified as a distinct privacy principle. In codifying the principle, however, lessons should be learnt from flawed attempts to implement the principle in data privacy laws, such as the GDPR.

5.3.2 Privacy by Default

Privacy by default, which requires that defaults are set to the highest privacy protections, complements the principle of privacy by design. Chapter 12 of the AGDP addresses pro-privacy default settings. In doing so, it examines the case for introducing pro-privacy defaults on a sectoral or some other basis. The AGDP identifies the following two options for reform:[36]

Option 1 – Pro-privacy settings enabled by default

Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.

Option 2 – Require easily accessible privacy settings

Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

Given the problems of information overload, consent fatigue and cognitive biases that plague the 'privacy self-management' model, and which are referred to later in this Part of the Report, Option 2 would seem unlikely to achieve the objectives of the principle of privacy by default. In general, this Report considers that the benefits of setting defaults to the most privacy protective – especially as a measure to promote transparency and accountability for data practices – outweigh any inconvenience. This Report therefore supports a statutory codification of the principle of privacy by default.

[35] European Union Agency for Cybersecurity (ENISA), *Recommendations on Shaping Technology According to GDPR Provisions: Exploring the Notion of Data Protection by Default* (Report, December 2018) <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2>.
[36] Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 99.

Nevertheless, there is much to be said for the concern expressed by some submissions to the Attorney-General's Issues Paper that a strict application of the principle in all contexts may lead to inflexibility and considerable inconvenience for some consumers. There is therefore a case for confining the principle of privacy by default to collection or processing of data that is not strictly necessary for the functioning of a product or service. This suggests a need for greater consideration to be given to how the principle may apply in particular contexts, which may mean that the principle is applied more restrictively to high risk acts and practices, as explained below. Subsequently, this section of the Report makes recommendations about how the principle may apply in the particular context of CIoT devices that engage in large-scale data collection.

Recommendation 29

The principle of privacy by default is an essential element of the new regulatory paradigm and should be codified as a distinct privacy principle. In codifying the principle, however, consideration should be given to how the principle applies in particular contexts, with a case for stricter application of the principle to high risk acts and practices.

5.3.3 Advantages and Limitations of 'Risk-based' Regulation

Some submissions to the Attorney-General's Issues Paper proposed that certain collections, uses or disclosures of personal information present such high risks that they should be more tightly regulated than other practices or prohibited entirely.[37] The AGDP therefore considered options for dealing with 'high risk' acts or practices, which might include prohibitions (or 'no go zones') or greater protections ('proceed with caution').

The two options identified by the AGDP were:

> **Option 1**[38]
>
> *APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:*
>
> - *Direct marketing, including online targeted advertising on a large scale;*
> - *The collection, use or disclosure of sensitive information on a large scale;*
> - *The collection, use or disclosure of children's personal information on a large scale;*
> - *The collection, use or disclosure of location data on a large scale;*

[37] Ibid 94.
[38] Ibid 95.

- *The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software;*
- *The sale of personal information on a large scale;*
- *The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale;*
- *The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects; or*
- *Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.*

Option 2[39]

In relation to the specified restricted practices, an individual's capacity to self-manage their privacy in relation to that practice should be increased.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices, or by ensuring that explicit notice for restricted practices is mandatory.

The AGDP also sought feedback on whether there is a case for prohibiting certain acts or practices, which it also referred to as 'no go zones'. The acts or practices considered to present risks that might justify prohibitions included: profiling and behavioural advertising knowingly directed at children, the scraping of personal information from online platforms, the tracking and sharing of mental health information other than by the individual's own health service providers, or the use of information about an individual's emotional stress, mental or physical health or financial vulnerability that is shown to cause harm or discrimination.[40]

As explained subsequently, this Report is sceptical of the extent to which privacy self-management by means of improvements to the 'notice and consent' model can effectively prevent privacy harms. Therefore, this Report does not consider that Option 2, as identified in the AGDP, is a feasible alternative for dealing with high risk acts or practices. However, so as to deal more effectively with the challenges of regulating contemporary data practices at scale, there is potential in better calibrating regulation in accordance with the risk posed by particular acts and practices. Unlike Option 1, however, which merely proposes that APP entities that engage in 'restricted practices' must take 'reasonable steps' to identify and mitigate risks, this Report suggests that there is a case for imposing

[39] Ibid 96.
[40] Ibid.

a tiered system of regulation, similar to that in the European Commission's proposed AI Regulation. Such a system might include the following tiers:

- Acts and practices that present unacceptable risks would be prohibited ('no go' zones);
- Acts and practices that present high risks would be subject to greater levels of *ex ante* and *ex post* regulation ('proceed with caution'), including privacy impact assessments, audits and greater regulatory obligations; and
- Acts and practices that present low risks would be subject to less regulation, but would still need to comply with the baseline APPs or a relevant privacy code.

In addition to assisting with focusing regulatory resources, a more highly calibrated or tiered approach to regulation could address issues arising from the removal of the current exceptions in the *Privacy Act*. For example, in considering the case for removing the small business exception, the AGDP examines the option of retaining the exception but prescribing further high risk acts and practices.[41] While the flexibility embedded in a principles-based approach to privacy regulation, such as the APPs, already arguably embodies a 'risk-based' paradigm, more expressly recognising this approach could potentially alleviate concerns about the costs of removing the small business exception, while still ensuring that high risk acts and practices engaged in by small business are appropriately regulated.

Acknowledging the limitations of privacy self-management, Chapter 10 of the AGDP proposes a new 'fair and reasonable' standard whereby the collection, use or disclosure of personal information would be required to be fair and reasonable 'in the circumstances'.[42] As explained subsequently in this Report, there is a good case for implementing a new 'fair and reasonable' test. However, the test needs to be supplemented by measures for assessing whether acts and practices comply with the standard. A 'risk-based' approach could supplement the proposed new standard by adding certainty to its application. For example, a list of high risk acts and practices could be regarded as presumptively unfair so that the onus for justifying these practices shifts to the APP entity.

The section of this Report addressing the unfair contract terms law in the *ACL* recommends the introduction of prescribed lists of prohibited and/or presumptively unfair terms as a means for improving regulatory certainty. In a similar way to this proposal for enhancing certainty in determining whether contractual terms are 'fair', this Report suggests that the proposed broad 'fair and reasonable' standard might be supported by a black list of practices that would be prohibited and/or a grey list of factors that would be presumptively unfair. It is conceivable that this could be based on

[41] Ibid 46–47.
[42] Ibid Proposal 10.1, 85.

an *ex ante* assessment of the risk posed by particular forms of data processing. For example, distinctions could be drawn between: data processing, which poses unacceptable risks that are therefore prohibited; processing that poses high risks, which might be presumed to be unfair or unreasonable unless they are justified or reasonable steps are taken to mitigate the risks; and processing that is deemed to be low risk. While the list of acts or practices identified by the AGDP in Option 1 is a reasonable starting point, more nuance would be needed to properly distinguish between acts and practices that pose an unacceptable risk and those that pose a high risk. For example, while the use of facial recognition software poses a high risk, it is possible that certain forms of facial recognition or uses of the technology in certain contexts might pose an unacceptable risk. Similarly, while data processing at scale for the purpose of influencing behaviour or decisions might be regarded as high risk, processing that is more clearly targeted at manipulating vulnerable adults or children might be regarded as unacceptably risky.

While this Report considers there is scope for improving the effectiveness of the *Privacy Act* by more carefully calibrating regulation in accordance with the risks posed by data processing practices, as mentioned above, it is important to bear in mind the limitations of and problems with applying purely risk-based approaches. For example, risk-based regulation faces epistemic challenges in that it is difficult to accurately estimate all risks.[43] Moreover, risk-based regulation is not a neutral, technocratic process as the identification and assessment of risks is often based on contestable social or political values. Risk-based approaches can be characterised by an over-emphasis on tools based on statistics and probabilities, which can lead to a focus on process over outcomes and easily degenerate into a form of cost-benefit analysis, which fails to give due consideration to all risks, including unpredictable and systemic risks.[44] Furthermore, a purely cost-benefit calculus may be inconsistent with regulation based on the protection of human rights, such as the right to privacy, which must take into account intangible and difficult to quantify effects on human rights. In other words, activities ostensibly categorised as low risk may well result in human rights breaches.

[43] See, for example, Robert Baldwin and Julia Black, 'Driving Priorities in Risk-Based Regulation: What's the Problem?' (2016) 43(4) *Journal of Law and Society* 565; Maria Eduardo Goncalves, 'The Risk-Based Approach Under the New EU Data Protection Regulation: A Critical Perspective' (2020) 23(2) *Journal of Risk Research* 139.

[44] See Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37(1) *Yearbook of European Law* 130.

Recommendation 30

Risk-based regulation is an essential element of the new regulatory paradigm and it should be more expressly incorporated into the design of the Privacy Act. For example, the Act could distinguish between acts and practices that pose unacceptable risks, high risks or low risks. However, in implementing this approach, it is important to take into account the significant limitations of and problems with risk-based approaches.

5.4 Definition of 'Personal Information'

In its *DPI,* the ACCC recommended amending the definition of personal information to clarify that it captures technical data or metadata, such as Internet Protocol (IP) addresses. In the Issues Paper released in October 2020, the Attorney-General's Department noted that some, including the OAIC in its submission to the *DPI*, had suggested that the definition should be aligned with the definition of 'personal data' in the GDPR.[45] Article 4(1) of the GDPR defines 'personal data' to mean 'any information relating to an identified or identifiable natural person' and gives a non-exhaustive list of such data, which expressly includes location data and online identifiers.

The majority of submissions to the Attorney-General's Issues Paper favoured aligning the definition of 'personal information' with the GDPR definition. In its DP, the Attorney-General's Department identified two main issues with the current definition: uncertainty about whether the definition encompasses (1) technical and (2) inferred information. To address these deficiencies, the DP recommended including both technical and inferred information, proposing the following revised definition:

> *Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:*
>
> *a) whether the information or opinion is true or not; and*
>
> *b) whether the information or opinion is recorded in a material form or not.*
>
> *An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly.*[46]

In addition, the AGDP proposed the following amendments to support the new definition:

[45] Attorney-General's Department, *Privacy Act Review Issues Paper* (n 20) Question 34, 18.
[46] Attorney-General's Department, *Privacy Act Review Discussion Paper* (n 22) 26.

- a non-exhaustive list of the types of information capable of falling within the new definition of personal information;
- define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly; and include a list of objective factors to assist APP entities to determine when an individual is 'reasonably identifiable'; and
- amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

By removing any reference to information being 'about an individual', amending the definition in the way proposed by the DP would address the problems arising from the *Telstra* decision,[47] in which the Federal Court adopted a narrow approach to the definition, and ensure that the *Privacy Act* is better equipped to address contemporary data practices. It would also make the *Privacy Act* more consistent with data privacy laws in comparable jurisdictions, including the GDPR. As the AGDP put it:

> *This proposed change would ensure that information 'related to' an individual would be captured by the definition where there is a risk of identification, even if the information is primarily about something else - such as the individual's telecommunications use. This change would capture a broader range of technical information without fundamentally changing the structure of the definition.*[48]

While this Report supports the suite of changes to the definition of 'personal information' proposed in the DP, they do not resolve all issues relating to the scope of data, including data collected by CIoT devices, which might merit regulation by data privacy laws. The Google Nest Hub case study illustrates the kinds of data that may be collected from CIoT devices.

CASE STUDY: Google Nest Hub

The Google Privacy Policy highlights the diverse range of data that may be captured by CIoT devices, especially those devices that collect 'ambient' information. The Privacy Policy identifies the following categories of information that may be collected:

- Individual information: such as user name, password, phone number

- Payment information

- Content: content created by users such as emails, photos, videos, documents, comments.

- Apps, browsers and devices: including unique identifiers, browser type and settings, device type and settings, operating system, mobile network information

[47] *Privacy Commissioner v Telstra Corporation Ltd* (2017) 249 FCR 24.
[48] Ibid.

