DRAFT

Regulating to Protect Security & Privacy in the Internet of Things (IoT)

Draft Report

David Lindsay, Genevieve Wilkinson & Evana Wright

January 2022

Regulating to Protect Security & Privacy in the IoT: Consultation Document

Authored by **David Lindsay, Genevieve Wilkinson & 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

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

Table of Contents

Preface & Acknowledgements

This is a draft report from the ACCAN funded-project, “Regulating to Protect Security & Privacy in the Internet of Things (IoT)”. This report is intended for the purpose of consultation.

The authors acknowledge the assistance of Dr Henry Fraser, who was primarily responsible for researching the sections of this report on data security and Dr Neva Collings, who was primarily responsible for researching the sections of this report on labelling.

Recommendations

Recommendation 1

General cyber security legislation should be introduced, following a public consultation process, to enhance cyber security standards across business sectors. General cyber security legislation could establish the framework for regulatory measures in particular industry sectors, such as mandating standards or the development of codes of practice, or mandating labelling schemes.

Recommendation 2

In the absence of general cyber security regulation (as described in Recommendation 1) legislation should be introduced to regulate the security of consumer IoT devices. The legislation should impose mandatory minimum obligations on relevant entities, such as manufacturers, importers and distributors of IoT consumer devices. The minimum obligations should require compliance with security principles set out in the Australian code and/or designated technical standards.

Recommendation 3

A mandatory labelling scheme should be introduced as part of an IoT security regulatory regime. Any mandatory labelling scheme must be properly resourced to ensure satisfactory testing, certification and enforcement. As part of the regime, a government entity should be responsible for evaluating products according to criteria that assist consumers with exercising informed choices concerning security risks.

Recommendation 4

In the absence of a mandatory labelling scheme, a voluntary scheme with government backing, such as Singapore's CLS, should be introduced and properly resourced. This should incorporate an obligation on relevant persons to include a Statement of Compliance and an authoritative list of labelled products.

Recommendation 5

A new sui generis *category for digital products, distinct from 'goods' and 'services', should be introduced to the ACL. A new category is recommended because digital products are sufficiently different from traditional consumer products to merit the application of specifically tailored consumer guarantees. A new category would also reduce uncertainties in determining whether a consumer IoT device, or elements of the device, are 'goods' or 'services'. In introducing a new legislative category,*

care would be needed in defining the category, and in determining when elements of a complex product are sufficiently integrated with the product so as to form part of that product.

Recommendation 6

In association with the introduction of a new category of digital products, a set of consumer obligations should be developed that are specifically tailored to such products, including consumer IoT devices. The obligations should include requirements for: any software elements to be up to date and regularly updated; the devices to be reasonably secure; and for the elements of hybrid devices (including hardware, software and data elements) to be properly integrated.

Recommendation 7

In the absence of a more fundamental reform, a deeming provision should be introduced to the ACL to provide that the consumer guarantees apply to software embedded in integrated products and to internet-connected products as a whole.

Recommendation 8

In the absence of more fundamental reforms, as recommended by the Productivity Commission, the ACL should be amended to include a new consumer guarantee to provide reasonable software updates for a reasonable time.

Recommendation 9

All suppliers of digital products should be required to ensure that clear explanations of prescribed contractual terms, including warranties, are made available to consumers before purchase. The contractual terms and conditions should also be publicly available on supplier websites. We recommend that additional proposals be investigated for improving access to terms and conditions for consumer IoT devices, such as requiring that the information about terms and conditions be disclosed to the ACCC to be published on a publicly available register of contracts for digital products with obligations to notify and update any changes or requiring terms and conditions to be lodged with any statement of compliance required to obtain a ratings label.

Recommendation 10

The government should expedite work on producing options for introducing a statutory prohibition of unfair trading, which should be aimed particularly at addressing predatory and manipulative conduct associated with data-driven business models. The boundaries of any prohibition should be carefully

calibrated so that it is proportionate and does not extend to legitimate business practices. The prohibition should be regarded as a 'safety net' that forms one element of a layered regulatory regime.

Recommendation 11

Consideration should be given to establishing a more 'layered' regime than the current unfair contract terms law for regulating unfair terms in standard form consumer contracts by introducing a black list of prohibited terms or a grey list of presumptively unfair terms, or a combination of both.

Recommendation 12

The ACCC should be resourced to investigate and potentially design machine learning tools to assist it in the identification of unfair terms in standard form consumer contracts. Such tools may be particularly helpful in enforcing the unfair contract terms law if the law is amended to include black and/or grey lists of categories of unfair terms.

Recommendation 13

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

Recommendation 14

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 may be enacted by introducing a new sub-section under section 142(a): '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.' It is acknowledged that such an approach is contingent upon the introduction of a category of 'digital products' being introduced into the ACL (consistent with recommendation 5 set out above).

Recommendation 15

In the event that a product liability claim involves a consumer IoT device with components, the consumer may bring an action against the ultimate supplier or manufacturer and the burden shall rest with the supplier or manufacturer to reach a determination as to liability between the providers of the component parts.

Recommendation 16

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 to tangible property or intangible personal property including data loss.

Recommendation 17

Australian data privacy law should be amended to 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 data processing practices, while allowing for more effective regulatory oversight. Such measures should include targeted privacy impact statements, data protection by default and by design, and targeted monitoring and auditing.*

Recommendation 18

As proposed by the Attorney-General's Discussion Paper (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, including the definition of 'personal data' under the GDPR.*

Recommendation 19

The amendments proposed by the DP 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 20

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 processing at scale. This could, for example, lead to some re-formulation of the APPs.*

Recommendation 21

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.

Recommendation 22

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.*

Recommendation 23

As proposed in the Attorney-General's DP, 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 any inconsistencies, should prevail. As further proposed in the DP, 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 DP could be improved, such as by ensuring that an objective standard is applied in assessing the risk of data processing.

Recommendation 24

Consideration should be given to whether certainty could be improved by introducing elements of a risk-based approach to the collection, use or disclosure of personal information. This could involve drawing distinctions between data processing which poses unacceptable risks, which would be prohibited, processing which poses high risks, which might be presumed to be unfair or unreasonable unless they are justified, and processing which is deemed to be low risk.

Recommendation 25

Except where data processing is essential for the functioning of a consumer IoT device, default settings allowing for data processing by means of such devices should be pre-selected to 'off'.

Recommendation 26

To minimise the possibility of inconsistency across regulatory regimes, the principle of 'joined-up regulation' should be applied across regimes that regulate device security, including any sui generis *security law, consumer protection law and data privacy law. At a minimum, the data security principle in APP 11.1 should be expressly linked to mandatory minimum security standards introduced by* sui

generis *legislation that applies to IoT devices and to any proposed new consumer guarantee of 'reasonable security' for digital products.*

Introduction

This is the draft report for the ACCAN-funded project, *"Regulating to Protect Security & Privacy in the Internet of Things (IoT)".* The report is designed primarily for the purposes of consultation with stakeholders but will be circulated widely to maximise the opportunity for feedback. It sets out the draft recommendations from the project and the reasoning supporting the recommendations.

This draft report takes into account substantial feedback on a preliminary report that was released in July 2021, and which was the subject of a stakeholder roundtable held on 15 July 2021. As explained further below, the report takes into account significant relevant policy developments that have occurred since the release of the preliminary report.

Objectives

The overall objectives of this project are:

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.
5. To produce informed commentary on, and analysis of, best practice guidelines for implementing high level principles for securing consumer IoT devices.

Scope of this report

The draft report addresses objectives (1) and (2) of the project objectives, in that it sets out recommendations for legal and regulatory reform, which are based on comprehensive analysis of Australian data security, consumer and privacy laws.