- User activity: such as search terms, content viewed, voice and audio information, purchase activity, browsing history

- Call history (where user uses Google services to make or receive calls or messages)

- Location information

The key problem that arises from attempts to distinguish between personally identifying data and other data is that the combination of mass, indiscriminate collection of data and advances in data analytics – which is facilitated by the IoT – mean that almost all data that are collected may potentially both identify and 'relate to' an individual. As Purtova has argued, 'in the age of the Internet of Things, datafication, advanced data analytics and data-driven decision-making, any information relates to a person in the sense of European data protection law'.[49] As Purtova further claims, the increasing scope of data falling within the definition of 'personal data', together with the high level of protection afforded to personal data under laws such as the GDPR, challenges the scalability of data privacy laws, potentially undermining the credibility and enforceability of the law. These considerable challenges do not necessarily mean that an unduly narrow definition should be applied to the concepts of 'personal information' or 'personal data', which would result in an inadequate level of privacy protection, but that the problem of 'scale' is a difficult problem that requires careful policy consideration.

There are two possible solutions to the challenge of ensuring the scalability of data privacy law in the face of contemporary data practices, which have been canvassed:

1. Retain a broad definition of personal data or personal information, but scale the intensity of data protection obligations to match the risks associated with the data; or
2. Abandon the attempt to distinguish between personal data and 'non-personal' data, and establish a new system of calibrated, scalable data privacy obligations, regardless of whether the information is 'personal'.

For some time, privacy scholars have argued against a 'one-size-fits-all' approach to the protection of personal data. For example, Schwartz and Solove have proposed that different regulatory regimes should apply to *identified information,* which singles out a specific individual, *identifiable information,* where there is a non-remote risk of future identification, and *non-identifiable information,* where

[49] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40, 42. See also Paul Ohm, 'Broken Promises of Privacy' (2010) *57 UCLA Law Review* 1701.

there is only a remote risk of identification.[50] Koops, on the other hand, has suggested that different sui generis regulatory regimes should apply to different sorts of data, such as online identifiers or profiling, regardless of whether or not they relate to identifiable individuals.[51] In Australia, the Australian Computer Society (ACS) has released white papers that propose a framework for assessing the risk of identifiability of data, based on a modified version of the 'Five Safes' framework.[52] The white papers propose a mathematical model for determining a 'Personal Identification Factor' (PIF), which is a measure of personal information in a dataset or in the outputs of data analytics.

As Purtova has argued, advances in data analytics mean that more and more data is likely to have the potential to identify and/or affect individuals.[53] This suggests the need for a broad scope for data privacy laws and accordingly, as proposed in the AGDP, a broad definition of personal data or personal information. On the other hand, a broad definition raises the problem of scalability, including the costs of regulating ever-greater amounts of data. It also retains the regulatory costs involved in distinguishing between personal data and non-personal data. Purtova therefore suggests abandoning the concept of personal data altogether on the basis that all data is potentially personal, in favour of a regime that applies to all automated information processing but subject to scalable rules that apply different levels of regulation depending upon the risks associated with the data.[54] On this, it is noteworthy that the privacy safeguards under the Australian Consumer Data Right (CDR) regime are not confined to 'personal information', but apply to 'CDR data', which is specified in instruments that designate a sector as being subject to the regime.[55] For example, the instrument designating the banking sector specifies information that goes beyond personal information to include such elements as information about financial products and uses of products.[56]

The Roomba case study illustrates how CIoT devices may collect data, in this case 'mapping data', which is not necessarily 'personal information' but which nevertheless may be significant for consumers.

[50] Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86(6) *New York University Law Review* 1814.
[51] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) *International Data Privacy Law* 250.
[52] See Ian Opperman (ed), *Privacy Preserving Data Sharing Frameworks: People, Projects, Data and Output* (Report, Australian Computing Society, 9 August 2019) < https://www.acs.org.au/insightsandpublications/reports-publications/privacy-preserving-data-sharing-frameworks.html>.
[53] Purtova (n 49) 73.
[54] Ibid 80. See also Omer Tene, 'Privacy: The New Generations' (2011) 1(1) *International Data Privacy Law* 15.
[55] *Competition and Consumer Protection Act 2010* (Cth) s 56AI(1).
[56] *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth).

CASE STUDY: Roomba

Roomba products can map homes to assist in navigation around rooms and obstacles. According to the iRobot web page on data security:

'iRobot considers maps of the home to be your sensitive, confidential information. Maps are protected following the industry standard guidelines to ensure the security of this data just like any other personal data. In addition to the standards mentioned above for encryption at-rest and in-flight, access to this data is tightly controlled, monitored and regularly audited. iRobot machines accessing this data have data-leak prevention software installed to ensure the data is tracked as it is accessed for use in customer and root improvement processes.'

The iRobot and IXL Home Privacy Policies do not contain specific provisions dealing with the protection of maps beyond standard provisions dealing with the protection of personal information. It is possible to avoid communicating data, including map data to iRobot, by not connecting the Roomba to WiFi or Bluetooth. However, this will necessarily change some of the functionality of the product.

Against the case made by scholars such as Purtova, Schwartz and Solove have argued in favour of retaining the concept of 'personal information' as it serves to confine the scope of data privacy regulation and avoids the prospect of all data needing to be subject to a risk assessment.[57] This approach implies that even if the concept of 'personal information' were to be abandoned over time, there would remain a need to distinguish data that is subject to regulation from unregulated data. It therefore seems that, at least for the immediate future, the concepts of 'personal information' or 'personal data' remain relevant.

Policy discussions relating to the concept of 'personal information', such as the AGDP, commonly focus on the 'risks' of *identifying* individuals, directly or indirectly, from the information.[58] Moreover, data privacy laws have long distinguished 'sensitive information' from other 'personal information'.[59] This distinction, and arguably data privacy law as a whole, is an early example of the increasingly common use of 'risk-based' approaches to address the problems of allocating scarce resources to regulate technologies at scale. To date, therefore, 'identifiability' has effectively been used as a proxy for broader privacy 'risks' to individuals. Given contemporary data practices, however, information or

[57] Schwartz and Solove (n 50) 1866.
[58] See also Gellert (n 29).
[59] See *Privacy Act 1988* (Cth) s 6 (definition of 'sensitive information').

data may clearly pose 'risks' to individuals regardless of the extent to which an individual is identifiable from the information or data.

As mentioned previously, in its consideration of whether or not to remove the current small business exemption, the AGDP canvassed the possibility of retaining the exemption but extending the operation of the *Privacy Act* to high-risk acts and practices engaged in by small businesses.[60] In examining this option, the AGDP referred to a list of 'high risk' practices set out in guidelines adopted by the UK Information Commissioner's Office (ICO) for data protection impact assessments. The list includes the following acts and practices:

- use of AI, machine learning and deep learning; IoT applications and smart technologies; targeting of children or other vulnerable individuals for marketing;
- intelligent transport systems and connected and autonomous vehicles; hardware and software offering fitness or lifestyle monitoring;
- social media networks;
- facial recognition and identity verification systems;
- medical research; data matching and aggregation;
- direct marketing and online advertising;
- web and cross-device tracking;
- re-use of publicly available data;
- loyalty schemes; and
- DNA testing.[61]

This is one specific example of the potential for regulation to be targeted in accordance with the risk of data practices. However, as explained above, this Report considers that there is potential for the *Privacy Act*, including the APPs, to be more generally re-formulated so that it is better calibrated to contemporary high risk data practices.

This Report therefore recommends that resources be allocated to an appropriate body, such as the OAIC, to undertake a comprehensive study into the potential for a 'risk-based' approach to deal with the challenges of regulating data that are significant for individuals at scale. Concurrently, as explained

[60] Attorney-General's Department, *Privacy Act Review Discussion Paper* (n 22) 47.
[61] 'Examples of Processing "Likely to Result in High Risk"', *Information Commissioner's Office (UK)* (Web Page) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>.

previously, it is important to bear in mind that 'risk-based' approaches are not a panacea and that there are significant limitations and weaknesses with regulatory approaches centred purely on 'risk'.

Recommendation 31

As proposed by the Attorney-General's DP, the definition of 'personal information' in the Privacy Act should be amended so that it more closely aligns with the approaches taken in comparable jurisdictions and, in particular, the definition of 'personal data' under the GDPR.

Recommendation 32

The amendments proposed by the AGDP to support the recommended new definition, including a non-exhaustive list of the types of personal information, a list of factors to determine when a person is 'reasonably identifiable' and an amended definition of 'collection' that covers inferred information, should also be introduced.

Recommendation 33

Resources should be allocated to an appropriate body, such as the OAIC, to investigate the potential for risk-based approaches, including a risk-based approach to defining the scope of the Privacy Act, to addressing the problems of regulating data collection and processing at scale.

5.5 Notice and Consent

The *Privacy Act*, like other data privacy laws, remains anchored in the general principle of data autonomy or 'privacy self-management': that individuals should be free to consent to the collection, use and disclosure of personal information.[62] In practice, however, the notice and consent model does not work. Confronted with complex privacy policies, people do not generally read notifications of data collection and processing policies. Moreover, people are often willing to 'consent' to data processing practices in return for convenient access to products or services; or consent is illusory, as there is no alternative but to consent in order to acquire a product or service. As the ACCC concluded in its *DPI* report:

> *… privacy self-management tools that rely on consumers to read privacy policies and provide consent may no longer be sufficient, in themselves, to provide consumers with adequate data*

[62] See Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 80; Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.

> *protection and privacy in a digital economy. The size of the task facing those consumers who want to provide truly informed consent suggests that it may be necessary to shift more of the responsibility for data protection and privacy on to the entities collecting, using, and disclosing personal information.*[63]

Similarly, Solove has pointed to the range of problems with the privacy self-management model, which together mean that it 'does not provide people with meaningful control over their data'.[64] First, behavioural science research reveals that individuals often do not make rational choices about the processing of their personal data. Second, structural problems inhibit self-management of privacy: so much data is collected about individuals that people suffer from information overload, and it is difficult for individuals to weigh the costs of privacy harms when the costs of each individual privacy harm might be relatively small but the cumulative societal costs of privacy harms are significant.[65]

As currently defined in the *Privacy Act,* consent means 'express consent or implied consent',[66] which sets a low consent threshold.[67] This can be compared with the definition in the GDPR which, in article 4(11), defines consent to mean:

> *[A]ny freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

In its *DPI* report, the ACCC recommended that the definition of 'consent' in the *Privacy Act* be amended to align with the higher standard of protection accorded by the GDPR.[68] In the current round of consultations on reforms, the AGDP included the following raft of proposals relating to the notice and consent provisions in the *Privacy Act*:

- Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.[69]
- Standardised privacy notices could be considered in the development of an APP code … including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of standardised notices.[70]

[63] ACCC, *Digital Platforms Inquiry Report* (n 11) 478.
[64] Solove (n 62) 1880.
[65] Ibid 1880–1881.
[66] *Privacy Act 1988 (Cth)* s 6(1).
[67] Damian Clifford and Jeannie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94(10) *Australian Law Journal* 741.
[68] ACCC, *Digital Platforms Inquiry Report* (n 11) 466.
[69] Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 69.
[70] Ibid 71.

- Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable, as soon as possible after collection, unless:
    - the individual has already been made aware of the APP 5 matters; or
    - notification would be *impossible* or would involve *disproportionate effort*.[71]
- Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.[72]
- Standardised consents could be considered in the development of an APP code …, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.[73]

As Solove has pointed out, the typical response to the failure of privacy self-management is to attempt to improve notice and consent but this can give rise to certain dilemmas. First, there is the 'consent dilemma', which refers to how making consent more difficult can potentially mean denying freedom of choice or, as Solove puts it, '(p)rivacy scholars must identify a conception of consent that both protects privacy and avoids paternalism'.[74] Second, making notices simpler and easier to understand risks resulting in people not being fully and accurately informed of the consequences of data collection and processing.[75] On the other hand, there are the well-known dilemmas facing consumers of 'notice fatigue' and 'consent fatigue'.

Consequently, there are limits on the extent to which improvements to notice and consent can address the endemic problem that the privacy self-management model fails to provide people with meaningful control of their data. These limits clearly direct attention to the ways in which systems for collecting data are designed, including the design of systems for notifying people and obtaining consent. The difficult balance to be struck essentially involves providing people with meaningful information and meaningful consent without over-burdening them. This can be done, at least in part, by enhancing the regulatory requirements for notice and consent. The AGDP therefore proposes the increased use of standardised layouts, wording, icons or consent taxonomies. At the same time, given the diverse contexts in which consent may be required, the AGDP cautioned that 'it is likely to be impractical to develop consent templates, icons or phrases across all sectors'.[76]

[71] Ibid 73.
[72] Ibid 78.
[73] Ibid 79.
[74] Solove (n 62) 1894.
[75] Ibid 1885.
[76] Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 79.

While it is common for claims to be made that improvements can be made to notifications provided to consumers through systems such as the use of standardised icons, designing effective systems is complex.[77] For example, Warren, Mann and Harkin have found that there are 'mixed views' about the value of certain privacy icons in promoting awareness of privacy issues, and that while consumers and other stakeholders may find the idea of icons to be appealing, other regulatory reforms may be more effective.[78] That said, properly designed systems aimed at simplifying information provided to consumers may have an effect, albeit at the margins and only when combined with other regulatory measures.

Based on the above considerations, this section of the Report endorses the proposals made for strengthening the notice and consent regime in the AGDP. Nevertheless, it cautions that the proposed measures may result in only marginal improvements, to the extent that they remain embedded in the privacy self-management model. To be effective, they must be matched by additional reforms that strengthen the protections in the *Privacy Act*, which are explained below.

Recommendation 34

The notice provisions of the Privacy Act should be strengthened. Notice should be concise, transparent, intelligible and easily accessible, and clearly set out how an APP entity collects, uses and discloses personal information. Resources should be expended on ensuring that user-friendly ways of presenting notices are adopted, such as layered notices and/or standardised icons. This should be based on rigorous consumer testing.

Recommendation 35

The consent provisions of the Privacy Act should be strengthened. Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed, and any settings for additional data should be preselected to 'off'. Measures should be introduced to minimise consent fatigue, such as the use of standardised icons or phrases, which should be based on rigorous consumer testing.

[77] Lorrie F Cranor, 'Informing California Privacy Regulations with Evidence from Research', (2021) 63(3) *Communications of the ACM* 29.
[78] Ian Warren, Monique Mann and Diarmaid Harkin, *Enhancing Consumer Awareness of Privacy and the Internet of Things* (Report, ACCAN and Deaking University, August 2021) <https://accan.org.au/grants/current-grants/1611-regulating-the-internet-of-things-to-protect-consumer>.

5.6 Additional General Protections

In its submission to the Attorney-General's Issues Paper, the OAIC observed that '(t)he burden of understanding and consenting to complicated practices should not fall on individuals but must be supported by enhanced obligations for APP entities that promote fair and reasonable personal information handling or organisational accountability'.[79] Acknowledging the limitations of the notice and consent model, and that the current APPs relating to the collection, use and disclosure of personal information confer considerable discretion on APP entities, the AGDP proposed that additional protections be introduced to ensure minimum acceptable standards for the processing of personal information. In particular, the AGDP proposed that:

> *A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances*.[80]

In formulating this proposal, the AGDP rejected the application of the 'legitimate interest' test under article 6(1)(f) of the GDPR, largely on the basis that the GDPR test incorporates a balancing of rights and interests under the EU rights-based legal regime, which cannot be readily transposed into the Australian legal context. Nevertheless, the test proposed in the AGDP clearly draws on standards in other data privacy laws, especially article 5(1) of the GDPR, which provides that:

> *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.*

The 'fair and reasonable' test proposed in the AGDP is obviously a flexible standard and as such, requires guidance as to how it would apply in practice. To address this, the AGDP proposed introducing a non-exhaustive list of legislative factors to be taken into account in determining whether processing of personal information is fair and reasonable. The factors proposed in the AGDP are:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances;
- The sensitivity and amount of personal information being collected, used or disclosed;
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information;
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity;

[79] Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 82.
[80] Ibid 85.

- Whether the individual's loss of privacy is proportionate to the benefits;
- The transparency of the collection, use or disclosure of the personal information; and
- If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.[81]

To illustrate the potential operation of the proposed 'fair and reasonable' test, the AGDP provided the following case study.

> *A digital platform offers social media services. The digital platform collects personal information about individuals that use its services, including inferred interests, demographics, location and behaviours. This data is used to serve individuals with relevant content in order to maximise user engagement with the platform. The digital platform does not sell or disclose users' personal information, but permits advertisers to market to platform users based on specific traits.*
>
> *The digital platform also actively infers users' moods and socio-economic status. The digital platform has received complaints that vulnerable individuals are receiving highly targeted content or advertisements relating to mental health, gambling and predatory loan services.*
>
> *The profiling of user moods and socio-economic status is unlikely to be fair and reasonable in these circumstances. An individual is unlikely to reasonably expect that a social media platform would infer these particularly sensitive traits without their knowledge. Profiling based on such traits is unlikely to be a proportionate use of individuals' personal information, particularly whereby advertising revenue and engagement could be driven by non-sensitive traits that pose less of a risk of adverse impact or harm to the individual.*
>
> *By contrast, if an entity offered specialised mental health therapy or financial coaching applications based on profiling of users' activity carried out transparently, and in the individuals' best interests, it could be more likely to meet the proposed fair and reasonable test.* [82]

The Attorney-General's Issues Paper sought specific feedback on how the personal information of individuals may be protected where CIoT devices installed in the home collect such information about third parties, such as household members or visitors, without consent. This scenario raises potentially difficult issues as some devices, such as personal digital assistants, can rely on the dragnet collection

[81] Ibid 89.
[82] Ibid 90.

of data for their functionality. As such devices indiscriminately collect data, they can clearly collect highly personal information from third parties without their consent. The collection of this sort of information from third parties is illustrated by some of the case studies in this Report, including the Ring Doorbell and Google Nest Hub case studies.

CASE STUDIES: Collection of Highly Personal Information

A number of the case studies provide examples of where highly personal information may be collected, particularly information that may be collected from third parties.

The Ring Doorbell captures both audio and video of visitors to the premises. This information may be viewed by the user and where the user has a Ring Protect plan, the information may be stored for future viewing or shared with the Ring Neighbors community or law enforcement. The Ring Terms of Service place the burden on the user to ensure they comply with all applicable laws relating to the recording or sharing of video or audio content or laws relating to notice and consent to recording.

The Google Nest Hub collects audio data from users who engage with Google Assistant. This may include audio data from minors, or third parties who are not normally resident in the household. Google states that audio is not sent to Google unless the user is interacting with Google Assistant and a visual indicator will be displayed to notify users that data is being sent to Google. There are specific privacy terms that apply to audio collection from children's features on Google Assistant.[83] *Children's audio recording settings may be managed through Family Link. According to the Google Nest Commitment to Privacy in the Home, Google will not use audio recordings, sensor or video data for ad personalisation but may use data from Google Assistant for ad personalisation. These settings may be managed by the user in the settings function for Google Assistant.*

The proposed 'fair and reasonable' test, as supplemented by legislative factors, would go some way to addressing legitimate concerns about the potential unconstrained collection of personal information by CIoT devices. For example, in elaborating on the 'reasonable expectations' factor, the AGDP explained that:

[83] 'Privacy Notice for Audio Collection from Children's Features on Google Assistant', *Hey Google* (Web Page, last updated 2 September 2021) <https://assistant.google.com/privacy-notice-childrens-features/?hl=en_GB>.

> *It is likely that certain kinds of information would attract higher expectations from an objective reasonable individual, for example, sensitive information or IoT smart home data, the handling of which may require a higher standard of privacy protection.*[84]

Furthermore, the factors identified in the AGDP include 'whether an individual is at foreseeable risk of unjustified adverse impacts or harm'.[85] This raises the issue of whether the risks of data processing should be regulated regardless of whether or not they are foreseeable. To address this possibility, this Report suggests that consideration should be given to rephrasing this proposed factor in more objective terms, such as:

> *… whether the collection, use or disclosure of personal information poses a risk of adverse impacts or harms to individuals.*

As previously explained in this section of the Report, we consider that the 'fair and reasonable' standard should be supplemented by a 'risk-based' approach, which would enhance certainty in applying the standard to particular acts or practices. As explained above and as set out in Recommendation 30, this could entail distinctions being drawn between: data processing that poses unacceptable risks, which would be prohibited; processing that poses high risks, which might be presumptively unfair or unreasonable, unless the practices are justified or the risks mitigated; and processing that is deemed to be low risk.

Based on the above analysis, this Report makes the following recommendations.

Recommendation 36

As proposed in the AGDP, a new privacy principle should be introduced requiring the collection, use or disclosure of personal information to be fair and reasonable. This principle should operate in addition to other principles that apply to the collection, use or disclosure of personal information and, in the event of inconsistencies, should prevail. As further proposed in the AGDP, the principle should be supplemented by a list of non-exhaustive statutory factors. Consideration should be given to whether the statutory factors proposed in the AGDP could be improved, such as by ensuring that a more objective standard is applied in assessing the risk of data processing.

[84] Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 86.
[85] Ibid 89.

5.7 Additional Safeguards for CIoT Devices

As referred to above, the Attorney-General's Issues Paper sought specific feedback on how the personal information of individuals may be protected where CIoT devices installed in the home collect information about third parties, such as household members or visitors, without consent. It is generally acknowledged that IoT applications, especially for CIoT devices installed in the home, present high risks to data subjects.[86] This is, at least in part, due to the highly sensitive personal information that may be collected in a domestic context. This Report therefore considers that over and above the general 'fair and reasonable' standard dealt with at 5.6, there is a case for additional safeguards for data processing involving these devices.

This Report has previously recommended the statutory codification of the principles of DPbDD. The default settings of technologies are fundamental in determining the choices made by users of those technologies. As a 2018 report produced by ENISA put it:

> *When designing IT systems or IT-based services, the default settings, i.e. the properties and functionalities that are in place at the very first employment (of these systems or services) without requiring any activity or choice by the user, are of vital importance, as they constitute the basis upon which the user will initiate his or her interaction. Indeed, the default determines at least the first usage and, if users are not able or willing to change it, it further determines the ongoing use.*[87]

Many purchasers and users of CIoT devices installed in the home will be ignorant or uncertain of the amount and types of data collected by the devices. One practical measure that could promote greater understanding of the functioning of devices that indiscriminately collect data would be, applying the general principle of privacy by default, to require consumers to take an affirmative action to 'opt in' to data collected and processed by such devices, other than data that is necessary for performing the principal function for which the device has been purchased. This proposal would differ from Option 1 identified in the AGDP for implementing 'privacy by default', referred to at 5.3.2, as that option canvasses pre-selecting privacy settings to the most restrictive, whereas this recommendation is to specifically set the 'functionality' of the device to 'off'. This proposal could be implemented either as a particular application of a general 'privacy by design' principle or as a specific provision requiring

[86] See Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 47, citing European Data Protection Board (n 31).
[87] ENISA (n 35) 7.

that to the maximum extent possible, default settings for data processing by CIoT devices in the home be set to 'off'.

It might be objected that there is a potential conflict between the recommendations in this Report imposing obligations to kept software updated[88] and the principle of privacy by default, and especially the proposal to set default settings to 'off'. However, objections such as this are more imagined than real. With CIoT devices, regular software updates are necessary to ensure the security and functionality of devices. On the other hand, software updates that are not necessary for those purposes can be irritating and in some cases, may even interfere with the functionality of devices. The obligations to keep software updated should therefore be confined to software necessary for functionality and security; the proposal for setting defaults to 'off' should not apply to data collection and processing that is necessary for device security and functionality.