The project is confined to analysing issues relating to **consumer IoT devices for the home,** such as connected appliances and smart assistants, and does not generally extend to all consumer IoT devices,

such as mobile devices and (with one exception) 'wearables'. The decision to target consumer IoT devices for the home was made to ensure that the project is manageable but was also based on the assumption that limiting the focus of the research in this way will deliver important insights. That said, there are common issues that arise in the regulation of all consumer IoT devices and, indeed, in the regulation of current generation 'disruptive technologies' more broadly. In particular, these technologies are based on business practices that rely largely upon the collection, analysis and use of data at scale. The regulation of consumer IoT devices for the home therefore represents a microcosm of 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 consumer IoT devices for the home.

As set out in objective (2), this project focuses on three substantive areas of the law, which we consider are most relevant to the regulation of consumer IoT devices, at least for the purposes of the project: **data 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 IoT devices. On the contrary, areas such as contract law and competition law are also clearly highly significant in the regulation of IoT devices. Nevertheless, it is clear that, from the perspective of consumers, the three identified areas are the most important and relevant. That said, the project refers to other areas of the law where they might be especially relevant to policy debates relating to the regulation of IoT devices.

The Evolving Policy Context

Given that, as explained above, the issues involved with the regulation of consumer IoT 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 are relevant to the project. One of the challenges faced by a project such as this is responding to a rapidly evolving policy context. While, on the whole, the policy initiatives do not specifically target the regulation of consumer IoT 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 privacy and consumer protection law to better reflect technological change essentially arose from the comprehensive 2019 report of the Australian Competition and Consumer Commission (ACCC) arising from its inquiry into digital platforms, which is known as the *DPI Report.*[1] The *DPI Report* addressed fundamental legal and regulatory issues relating to data-centric business models and practices, which extended beyond the specific issues raised by

[1] Australian Competition and Consumer Commission (ACCC). 2019. Digital Platforms Inquiry, Final Report, June 2019.

digital platforms; and the scope of the report is illustrated by the extent to which its reverberations are being felt across a range of policy areas. Other policy processes, including those relating to data security, have distinct origins. The main substantive policy developments which have occurred since the release of the preliminary report, and which are taken into account in this draft report, are as follows:

- Department of Home Affairs, discussion paper on *Strengthening Australia's cyber security regulations and incentives,* released on 13 July 2021.[2] The discussion paper, arising from Australia's Cyber Security Strategy, includes options for setting cyber security expectations, increasing transparency and protecting consumer rights, including for smart IoT devices.
- Attorney-General's Department, discussion paper on the *Privacy Act Review,* released on 25 October 2021.[3] The Privacy Act Review, which arise from the ACCC's *DPI,* is a fundamental review of Australian data privacy law, and 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,* released on 29 October 2021.[4] 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.

In addition to these significant policy processes, this report takes into account relevant legislative amendments, or proposed amendments, such as the exposure draft legislation released in August 2021, aimed at strengthening and clarifying the unfair contracts law.[5]

While taking into account these policy initiatives, this draft report places these developments in the specific context of the challenges of regulating consumer IoT devices. As illustrated by this report, this casts light on the connections between what are commonly regarded as distinct areas of the law, and the distinct policy processes. As explained immediately below, the project is investigating measures to address the challenges of what is commonly known as 'joined-up regulation'.

[2] Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021.
[3] Attorney-General's Department, Privacy Act Review, Discussion Paper (25 October 2021).
[4] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021.
[5] Treasury Law Amendment (Measures for a later sitting) Bill 2021: Unfair contract terms reform (Cth).

The Challenge of Joined-up Regulation

In a report released in December 2021, the Communications and Digital Committee of the UK House of Lords reiterated the findings of a 2019 report on digital regulation, 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.[6]

As is clear from this draft report, policy development in Australia faces similar problems, with gaps and inconsistencies in the law arising from separate legal silos – such as data security, consumer protection and data privacy laws – and piecemeal policy processes following their own regulatory tracks. For example, the Productivity Commission report on the *Right to Repair* considers reforms to the consumer guarantees within the context of durability and repair of consumer devices that incorporate software but does not address broader problems raised by the application of the consumer guarantees to smart, connected consumer devices. Similarly, while the data security principle embodied in APP 11.1 is an accepted element of data privacy law, the Attorney-General's discussion paper on the *Privacy Act Review,* does not directly address the implications of potential inconsistencies arising from multiple legal regimes applying to data or device security.