Recommendation 37

Except where data processing is essential for the security and functionality of CIoT devices, default settings allowing for data processing by means of such devices should be pre-selected to 'off'.

5.8 Data Security

As this Report has explained, there are potential overlaps between laws mandating minimum security standards for CIoT devices, the protection of security as part of consumer protection law and the protection of data security as part of data privacy law. This section of the Report focuses on data security as a fundamental principle of data privacy law.

Under the *Privacy Act*, APP 11 embodies the data security principle, with APP 11.1 requiring APP entities that hold personal information to take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure. While the AGDP supported retaining a principles-based and technology neutral data security principle, it canvassed some proposals for increasing the certainty of the 'reasonable steps' test. In particular, the AGDP raised the following options:

- Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures; and

[88] See Recommendations 3 and 14.

- Include a list of factors that indicate what reasonable steps may be required.[89]

This Report supports the AGDP's proposals for clarifying and strengthening APP 11.

Recommendation 38

As recommended by the AGDP, APP 11 should be amended to clarify what amounts to 'reasonable steps' to secure personal information, including by expressly providing that such steps include technical and organisational measures, and a list of factors indicating what reasonable steps may be required.

However, over and above amendments to APP 11, as this Report has emphasised, it is important to ensure that security requirements imposed by distinct legal regimes are coherent and cohesive. Therefore, as set out in the Conclusion, this Report makes recommendations for more expressly linking the security standards under the different legal regimes that apply to CIoT devices, including the data security principle in APP 11 of the *Privacy Act*.

[89] Attorney General's Department, *Privacy Act Review Discussion Paper* (n 22) 146.

Conclusion

CIoT devices are transformative technologies, which promise considerable benefits for consumers but also carry risks of substantial harms. As the research for this project has revealed, the technologies pose fundamental challenges for existing laws and regulations, especially laws designed to protect consumers.

The challenges, which are introduced in Part 1 of this Report, essentially arise from the differences between these devices and traditional consumer products. In particular, the devices incorporate significant software and data components and are commonly always connected. The 'always connected' nature of the products, and their limited processing power, create potential security vulnerabilities. The types and scale of data collected from the devices pose considerable risks of privacy harms. The devices depend upon software, which must be remotely updated, particularly to counter security threats. But this means that changes can be made to the nature and functionality of the products, potentially without consumer knowledge or prior notice. The complexity of the devices – which include hardware, software, data and service elements – creates difficulties in detecting defects and repairing the products. As illustrated by the case studies presented in Part 2 of this Report, this product complexity is reflected in the complex nest of contracts and policies that apply to CIoT devices. It is often difficult for consumers to locate and understand these documents, which means that most consumers have limited information about what they have purchased and what legal recourse is available if something goes wrong.

As explained in Part 1 of the Report, the precise legal and policy challenges posed by CIoT devices differ, depending upon the specific areas of law and regulation. The most important immediate challenge is increasing the security of CIoT devices. Part 3 of the Report explains the case for introducing legislation mandating minimum device security standards. This Part includes recommendations for implementing mandated standards, including how the standards should be enforced, which broadly align with legislation that has been introduced in the UK. As this Part points out, however, mandated minimum standards should be supplemented by other measures. In particular, a comprehensive regime for enhancing security of CIoT devices should include a labelling scheme. However, the effectiveness of a labelling scheme depends upon how the scheme is implemented. To ensure uptake and enforcement of the scheme, this Report favours a mandatory scheme. However, in the absence of mandatory labelling, the Report supports a voluntary scheme with appropriate government backing.

Part 4 of the Report recommends reforms to address identified gaps or weaknesses in the *ACL*. This includes supporting current proposals for enhancing enforcement of the *ACL*, namely introducing a prohibition on failing to provide a remedy for breach of a consumer guarantee and enhanced enforcement of the unfair contract terms law. Beyond these immediate reforms, however, this Part of the Report argues for more fundamental reforms. In relation to consumer guarantees, given the difficulties of shoe-horning CIoT devices into the existing categories of 'goods' or 'services', this Report recommends introducing a new sui generis category of 'digital products', which would include CIoT devices. Apart from addressing the uncertainties in applying the existing categories to CIoT devices, this would enable the introduction of new consumer guarantees that are specifically designed for digital products, including CIoT products. Given the considerable difficulties in accessing and understanding contractual terms and conditions and other product information, illustrated by the case studies in Part 2 of the Report, Part 4 includes recommendations for introducing obligations for greater pre-contractual disclosure of information. It also supports the development of new technology tools to assist consumers in accessing and interpreting contractual information.

CIoT products should be seen as part of a broader constellation of data-centric technologies and business practices. To address the risks posed by these practices, including the risks of consumer manipulation, Part 4 of the Report supports recommendations made by the ACCC for introducing a new general prohibition of unfair trading. That said, there are difficulties in applying consumer safeguards that are expressed in highly general terms, such as the statutory prohibition of unconscionable conduct and the unfair contract terms law, to new technologies and practices. To improve certainty in the application of the unfair contract terms law, Part 4 of the Report recommends that consideration be given to the introduction of a black list of prohibited contractual terms and/or a grey list of presumptively unfair terms. In light of the concerning contractual practices identified in the case studies in Part 2 of the Report, the introduction of prescribed lists of unfair terms would send a strong message that such terms are not acceptable. To better support enforcement of the unfair contract terms law, the Report also supports the development and use of RegTech tools by the ACCC and other regulators to assist in the identification of unfair, and potentially unfair, terms and conditions in standard form consumer contracts.

Just as CIoT devices challenge other areas of consumer law, they challenge the product liability provisions of the *ACL*, which are designed to ensure the safety of consumer products. Given the uncertainty in determining what amounts to a 'safety defect' in a CIoT device, Part 4 of the Report recommends producing consumer guidance, especially in relation to when a security vulnerability will amount to a safety defect. This Part of the Report also recommends amending the defences in the

product liability regime to ensure that it applies to defects introduced after the point of sale, such as defects introduced by software updates, and improvements to how the liability regime applies to defective components of complex products. Furthermore, the Report proposes expanding the liability regime for defective products to allow for recovery for intangible harms, such as data loss and invasion of privacy. Similarly, the Report recommends reforming the product recall regime by allowing for recalls where a device causes, or is likely to cause, intangible harms, such as data loss or invasion of privacy. Finally, this Part of the Report recommends a new mandatory information standard for CIoT devices that would include information about security and privacy risks, software updates and steps consumers can take to secure their devices.

Part 5 of the Report focuses on proposals for reforming the *Privacy Act* to respond to the challenges of CIoT devices and better protect consumer privacy. As with consumer law, the constellation of data-centric technologies and practices, of which CIoT devices form a part, demands new approaches. In particular, data privacy law faces the challenges of regulating data collection, processing and use at scale. In the context of the current fundamental review of the *Privacy Act*, this Report recommends adopting a new paradigm for data privacy regulation. This new paradigm would involve: ex ante measures, such as targeted privacy impact assessments; better calibrating protection in accordance with the risks of data technologies and practices; and ex post measures, such as targeted monitoring and auditing. The principles of privacy protection by default and by design are essential elements of this proposed new paradigm; in implementing these principles, lessons should be learnt from problems encountered with applying these important principles in other jurisdictions, especially the EU. While consideration should be given to adopting a risk-based approach to data privacy regulation, due to inherent limitations in this approach, care should be taken in how the principle is applied in practice.

Approaching the key issues that have been raised as part of the current *Privacy Act* reform process from the perspective of consumers of CIoT devices, this Report supports expanding the definition of 'personal information' and tightening the 'notice and consent' provisions. However, within this context, it is important to bear in mind the limitations of the 'privacy self-management' model, which underpins traditional data privacy laws but falls down in practice. Strengthened 'notice and consent' provisions must therefore be accompanied by measures designed to minimise information and consent fatigue, such as layered notices and standardised consents.

Also following from the limitations of 'privacy self-management', Part 5 of the Report supports proposals for introducing a new privacy principle, requiring the collection, use or disclosure of personal information to be fair and reasonable. When accompanied by an appropriate list of statutory

factors, this broad principle has the potential to establish proportionate limits on new data-centric technologies and practices, including those involving CIoT devices. For example, the principle could be applied to difficult factual circumstances, such as CIoT devices that collect and process third party data without their consent. However, given that CIoT devices installed in the home are acknowledged to be 'high risk', this Report considers that there is a case for additional safeguards over and above the proposed new 'fair and reasonable' standard. In particular, the Report recommends that in a particular application of the principle of privacy by default, where data processing is not essential for the functioning and security of devices, default settings for data processing by CIoT devices installed in the home should be pre-selected to 'off'.

Finally, acknowledging the importance of device security for protecting consumer privacy, Part 5 of the Report supports recommendations for improving the data security principle in APP 11 by clarifying what amounts to 'reasonable steps' to secure personal information.

The recommendations in Parts 3 to 5 of the Report relate to the three specific areas of law and regulation addressed in this Report. As indicated in the Introduction, however, there are issues that cut across these areas. The following sections therefore conclude this Report by taking up the overall themes referred to in the Introduction.

Aligning Laws and 'Joining Up' Regulation

CIoT devices pose challenges to existing laws and regulation that are at least as fundamental as those posed by digital platforms. As Parts 3 to 5 of the Report explain, these expose gaps, weaknesses and potential overlaps in existing laws. This Report suggests that from the perspective of consumers, these challenges merit a response that is at least as comprehensive as the ACCC's process for addressing the legal and policy issues raised by digital platforms.

As explained in the Introduction, a comprehensive and consistent approach is required to respond to the challenges of CIoT devices. This means ensuring that applicable laws are properly aligned. One area that illustrates the importance of aligning laws and regulation is the potential application of multiple regimes to ensuring the security of CIoT devices. Part 3 of this Report made the case for introducing legislation, similar to that introduced in the UK, mandating minimum security standards for CIoT devices, and it seems likely that this will occur. Meanwhile, as referred to in Part 5 of the Report, the data security principle in APP 11 of the *Privacy Act* requires APP entities that hold personal information to take 'reasonable steps' to secure that information. While this Report supports the recommendations in the Attorney-General's 2021 DP aimed at clarifying this principle, the current

reform process has not considered how to align APP 11 with other laws or standards, such as mandatory security standards for CIoT devices.

Turning to consumer protection, as outlined in Part 4 of this Report, the *ACL* includes provisions that may be relevant to the security of CIoT devices. For example, the consumer guarantee that goods must be of an acceptable quality includes the guarantee that they must be reasonably safe and free from defects. The consumer law also includes a guarantee to take reasonable action to provide spare parts and repair facilities. However, there are considerable uncertainties about how the guarantees apply to CIoT devices, and especially how they may apply to security vulnerabilities or defects. While the PC's report on the *Right to Repair* recommended introducing a new consumer guarantee to ensure that consumers have reasonable access to critical software upgrades, including security patches, this falls short of a guarantee that CIoT devices are appropriately secured. Given the importance of securing devices for consumers, however, Part 4 of this Report canvasses the possibility of introducing a new guarantee requiring digital products to be reasonably secure.

There is clearly the potential for inconsistencies between the regimes that may apply to device security. Where there are overlapping laws with different objectives, there are three possible ways for addressing potential overlaps and inconsistencies. First, the distinctive objectives of the existing laws could be accepted as valid, with the laws working in parallel, and inconsistencies or misalignments accepted as necessary by-products of traditional legal silos. While this is not unusual, it can create uncertainty and costs for business and consumers alike, and risks the laws not achieving their objectives. Second, attempts could be made to achieve greater consistency between laws, such as by linking the data security principle in APP 11 to other security standards, such as any mandatory standard for CIoT devices. On this approach, the legal silos could be regarded as complementing each other, with potential inconsistencies minimised. On the other hand, this approach does not necessarily recognise the distinctive rationales for different legal regimes and, for consumers that suffer harm, raises questions about which regime should be pursued to seek redress. Third, an attempt could be made to formulate common principles cutting across legal silos. For example, recognising the central importance of data in the digital economy, a common set of principles could be established to regulate all data collected from consumers, or consumer devices, regardless of whether or not the data are 'personal information'.

While this Report has made a considerable number of recommendations for reforming security, consumer protection and data privacy laws to address the challenges of CIoT devices, the scope of this project means that it has not reviewed all potentially applicable laws. For example, as outlined in the Introduction, this Report does not analyse the application of state and territory surveillance or

listening devices laws to CIoT products. Without further research, the Report has not been able to reach a concluded view on how best to align laws and regulations that apply to CIoT devices. In light of the above analysis, this Report makes the following recommendation.

Recommendation 39

Given the extent to which CIoT devices pose fundamental legal and regulatory challenges, they should be subject to a public policy law reform process, potentially as extensive as the ACCC process investigating the regulation of digital platforms. As part of this process, further research is needed on how best to ensure that all applicable laws and regulations are aligned, including by minimising unnecessary gaps, overlaps or inconsistencies. This process could extend beyond CIoT to include the legal and policy implications of other IoT implementations.

As pointed out in the Introduction to this Report, while aligning laws is important, it is also important to aim for 'joined-up' regulation to promote greater consistency in regulatory practices. The need for 'joined-up' regulation arises from differences in available remedies and enforcement, but also from differences in the skills and perspectives of regulators, and differences in regulatory cultures. For example, in consultations undertaken for this project, understandable questions were raised about the appropriateness and capacity for a consumer protection regulator, such as the ACCC, to regulate technical issues relating to cyber security. In Part 3, this Report recommended that consideration be given to investigating a role for the CISC in regulating the security of CIoT devices. This, however, does not address the proposition, advanced in Part 4 of the Report, that from the point of view of consumers, device security has become a consumer protection issue.

The difficulty in allocating regulatory responsibility for the security of CIoT devices suggests that there is a gap in the regulatory framework. How best to fill this gap is an issue that could be taken up in the fundamental review suggested above. Meanwhile, however, recent and current review processes – such as those being undertaken by the PC, the Attorney-General's Department and Treasury – illustrate the extent to which law reform is being undertaken in policy silos, with many processes taking little or no account of the inter-linkages between legal and regulatory regimes traditionally regarded as distinct. One clear exception to this pattern has been the ACCC's digital platforms process, which represents a positive example of the need for policy reform involving transformative technologies to cut across regulatory regimes. However, this report considers that the challenge of promoting 'joined-up' regulation for transformative technologies requires a more systematic approach.

One theme underlying many of the recommendations relating to regulation made in this Report is the need for government and regulators to adopt a more proactive approach to regulation. Given that, as emphasised throughout this Report, CIoT devices are just one of a constellation of emerging technologies, and that new waves of technologies are on the horizon, this Report suggests that what is needed is a dedicated, multi-disciplinary expert body that proactively investigates the social and legal implications of transformative, or potentially transformative, technologies. Such a body could investigate or apply forward-looking practices, such as horizon scanning, promoting the appropriate use of RegTech and harmonising technical standards and legal rules, as well as proactively identifying gaps, inconsistencies or misalignments in existing laws.[1]

This proposal is not novel. The 2021 Australian Human Rights Commission report on *Human Rights and Technology* recommended establishing a new AI Safety Commissioner.[2] However, this report suggests that as AI is but one of many emerging technologies with immense social implications, it is necessary to go beyond this. This proposal could not only address the problem of the patchwork of approaches taken to law reform identified in this Report, but could assist with more effectively using regulatory resources, such as by proactively addressing problems and avoiding the costs involved with retrofitting or patching laws only after problems emerge. This Report therefore makes the following recommendation.

Recommendation 40

Consideration should be given to establishing a dedicated, multi-disciplinary expert body that proactively investigates the social and legal implications of powerful new technologies. While not directly responsible for regulating, such a body could investigate or apply forward-looking practices such as horizon scanning, promoting the appropriate use of RegTech, and aligning applicable laws and technical standards. Consultation with diverse stakeholders, including consumer representatives and representatives of vulnerable groups, would be an important part of this work.

Consumer Education

As the Introduction to this Report points out, reforming laws alone is not sufficient to address the challenges and risks of the proliferation of CIoT devices; what is needed is a whole-of-society

[1] See World Economic Forum (WEF), *Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators* (Report, December 2020) 40 <https://www3.weforum.org/docs/WEF_Agile_Regulation_for_the_Fourth_Industrial_Revolution_2020.pdf>.
[2] Australian Human Rights Commission, *Human Rights and Technology* (Final Report, June 2021) Recommendation 22, 128 <https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf>.

approach. Empowering consumers by, for example, building greater understanding of the promises and risks of CIoT devices, is an essential element of any strategy aimed at minimising harms. After all, it is always better to avoid problems rather than relying upon legal redress after the event. Just as education is an important component in addressing the challenges of products that pose safety risks – ranging from health products, to children's toys and automobiles – so it must be a part of any policy directed at minimising the threats of CIoT devices. This Report therefore makes the following recommendation.

Recommendation 41

As part of a whole-of-society approach to addressing the risks posed by CIoT devices, a public education campaign should be resourced to assist consumers with managing these risks. If the recommendation for establishing the new advisory body is accepted, this body could play a role in consumer education.

Vulnerable Groups and CIoT Devices

This Report has focused on making general recommendations for reforming cyber security, consumer protection and data privacy laws and regulation to better protect consumers of CIoT devices. The Introduction to this Report explained the particular complexities involved in balancing the undoubted benefits promised by CIoT devices for vulnerable groups and the equally important risks posed for those groups. Furthermore, the Introduction suggests that the best approach to achieving this is to build accessibility and inclusivity into the design of CIoT devices.

Appropriately protecting vulnerable groups raises complex issues that could potentially be addressed by law reforms, but that also require whole-of-society measures, including education of manufacturers and suppliers. The importance of these issues means that they should not be seen as merely an addendum to other policy processes; the issues must be addressed comprehensively and in their own right. Given the need for further research to appropriately address these complexities, this Report does not make any specific recommendations for reforms aimed at maximising the benefits and minimising the harms of CIoT devices for vulnerable groups. If the recommendation for establishing a comprehensive public policy process made in this Report were accepted, how to best promote the interests of vulnerable groups could form a distinct part of that process. Meanwhile, this Report makes the following final recommendation.

Recommendation 42

Further research is needed on how to promote accessibility and inclusivity in relation to CIoT devices to promote the interests of vulnerable groups. This should include research on establishing a framework for promoting inclusive design of CIoT devices. Any public policy law reform process established to comprehensively address the issues raised by CIoT devices should incorporate a distinct component that investigates how to maximise the benefits and minimise the harms posed for vulnerable groups by CIoT devices.

Authors

David Lindsay

Professor David Lindsay is an expert in law and technology, and is widely published in the areas of copyright, privacy and cyberlaw. He is the author of *International Domain Name Law* (Hart, 2007) and co-author of *Public Rights: Copyright's Public Domains* (CUP, 2018). At the University of Technology Sydney, he is the convenor of the Legal Futures and Technology major and co-convenor of the Technology and Intellectual Property Research Cluster. David is a co-editor of the *Australian Intellectual Property Journal.*

Genevieve Wilkinson

Genevieve Wilkinson is a Senior Lecturer in the Faculty of Law, University of Technology Sydney. Her recent publications consider the human rights implications of trade mark law and her current research focuses on the intersection between technology and human rights. She is the Law Tech Challenge Director at UTS and teaches in the areas of technology law, intellectual property law, human rights and international law.

Evana Wright

Evana Wright is a Senior Lecturer in the Faculty of Law, University of Technology Sydney, researching in the fields of intellectual property, the protection of Indigenous traditional knowledge, as well as the regulation of technologies such as IoT devices and databases. Evana was admitted as a legal practitioner in the Supreme Court of New South Wales in 2006 and has previously worked as an in-house legal counsel in Australia and Silicon Valley for major IT corporations and in an ICT research and development incubator. Evana holds a PhD from the University of Technology Sydney, Master of Laws (Honours) also from the University of Technology Sydney, and a Bachelor of Science/Bachelor of Laws from Macquarie University.

Glossary

Definitions of terms commonly used in this document are contained here.

ACCAN	Australian Communications Consumer Action Network
ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ACS	Australian Computer Society
AES	Advanced Encryption Standard
AGDP	Attorney-General's Discussion Paper
AHRC	Australian Human Rights Commission
AI	Artificial Intelligence
APP	Australian Privacy Principles
ASD	Australian Signals Directorate
AWS	Amazon Web Services
CAANZ	Consumer Affairs Australia and New Zealand
CCC	Cybersecurity Certification Centre (Singapore)
CDR	Consumer Data Right (AUS)
CEPT	Conference of Postal and Telecommunications Administrations (EU)
CGL	Consumer Guarantee Law
CIoT	Consumer Internet of Things
CIS	Center for Internet Security (US)
CISC	Cyber and Infrastructure Security Centre
CL	Cybersecurity Label (Finland)
CLS	Cybersecurity Label Scheme (Singapore)
CPRC	Consumer Policy Research Centre
CRA	Consumer Rights Act 2015 (UK)
CSA	Cyber Security Agency (Singapore)
CSD	Consumer Sales Directive (EU)
DCD	Digital Content Directive (EU)

DDCMS	Department for Digital, Culture, Media & Sport (UK)
DDoS	Distributed Denial of Service
DP	Discussion Paper
DPbDD	Data Protection by Design and by Default
DPI	Digital Platforms Inquiry
DRCF	Digital Regulation Cooperation Forum (UK)
ENISA	European Union Agency for Cybersecurity
ESO	European Standards Organization
ETSI	European Telecommunications Standards Institute
EULA	End User Licencing Agreement
GDPR	General Data Protection Regulation (EU)
HIoT	Healthcare Internet of Things
ICO	Information Commissioner's Office (UK)
IGA	Intergovernmental Agreement for the Australian Consumer Law
IIoT	Industrial Internet of Things
IMDA	Info-Communications Media Development Authority (Singapore)
IoT	Internet of Things
IoTAA	Internet of Things Alliance Australia
ioXt	Internet of Secure Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
MoU	Memorandum of Understanding
NCSC	National Cyber Security Centre
NCSC-FI	National Cyber Security Centre Finland
NIST	National Institute of Standards and Technology (US)
NLP	Natural Language Processing
OAIC	Office of the Australian Information Commissioner
OVIC	Office of the Victorian Information Commissioner
PC	Productivity Commission
PIA	Privacy Impact Assessment

PIF	Personal Identification Factor
RIS	Regulation Impact Statement
SGD	Sale of Goods Directive (EU)
SoNS	Systems of National Significance
SRTP	Secure Real Time Protocol
SSRN	Social Science Research Network
TIO	Telecommunications Industry Ombudsman
TLS	Transport Layer Security
ToS	Terms of Service
TPA	Trade Practices Act 1974 (Cth)
TPM	Technological Protection Measure
UCTD	Unfair Contract Terms Directive (EU)
UK CCP	UK Consumer Connectable Products
UNCTAD	United Nations Conference on Trade and Development
WEF	World Economic Forum

References

ABC News, 'New Security Warning for In-Home Smart Cameras' (You Tube, 13 December 2019) https://www.youtube.com/watch?v=GnlIEQt_QFo&t=155s

'About Us', *ETSI* (Web Page, 2022) https://www.etsi.org/about/about-us

Akerlof, George, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 *Quarterly Journal of Economics* 488

Anderson, Ross and Tyler Moore, 'The Economics of Information Security' (2006) 314 *Science* 610

'Apply for the Label', *Traficom* (Web Page, 9 March 2022) https://tietoturvamerkki.fi/en/apply-label