Addressing this overall problem is commonly known as the challenge of 'joined-up regulation' or 'joined-up government'.[7] While this draft report has identified the importance of establishing appropriate links between different legal and regulatory regimes, the project is still working on proposals for promoting 'joined-up regulation' in the context of consumer IoT devices. As suggested by the House of Lords' report referred to above, this may well involve some degree of institutional reform, or procedural reforms aimed at enhancing coordination across regulatory silos. In the meantime, we would appreciate feedback which includes suggestions about practical measures that may be taken to improve 'joined-up regulation' in the context of the issues explored in this project.

[6] House of Lords (UK), Communications and Digital Committee, Digital regulation: joined-up and accountable, HL Paper 126, 13 December 2021, citing Communications and Digital Committee, Regulating in a digital world (2nd Report, Session 2017–19, HL Paper 299), para 223

[7] See, for example, V. Bogdanor (ed), Joined-up Government (OUP, 2005); World Economic Forum (WEF), Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators (December 2020).

Structure of this report

This draft report is structured in three parts. First, it introduces consumer IoT devices for the home, and identifies the features of those devices that pose challenges for data security, consumer protection and data privacy laws and regulation.

Secondly, the report sets out the case studies, which focus on specific consumer IoT devices, and which the project uses to identify and illustrate the problems faced by consumers in relation to consumer IoT devices. The case studies are referred to, at relevant points, in the analysis of the legal and policy issues addressed in the substantive areas of the report.

Thirdly, the report identifies the legal challenges, and makes recommendations for law reform in each of the three areas addressed by the report: data security, consumer protection and data privacy law. For the purpose of this report, the focus is on the recommendations and the reasoning supporting the recommendations. The recommendations in this draft report have been substantially revised and amended to take into account feedback received on the preliminary report, and the significant policy developments that have occurred since the preliminary report. In addition, since the release of the preliminary report, significant research has been completed on areas that were not fully addressed in the preliminary report, specifically security labelling of consumer devices and the product safety provisions of the Australian Consumer Law (ACL), which regulate unsafe products and product-related services.

Future Research Directions

The final report from this project will be delivered in May 2022. The final report will take into account feedback received on this draft report. In addition, the final stage of this project will include research on three areas not covered in full in this draft report. First, as signalled above, the final report will incorporate proposals for dealing with the challenges of enhancing 'joined-up regulation' in this area. Secondly, the project will include further research on measures to improve protection for vulnerable consumers. This will incorporate feedback on proposals that were made for reforming statutory unconscionability provisions in the ACL in the preliminary report but will go beyond this to consider further reforms that recognise the particular impact of the problems identified in this report on the vulnerable. Finally, feedback received on the preliminary report emphasised the importance of effective arrangements for enforcing laws aimed at protecting consumers. While this draft report includes some analysis of reforms to enhance enforcement of the ACL, the final stage of the project will expand upon this with a view to developing proposals for improving enforcement of the data privacy and data security laws.

1. Regulatory challenges of consumer IoT devices

What are consumer IoT devices?