Attorney-General's Department (Cth), *Privacy Act Review* (Issues Paper, October 2020) https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf

Attorney-General's Department (Cth), *Privacy Act Review* (Discussion Paper, October 2021) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf

'August End User Agreement', *August* (Web Page) https://august.com/pages/end-user-agreement

'August Privacy Policy', *August* (Web Page, 24 July 2020) https://august.com/pages/privacy-policy-july-24-2020

'August Terms of Service', *August* (Web Page) https://august.com/pages/terms-of-service

'August Warranty', *August* (Web Page) https://august.com/pages/warranty

Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry* (Final Report, June 2019) https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

Australian Competition and Consumer Commission (ACCC), *Digital Platform Services Inquiry. Discussion Paper for Interim Report No 5: Updating Competition and Consumer Law for Digital Platform Services* (Discussion Paper, 28 February 2022) https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry.pdf

Australian Competition and Consumer Commission (ACCC), *Digital Platform Services Inquiry. Interim Report No 4: General Online Retail Marketplaces* (Interim Report, 31 March 2022) https://www.accc.gov.au/publications/serial-publications/digital-platform-services-inquiry-2020-2025/digital-platform-services-inquiry-march-2022-interim-report

Australian Consumer Law, *Guidance on the Consumer Guarantee as to Acceptable Quality and 'Durability'* (Report, September 2019) https://consumer.gov.au/sites/consumer/files/inline-files/ACL-guidance-durability_0.pdf

Australian Consumer Law, *Guidance on the Consumer Guarantee as to Acceptable Quality and 'Safe'* (Report, December 2017) https://consumer.gov.au/sites/consumer/files/inline-files/ACL-guidance-safe.pdf

Australian Human Rights Commission, *Human Rights and Technology* (Final Report, June 2021) https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf

'Authentication', *Google Safety* (Web Page) https://safety.google/authentication/

Ayres, Ian and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992)

Bailey, Melissa W, 'Seduction by Technology: Why Consumers Opt Out of Privacy in Buying into the Internet of Things' (2016) 94(5) *Texas Law Review* 1023

Baker, Stewart A et al, 'E-Products and the WTO' (2001) 35(1) *International Lawyer* 5

Baldwin, Robert and Julia Black, 'Driving Priorities in Risk-Based Regulation: What's the Problem?' (2016) 43(4) *Journal of Law and Society* 565

Black, Paul, 'Ring Hacked: Doorbell and Camera Security Issues' *NordVPN* (Blog Post, 4 June 2020) https://nordvpn.com/blog/ring-doorbell-hack/

Bogdanor, Vernon (ed), *Joined-Up Government* (Oxford University Press, 2005)

Bradgate, Robert, *Consumer Rights in Digital Products: A Research Report prepared for the UK Department for Business, Innovation and Skills* (Report, Institute for Commercial Law Studies, University of Sheffield, September 2010) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/31837/10-1125-consumer-rights-in-digital-products.pdf

'Browse All Recalls – Smart Devices', *ACCC Product Safety Australia* (Web Page, last updated 14 April 2022) https://www.productsafety.gov.au/recalls/browse-all-recalls?f%5B0%5D=field_psa_product_category%3A4803

'Bug Hunters', *Google* (Web Page) bughunters.google.com

'Built-In Security', *Google Safety* (Web Page) https://safety.google/security/built-in-protection/

Butler, Alan, 'Products Liability and the Internet of (Insecure) Things: Should Manufacturer's Be Liable for Damage Caused by Hacked Devices?' (2017) 50 *University of Michigan Journal of Law Reform* 913

Chamberlain, Lisa, 'Global Consensus Emerges to Secure Internet-Connected Home and Wearable Devices', *World Economic Forum Blog* (Blog Post, 15 February 2022) https://www.weforum.org/press/2022/02/global-consensus-emerges-to-secure-internet-connected-home-and-wearable-devices/

Chapman, Eliza and Tom Uren, *The Internet of Insecure Things* (Issues Paper, Australian Strategic Policy Institute, 2018) https://www.aspi.org.au/report/InternetOfInsecureThings

'CIS Critical Security Controls v 7.1', *Center for Internet Security* (Web Page, 2019) https://www.cisecurity.org/controls/v7

Clifford, Damian and Jeannie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94(10) *Australian Law Journal* 741

Clifford, Damian and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37(1) *Yearbook of European Law* 130

Collingridge, David, *The Social Control of Technology* (Francis Pinter, 1980)

Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council on Consumer Rights*, COM(2008) 614 final

Communications and Digital Committee, House of Lords (UK), *Digital Regulation: Joined-Up and Accountable* (Report No 3 of Session 2021–22, 13 December 2021) https://committees.parliament.uk/publications/8186/documents/83794/default/

Competition & Markets Authority, Information Commissioner's Office and Ofcom, *Digital Regulation Cooperation Forum* (Report, July 2020) https://www.ofcom.org.uk/__data/assets/pdf_file/0021/192243/drcf-launch-document.pdf

'Consolidated Terms and Conditions for Learning Lodge (Australia)', *VTech Electronics (Australia)* (Web Page, last updated 7 April 2016) https://www.vtech.com.au/assets/data/terms_html/VTech-Consolidated_Terms_and_Conditions_for_Learning_Lodge_Australia.html

Consumer Affairs Australia and New Zealand (CAANZ), *Australian Consumer Law Review* (Final Report, March 2017) https://consumer.gov.au/sites/consumer/files/2017/04/ACL_Review_Final_Report.pdf

'Consumer Guarantees', *VTech Australia* (Web Page) https://www.vtech.com.au/consumerguarantees

Consumer Policy Research Centre (CPRC), *Unfair Trading Practices in Digital Markets – Evidence and Regulatory Gaps* (Research and Policy Briefing, December 2020) https://cprc.org.au/wp-content/uploads/2021/11/Unfair-Trading-Practices-in-Digital-Markets.pdf

Consumers International, *The Internet of Things and Challenges for Consumer Protection* (Report, April 2016) https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

Council Directive 2019/2161 of 27 November 2019 on Better Enforcement and Modernisation of Union Consumer Protection Rules [2019] OJ L 328/7

Council Directive 2011/83/EU on Consumer Rights [2011] OJ L 304/64

Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts [1993] OJ L 095/29

Cranor, Lorrie F, 'Informing California Privacy Regulations with Evidence from Research', (2021) 63(3) *Communications of the ACM* 29

'Cybersecurity Labelling Scheme (CLS)', *Cyber Security Agency of Singapore* (Web Page, 30 March 2022) https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls

Cyber Security Agency Singapore, *Cybersecurity Certification Guide* (Report, 2021) https://www.csa.gov.sg/-/media/Csa/Documents/CLS/CSA-Cybersecurity-Certification-Guide.pdf

Cyber Security Agency Singapore, *Cybersecurity Labelling Scheme (CLS): Minimum Test Specifications and Methodology for Tier 4* (Report, v 1.1, April 2021) https://www.csa.gov.sg/-/media/csa/documents/cls/pub-cls--minimum-test-specification-v1-1.pdf

Cyber Security Agency Singapore, *Cybersecurity Labelling Scheme (CLS) Publication No. 1: Overview of the Scheme* (Report, v 1.1, April 2021) https://www.csa.gov.sg/-/media/csa/documents/cls/pub-cls-pub-1---overview-of-cls-v1-1.pdf

Dean, Benjamin C, *Strict Product Liability and the Internet of Things* (Report, Center for Democracy and Technology, 16 April 2018) https://cdt.org/insights/report-strict-product-liability-and-the-internet-of-things/

Department for Digital, Culture, Media & Sport (UK), *Code of Practice for Consumer IoT Security* (Guidelines, 14 October 2018) https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

Department for Digital, Culture, Media & Sport (UK), *Consultation on the Government's Regulatory Proposals Regarding Consumer Internet of Things (IoT) Security* (Report, 1 May 2019) https://www.iotjournaal.nl/wp-content/uploads/2019/05/Consultation_on_the_Government_s_regulatory_proposals_regarding_consumer_Internet_of_Things_security.pdf

Department for Digital, Culture, Media & Sport (UK), *Government Response to the Call for Views on Consumer Connected Product Cyber Security Legislation* (Policy Paper, 21 April 2021) https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation

Department for Digital, Culture, Media and Sport (UK), *Government Response to the 'Regulatory Proposals for Consumer Internet of Things (IoT) Security' Consultation* (Command Paper No Cp213, January 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/862953/Government_response_to_consultation__Regulatory_proposals_for_consumer_IoT_security.pdf

Department for Digital, Culture, Media and Sport (UK), *Mandating Security Requirements for Consumer 'IoT' Products: Consultation Stage Impact Assessment* (Report, May 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950420/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment_V2.pdf

Department for Digital, Culture, Media & Sport (UK), *Secure by Design: Improving the Cyber Security of Consumer Internet of Things* (Report, 7 March 2018) https://www.gov.uk/government/publications/secure-by-design-report

Department for Digital, Culture, Media & Sport (UK), *The Product Security and Telecommunications Infrastructure (PTSI) Bill – Product Security Factsheet* (Factsheet, 24 November 2021, updated 1 December 2021) https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet

Department of Business Innovation & Skills (UK), *Investigatory Powers of Consumer Law Enforcers: Guidance for Businesses on the Consumer Rights Act 2015* (Report, October 2015)

https://www.businesscompanion.info/sites/default/files/Investigatory-powers-of-consumer-law-enforcers-guidance-for-businesses-on-the-Consumer-Rights-Act-2015-Oct-2015.pdf

Department of Home Affairs (Cth), *Australia's Cyber Security Strategy 2020* (Report, 6 August 2020) https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Department of Home Affairs (Cth), *Strengthening Australia's Cyber Security Regulations and Incentives: A Call for Views* (Discussion Paper, 13 July 2021) https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf

Department of Home Affairs and Cyber and Infrastructure Security Centre (Cth), *Protecting Australia Together: Securing Australia's Critical Infrastructure with Asset Owners and Operators, Governments and the Community* (Report, April 2022) https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/protecting-australia-together.pdf

Department of Home Affairs, Australian Signals Directorate and Australian Cyber Security Centre (Cth), *Code of Practice: Securing the Internet of Things for Consumers* (Guidelines, September 2020) https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

Department of Home Affairs, Australian Signals Directorate and Australian Cyber Security Centre (Cth), *Securing the Internet of Things for Consumers: Draft Code of Practice* (Guidelines, December 2019) https://www.iot.org.au/wp/wp-content/uploads/2019/11/19.11.2019-DRAFT-Voluntary-Internet-of-Things-Code-Of-Practice.pdf

Department of the Prime Minister and Cabinet (Cth), *Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity* (Report, 21 April 2016) https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf

Department of the Treasury (Cth), *Enhancements to Unfair Contract Term Protections: Regulation Impact Statement for Decision* (Report, September 2020) https://treasury.gov.au/sites/default/files/2020-11/p2020-125938-ris.pdf

Department of the Treasury (Cth), *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Report, 12 December 2019) https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf

Department of the Treasury on behalf of Consumer Senior Officials, *Improving the Effectiveness of the Consumer Guarantee and Supplier Indemnification Provisions under the Australian Consumer Law* (Consultation Regulation Impact Statement, December 2021) https://treasury.gov.au/sites/default/files/2021-12/c2021-224294-cgsicris_2.pdf

Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Sale of Goods [2019] OJ L 136/28

Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Sale of Goods, Amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L 136/28

Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on Certain Aspects of the Sale of Consumer Goods and Associated Guarantees [1999] OJ L 171/12

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services [2019] OJ L 136/1

Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products [1985] OJ L 210/29

'Enhancements to Unfair Contract Term Protections', *Department of the Treasury (Cth)* (Web Page, November 2020) https://consult.treasury.gov.au/consumer-and-corporations-policy-division/enhancements-to-unfair-contract-term-protections/

Etzioni, Amitai, 'Behavioural Economics: Next Steps' (2011) 34 *Journal of Consumer Policy* 277.

European Commission, *Commission Staff Working Document: A Digital Single Market Strategy for Europe – Analysis and Evidence*, COM(2015) 192 final

European Commission, *Inception Impact Assessment: Adapting Liability Rules to the Digital Age and Circular Economy* (Report No Ref Ares(2021)4266516, 30 June 2021) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en

European Commission, *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*, COM(2015) 634 final 2015/0287

European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence*, COM(2021) 206 final, 21 April 2021

European Data Protection Board, *Guidelines 4/2019 on Article 25: Data Protection by Design and by Default* (v 2.0, adopted on 20 October 2020) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

European Telecommunications Standards Institute (ETSI), *Cyber Security for Consumer Internet of Things* (Technical Specification No ETSI TS 103 645 v1.1.1, February 2019) https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

European Union Agency for Cybersecurity (ENISA), *Good Practices for Security of IoT: Secure Software Development Lifecycle* (Report, 19 November 2019) https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

European Union Agency for Cybersecurity (ENISA), *Industry 4.0 Cybersecurity: Challenges and Recommendations* (Report, 20 May 2019) https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

European Union Agency for Cybersecurity (ENISA), *Recommendations on Shaping Technology According to GDPR Provisions: Exploring the Notion of Data Protection by Default* (Report, December 2018) https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2

'Examples of Processing "Likely to Result in High Risk"', *Information Commissioner's Office (UK)* (Web Page) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-

data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

Fagan, Michael et al, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline* (Report Draft No NISTIR 8259C, National Institute of Standards and Technology, US Department of Commerce, December 2020) https://doi.org/10.6028/NIST.IR.8259C-draft

Fagan, Michael et al, *IoT Device Cybersecurity Capability Core Baseline* (Report No NISTIR 8259A, National Institute of Standards and Technology, US Department of Commerce, May 2020) https://doi.org/10.6028/NIST.IR.8259A

Fagan, Michael et al, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* (Draft NIST Special Publication No 800-213, National Institute of Standards and Technology, US Department of Commerce, December 2020) https://doi.org/10.6028/NIST.SP.800-213-draft

Fagan, Michael et al, *IoT Non-Technical Supporting Capability Core Baseline* (Report Draft No NISTIR 8259B, National Institute of Standards and Technology, US Department of Commerce, December 2020) https://doi.org/10.6028/NIST.IR.8259B-draft

Fagan, Michael et al, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* (Report Draft No NISTIR 8259D, National Institute of Standards and Technology, US Department of Commerce, December 2020) https://doi.org/10.6028/NIST.IR.8259D-draft

'FAQ about Cyber Attack on VTech Learning Lodge', *VTech* (Web Page, last updated 9 January 2018) https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/#!#18

Five Country Ministerial Communiqué, 'Statement of Intent Regarding the Security of the Internet of Things', *GOV.UK* (Web Page, 29-31 July 2019, updated 23 October 2019) https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

Fleuter, Sam, 'The Role of Digital Products under the WTO: A New Framework for GATT and GATS Classification' (2016) 17 *Chicago Journal of International Law* 153

Gellert, Raphaël, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 *International Data Privacy Law* 3

Giliker, Paula, 'The Consumer Rights Act 2015 – A Bastion of European Consumer Rights' (2017) 37 *Legal Studies* 78

Global iRobot (Website) www.global.irobot.com

Goncalves, Maria Eduardo, 'The Risk-Based Approach Under the New EU Data Protection Regulation: A Critical Perspective' (2020) 23(2) *Journal of Risk Research* 139

'Google Privacy Policy', *Google* (Web Page, last update 10 February 2022) https://policies.google.com/privacy?hl=en

'Google Terms of Service', *Google* (Web Page, last updated 5 January 2022) https://policies.google.com/terms?hl=en

Green, Sarah and Djakhongir Saidov, 'Software as Goods' [2007] (March) *Journal of Business Law* 161

Greenleaf, Graham, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford University Press, 2014)

Greenleaf, Graham and Bertil Cottier, 'International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis' (2022) 44 *Computer & Security Law Review* 1

Hadfield, Gillian K, Robert Howse and Michael J Trebilcock, 'Information-Based Principles for Rethinking Consumer Protection Policy' (1998) 21 *Journal of Consumer Policy* 131

Hagemann, Ryan, Jennifer Huddlestone Skees and Adam Thierer, 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (2018) 17(1) *Colorado Technology Law Journal* 37

Hagen, Margaret, *Law by Design* (online, 2020) https://lawbydesign.co/

Harkin, Diarmid, Monique Mann and Ian Warren, 'Consumer IoT and its Under-Regulation: Findings from an Australian Study' (2022) 14 *Policy & Internet* 96

Harris, Kamala D, *California Data Breach Report 2012-2015* (Report, California Department of Justice, Attorney General, February 2016) https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

Harris Interactive, *Consumer Internet of Things Security Labelling Survey Research Findings* (Report, prepared for the UK Government DDCMS, 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf

Hayward, Benjamin, 'E-books and Other Digital Products: Why Australia's Consumer Laws are Lacking' (2018) 44 *Law Society Journal* 28

Hayward, Benjamin, 'What's in a Name? Software, Digital Products and Sale of Goods' (2016) 38 *Sydney Law Review* 441

Helberger, Natali, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 *Common Market Law Review* 1427

Hendry, Justin, 'Gov Pledges to Mandate IoT Cyber Security Standards', *IoTHub* (online, 13 May 2022) https://www.iothub.com.au/news/gov-pledges-to-mandate-iot-cyber-security-standards-579966

'Hippocratic Oath for Connected Medical Devices', *I Am the Cavalry* (Web Page) https://iamthecavalry.org/issues/medical/oath/

Howells, Geriaint, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking EU Law* (Routledge, 2018)

Hypponen, Mikko and Linus Nyman, 'The Internet of (Vulnerable) Things: On Hyponnen's Law, Security Engineering, and IoT Legislation' (2017) 7(4) *Technology Innovation Management Review* 5

Info-Communications Media Development Authority, in consultation with Cyber Security Agency Singapore, *Internet of Things (IoT) Cyber Security Guide* (Guidelines, v 1, March 2020) https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf

'Inspection', *Traficom* (Web Page, 25 April 2022) https://tietoturvamerkki.fi/en/inspection

'Interconnected Devices', *ACCC Product Safety Australia* (Web Page) https://www.productsafety.gov.au/products/electronics-technology/interconnected-devices

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Internet of Things (IoT) – Reference Architecture* (Standard No ISO/IEC 30141:2018(en), 2018) https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en

International Telecommunication Union, *Overview of the Internet of Things* (Recommendation No ITU-T Y.2060, June 2012) https://www.itu.int/rec/T-REC-Y.2060-201206-I

Internet of Things Alliance Australia (IoTAA), *Response to Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper* (Report, 26 August 2021) https://iot.org.au/wp/wp-content/uploads/2021/11/IoTAA-Response-to-Strengthening-Australias-Cyber-Security-Regulations-and-Incentives-Discussion-Paper.pdf

Internet of Things Alliance Australia (IoTAA), Submission to the Department of Home Affairs, *Consultation on Securing the Internet of Things for Consumers: Draft Code of Practice* (1 March 2020) https://www.iot.org.au/wp/wp-content/uploads/2020/03/IoTAA-Submission-to-IoT-Security-Code-of-Practice-1-Mar-2020-Final.pdf

Internet Society, *Internet Society Policy Brief: IoT Privacy for Policymakers* (Report, September 2019) https://www.internetsociety.org/wp-content/uploads/2019/09/IoT-Privacy-Brief_20190912_Final-EN.pdf

'ioXt Security Pledge: The Global Standard for IoT Security', *ioXt* (Web Page, 2021) https://www.ioxtalliance.org/the-pledge

'iRobot & Data Security', *iRobot* (Web Page) https://webapi.irobot.com/Legal/Documents/Asia-Pacific/Australia/Legal-Documents/Data-Security.aspx?sc_lang=eu-GB

'iRobot Terms of Service', *iRobot* (Web Page, last updated 30 September 2016) https://webapi.irobot.com/Legal/Documents/Asia-Pacific/Australia/Legal-Documents/Terms-of-Service.aspx?sc_lang=en-GB&utm_source=App&utm_campaign=App&utm_medium=App

Ivec, Mary and Valerie Braithwaite with Charlotte Wood and Jenny Job, *Applications of Responsive Regulatory Theory in Australia and Overseas: Update* (Occasional Paper 23, Regulatory Institutions Network, Australian National University, March 2015) https://regnet.anu.edu.au/sites/default/files/publications/attachments/2015-05/Occasional%2520Paper%252023_Ivec_Braithwaite_0.pdf

'IXL Home Terms and Conditions of Purchase', *ShopiRobot* (Web Page, 2022) https://www.shopirobot.com.au/terms-and-conditions/

Kaldor, Thomas, '5 Reflections about Legal Design and Reimaging Contract', *LegalVision* (13 July 2020) https://legalvision.com.au/legal-design-and-reimagining-contracts/

Koh, David, 'The Memorandum of Understanding (MoU) on Cooperation in the Field of Recognition of Cyber Security Labelling between the Cyber Security Agency of the Republic of Singapore and the Transport and Communications Agency of the Republic of Finland (Traficom)' (Speech, International IoT Security Roundtable, 6 October 2021) https://www.csa.gov.sg/News/Speeches/speech-by-mr-david-koh-at-the-opening-of-international-iot-security-roundtable-2021

Koops, Bert-Jaap, 'The Trouble with European Data Protection Law' (2014) 4(4) *International Data Privacy Law* 250

Larsen, Gretchen and Rob Lawson, 'Consumer Rights: An Assessment of Justice' (2013) 112 *Journal of Business Ethics* 515

Law Reform Commission, *Product Liability* (Report No 51, 1 June 1989) https://www.alrc.gov.au/publication/product-liability-alrc-report-51/

Legg, Michael and Felicity Bell, *Artificial Intelligence and the Legal Profession* (Hart Publishing, 2020)

Lindsay, David, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131

Lindsay, David, Submission to Attorney General's Department, *Privacy Act Review Discussion Paper* (21 January 2022) https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/view_respondent?_b_index=120&uuId=692946534

Lindsay, David, Evana Wright and Genevieve Wilkinson, *Regulating to Protect Security & Privacy in the Internet of Things (IoT)* (Draft Report, ACCAN, UTS, 11 February 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4052068

Lippi, Marco et al, 'CLAUDETTE: An Automated Detector of Potentially Unfair Clauses in Online Terms of Service' (2019) 27 *Artificial Intelligence and Law* 117

Loos, Marco and Joasia Luzak, *Update the Unfair Contract Terms Directive for Digital Services* (Report No PE 676.006, Study requested by the European Parliament's Committee on Legal Affairs (JURI), February 2021) https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf

Malbon, Justin, Submission to the Department of the Treasury, *Consultation on Enhancements to Unfair Contract Terms Protection – Regulation Impact Statement* (December 2019) https://treasury.gov.au/sites/default/files/2020-11/c2019-5386_dr_justin_malbon.pdf

Manwaring, Kayleen, 'Will Emerging Information Technologies Outpace Consumer Protection Law? – The Case of Digital Consumer Manipulation' (2018) 26 *Competition and Consumer Law Journal* 141

'Mapping Security & Privacy in the Internet of Things', *Copper Horse* (Website, 3 October 2021) https://iotsecuritymapping.uk/

Margolis, Joel et al, 'An In-Depth Analysis of the Mirai Botnet' in Juan E Guerrero (ed), *Proceedings — 2017 International Conference on Software Security and Assistance (ICSSA)* (Conference Paper, Institute of Electrical and Electronics Engineers, 2018)

McConnell, Siobhan, 'Contractual Liability for Defective Internet of Things (IoT) Products – What can the UK Learn from the EU Approach?' (2020) 3 *European Journal of Consumer Law* 481

Micklitz, Hans-W, Lucia A Reich and Kornelia Hagen, 'An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law"' (2011) 34 *Journal of Consumer Policy* 271

Molitorisz, Sacha, *Net Privacy: How We Can Be Free in an Age of Surveillance* (New South Publishing, 2020)

Møller, Gregers, 'Singapore and Finland Sign Agreement to Mutually Recognise IoT Security Labels', *ScandAsia* (online, 9 October 2021) https://scandasia.com/singapore-and-finland-sign-agreement-to-mutually-recognize-iot-security-labels/

Moon, Nathan W, Paul MA Baker and Kenneth Goughnour, 'Designing Wearable Technologies for Users with Disabilities: Accessibility, Usability, and Connectivity Factors' (2019) 6 *Journal of Rehabilitation and Assistive Technologies Engineering* 1

'Nest Additional Terms of Service', *Google Support* (Web Page, last updated 28 February 2022) https://support.google.com/product-documentation/answer/9327735?hl=en&ref_topic=10083519

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009)

Noto La Diega, Guido and Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 7(2) *European Journal of Law and Technology* 1

Obar, Jonathan A and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2018) 23(1) *Information, Communication & Society* 128

Office of the Australian Information Commissioner (OAIC), *MOU with ACCC – Exchange of Information* (MoU, August 2020) https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-of-understanding/mous/mou-with-accc-exchange-of-information

Office of the Victorian Information Commissioner (OVIC), *The Internet of Things and Privacy: Issues and Challenges* (Issues Paper, February 2020) https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/

Ohm, Paul, 'Broken Promises of Privacy' (2010) *57 UCLA Law Review* 1701

O'Neill, Marie, 'Insecurity by Design: Today's IoT Device Security Problem' (2016) 2 *Engineering* 48

Opperman, Ian (ed), *Privacy Preserving Data Sharing Frameworks: People, Projects, Data and Output* (Report, Australian Computing Society, 9 August 2019) https://www.acs.org.au/insightsandpublications/reports-publications/privacy-preserving-data-sharing-frameworks.html

Pasquier, Thomas et al, 'Data provenance to audit compliance with privacy policy in the Internet of Things' (2018) 22 *Personal Ubiquitous Computing* 333

Paterson, Jeannie, 'RegTech and the Future of Customer Protection', *Pursuit* (online, University of Melbourne, 8 September 2017) https://pursuit.unimelb.edu.au/articles/regtech-and-the-future-of-customer-protection

Paterson, Jeannie, 'The Australian Unfair Contract Terms Law: The Rise of Substantive Unfairness as a Ground for Review of Standard Form Consumer Contracts' (2009) 33(3) *Melbourne University Law Review* 934

Paterson, Jeannie, 'Unconscionable Bargains in Equity and Under Statute' (2015) 9 *Journal of Equity* 188

Paterson, Jeannie Marie, 'Critique and Comment: The New Consumer Guarantee Law and the Reasons for Replacing the Regime of Statutory Implied Terms in Consumer Transactions' (2011) 35(1) *Melbourne University Law Review* 252

Paterson, Jeanie Marie, *Corones' Australian Consumer Law* (Thomson Reuters, 4th ed, 2019)

Paterson, Jeannie Marie and Elise Bant, 'Should Australia Introduce a Prohibition on Unfair Trading? Responding to Exploitative Business Systems in Person and Online' (2021) 44 *Journal of Consumer Policy* 1

Paterson, Jeannie Marie and Gerard Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) 38 *Journal of Consumer Policy* 331

Peppet, Scott R, 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent' (2014) 93 *Texas Law Review* 85

Piasecki, Stanislaw and Jiahong Chen, 'Complying with the GDPR when Vulnerable People use Smart Devices' (2022) *International Data Privacy Law* (forthcoming)

'Privacy and Terms of Use', *Tapo* (Web Page, 24 July 2019) https://www.tapo.com/au/privacy/#terms-of-use

'Privacy Notice for Audio Collection from Children's Features on Google Assistant', *Hey Google* (Web Page, last updated 2 September 2021) https://assistant.google.com/privacy-notice-childrens-features/?hl=en_GB

'Privacy Policy', *VTech Australia* (Web Page, last updated 17 March 2020) https://www.vtech.com.au/privacy_policy

'Privacy Policy VTech', *Leap Frog* (Web Page, 24 May 2018) https://www.leapfrog.com/en-gb/legal/vtech-privacy-policy/vtech-privacy-policy-uk

Productivity Commission, *Review of Australia's Consumer Policy Framework* (Inquiry Report No 45, 30 April 2008) v1 https://www.pc.gov.au/inquiries/completed/consumer-policy/report/consumer1.pdf

Productivity Commission, *Right to Repair* (Inquiry Report No 97, 29 October 2021) https://www.pc.gov.au/inquiries/completed/repair/report/repair.pdf

'Products', *Traficom* (Web Page) https://tietoturvamerkki.fi/en/products

Purtova, Nadezhda, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40

Richardson, Megan et al, 'The Internet of Things (IoT) and the Meaning of "Personal Data": A Case Study in Regulation for Rights' (2020) 3 *European Journal of Consumer Law* 503

Ring (Website) https://ring.com/au/en

'Ring Australia Terms of Service', *Ring* (Web Page, last updated 6 May 2020) https://ring.com/au/en/terms#TOS-AU

Ring, *End-to-End Encryption* (White Paper, January 2021) https://assets.ctfassets.net/a3peezndovsu/7bwgu7ybi1XoyH61pDraYT/94e4bab9347d4abe07f8d843fdfd4bd4/Ring_Encryption_Whitepaper_FINAL.pdf

Rodríguez-Rodríguez, Ignacio et al, 'Towards a Holistic ICT Platform for Protecting Intimate Partner Violence Survivors Based on the IoT Paradigm' (2020) 12(1) *Symmetry* 37

Rosner, Gilad and Erin Kenneally, *Clearly Opaque: Privacy Risks of the Internet of Things* (Report, Internet of Things Privacy Forum, May 2018) https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54

Schwartz, Paul M and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86(6) *New York University Law Review* 1814

'Security and Privacy', *Google Safety* (Web Page) https://safety.google/security-privacy/

'Security Center', *August* (Web Page) https://august.com/pages/security-center

'Security Updates and Security Validation Results for Google Nest Devices', *Google Support* (Web Page, 2022) https://support.google.com/product-documentation/answer/10231940#

Sein, Karin, 'What Rules Should Apply to Smart Consumer Goods? Goods with Embedded Digital Content in the Borderland between the Digital Content Directive and "Normal" Contract Law' (2017) 8(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* 96

Solove, Daniel J, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880

Telecommunications Industry Ombudsman (TIO), *Terms of Reference* (12 November 2019) https://www.tio.com.au/sites/default/files/2020-03/TIO%20TERMS%20OF%20REFERENCE_FINAL%2012%20November%202019.pdf

Tene, Omer, 'Privacy: The New Generations' (2011) 1(1) *International Data Privacy Law* 15

Traficom, *Cybersecurity Label – Help your Customers Make Secure Choices* (Report, 2022) https://tietoturvamerkki.fi/sites/default/files/media/file/cybersecurity-label-infopack-for-companies.pdf

Traficom, *Statement of Compliance for the Cybersecurity Label* (Application Form, 2022) https://tietoturvamerkki.fi/sites/default/files/media/file/statement-of-compliance-for-the-cybersecurity-label.pdf

Traficom, *Terms of Use – Cybersecurity Label for IoT Consumer Devices* (Terms of Use, 1 March 2022) https://tietoturvamerkki.fi/sites/default/files/media/file/Terms%20of%20Use%20%E2%80%93%20Cybersecurity%20Label%20for%20IoT%20consumer%20devices.pdf

Traficom, The Finnish Cybersecurity Label (Presentation, 28 August 2020) https://tietoturvamerkki.fi/sites/default/files/media/file/cybersecurity_label_presentation-280920.pdf

Tusikov, Natasha, 'Regulation Through "Bricking": Private Ordering in the "Internet of Things"' (2019) 8(2) *Internet Policy Review* 1.

Twigg-Flesner, Christian, 'Information Disclosure about the Quality of Good – Duty or Encouragement?' in Geraint Howells, André Janssen and Reiner Schultz (eds), *Information Rights and Obligations: A Challenge for Party Autonomy and Transactional Fairness* (Routledge, 2005) 135.

United Nations Conference on Trade and Development (UNCTAD), *Manual on Consumer Protection* (United Nations Publication No UNCTAD/WEB/DITC/CLP/2016/1, 2016) https://unctad.org/system/files/official-document/webditcclp2016d1.pdf

Vanherpe, Jozefien, 'White Smoke, but Smoke Nonetheless: Some (Burning) Questions Regarding the Directives on Sale of Goods and Supply of Digital Content' (2020) 2 *European Review of Private Law* 251

Waldman, Ari Ezra, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53(1) *Cornell International Law Journal* 147

Warren, Ian, Monique Mann and Diarmaid Harkin, *Enhancing Consumer Awareness of Privacy and the Internet of Things* (Report, Deakin University, ACCAN, August 2021) https://accan.org.au/files/Grants/2021%20Deakin%20IoT/Deakin%20grants%20report_v5_web.pdf

Wendehorst, Christianne, 'Sale of Goods and Supply of Digital Content – Two Worlds Apart? Why the Law on Sale of Goods Needs to Respond Better to the Challenges of the Digital Age' (Research Paper No PE556.928, European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, 2016) https://www.europarl.europa.eu/cmsdata/98774/pe%20556%20928%20EN_final.pdf

Whitmore, Andrew, Anurag Agarwal and Li Da Xu, 'The Internet of Things – A Survey of Topics and Trends' (2015) 17 *Information System Frontiers* 261

Whittaker, Zack, 'Amazon Ring Doorbells Exposed Home Wi-Fi Passwords to Hackers' *Tech Crunch* (Web Page, 8 November 2019) https://techcrunch.com/2019/11/07/amazon-ring-doorbells-wifi-hackers/

'Who We Are', *Cyber Security Agency of Singapore* (Web Page, 25 April 2022) https://www.csa.gov.sg/Who-We-Are/Our-Organisation

Wilhelmsson, Thomas, 'Consumer Law and Social Justice' in Iain Ramsay (ed), *Consumer Law in the Global Economy: National and International Dimensions* (Ashgate, 1997) 217

Winn, Jane K, 'Information Technology Standards as a Form of Consumer Protection Law' in Jane K Winn (ed), *Consumer Protection in the Age of the 'Information Economy'* (Ashgate, 2006) 99

World Economic Forum (WEF), *Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators* (Report, December 2020) https://www3.weforum.org/docs/WEF_Agile_Regulation_for_the_Fourth_Industrial_Revolution_2020.pdf

World Economic Forum, with Consumers International, Cybersecurity Tech Accord and I Am the Cavalry, *Joint Statement of Support on Consumer IoT Device Security: Industry, Hackers, and Consumers for a Global Baseline for Consumer IoT Security* (Consensus Statement, 15 February 2022) https://cybertechaccord.org/industry-hackers-and-consumers-for-a-global-baseline-for-consumer-iot-security/

Wright, Evana et al, Submission to Department of Home Affairs, *Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper* (27 August 2021) https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/wright-lindsay-wilkinson-fraser-and-collings.pdf

Yeung, Karen, Andrew Howes and Ganna Progebna, 'AI Governance by Human-Rights Centred Design, Deliberation and Oversight: An End to Ethics Washing' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (Oxford University Press, 2019)

'Your Privacy with Ring', *Ring* (Web Page) https://support.ring.com/hc/en-us/articles/360043469371-Your-Privacy-with-Ring

Yu, Eileen, 'Singapore Inks Pact with Finland to Mutually Recognise IoT Security Labels', *ZDNet* (online, 7 October 2021) https://www.zdnet.com/article/singapore-inks-pact-with-finland-to-mutually-recognise-iot-security-labels/

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)

Regulation of Internet of Things Devices to Protect Consumers