There is no single, accepted definition of the Internet of Things (IoT).[8] In colloquial terms, it refers to physical products with embedded software that are connected ('always on') to the Internet.[9] The following more formal, technical definition was adopted by the International Telecommunication Union (ITU) in 2012, which remains applicable today:

> 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.[10]

An essential characteristic of an IoT device is that it incorporates 'sensors' which enable data to be collected, distributed and acted upon.[11]

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, consumer IoT and healthcare IoT.[12] Due to the distinct and significant security challenges arising from consumer devices, initial IoT-specific regulation has focused on 'consumer IoT', which a 2019 European technical specification defines as:

> network-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.[13]

The specification includes an illustrative list of consumer IoT devices, including: connected children's toys and baby monitors; connected safety-relevant products, such as smoke detectors and door locks;

[8] A. Whitmore, A. Agarwal & L.D. Shu, 'The Internet of Things – A survey of topics and trends' (2015) 17 Information System Frontiers 261.
[9] N. Tusikov, 'Regulation through "bricking": private ordering in the "Internet of Things"' (2019) 8(2) Internet Policy Review 1, 2.
[10] International Telecommunication Union, Overview of the Internet of things: Recommendation ITU-T Y.2060, Geneva, ITU, 2012.
[11] N. Tusikov, 'Regulation through "bricking": private ordering in the "Internet of Things"' (2019) 8(2) Internet Policy Review 1, 2.
[12] 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 (2019), Industry 4.0 Cybersecurity: Challenges and Recommendations; ENISA (2019), Good Practices for Security of IoT.
[13] ETSI (2019), CYBER: Cyber Security for Consumer Internet of Things, Technical Specification ETSI TS 103 645.

smart cameras, TVs and speakers; wearable health trackers; connected home automation and alarm systems; connected appliances (eg, washing machines, fridges); and smart home assistants.[14]

In general, this report adopts this approach to the scope of consumer IoT devices, but it confines itself to consumer devices that are used in the home. It therefore excludes devices which are intended to be worn on the person, such as health monitors (which raise specific regulatory issues) and other wearables (with the exception of a case study on a children's smartwatch). 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 regulatory issues. As a result, most, but not necessarily all, of these communications devices are commonly excluded from regulations that apply to IoT devices.

Data security challenges

At its core, the rationale for regulating the safety and security of consumer IoT 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.[15] However, insecure IoT devices give rise to the following problems - largely associated with their connected, 'always on' characteristic – over and above the safety concerns relating to 'unconnected' products:

- *Vulnerability and weak security.* IoT consumer devices are vulnerable because they have limited processing power, which creates challenges for the processing of data necessary to ensure security. Moreover, the large number of connected IoT devices with poor security creates a large attack surface for malicious actors.[16] As summed up in Hyponnen's law, 'Whenever an appliance is described as "smart", it's vulnerable'.[17] This means that the security of sensitive IoT devices, such as IoT-enabled locks, temperature-control devices or children's toys, may be compromised.
- *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

[14] Ibid. 6.

[15] G. Hadfield, R. Howse & M. Trebilcock, 'Information-based Principles for Rethinking Consumer Protection Policy' (1998) 21 Journal of Consumer Policy 131; C. Twigg-Flesner, 'Information Disclosure about the Quality of Good – Duty or Encouragement?' in G. Howells, A. Janssen & R. Schultz (eds), Information Rights and Obligations: A Challenge for Party Autonomy and Transactional Fairness (Routledge, New York, 2005) 135-153.

[16] M. O'Neill, 'Insecurity by Design: Today's IoT Device Security Problem' (2016) 2 Engineering 48; E. Chapman & T. Uren, The Internet of Insecure Things: Issues Paper, Australian Strategic Policy Institute, 2018.

[17] Mikko Hypponen & Linus Nyman, 'The Internet of (Vulnerable) Things: On Hyponnen's Law, Security Engineering, and IoT Legislation' (2017) 7(4) Technology Innovation Management Review 5.

third parties to cause harms, such as unauthorised access to data or adverse effects on the operation of devices, remotely.

- *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.[18] The best known of these attacks have involved the Mirai 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.[19]

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 has 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'.[20]

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 which arise from consumers having inadequate information or behavioural biases.[21] Secondly, consumer law can be seen as being necessary to protect the positive rights of consumers, and so as protecting consumer autonomy and dignity.[22] Thirdly, taking inequality as a starting point, consumer law can be conceived as a means for promoting distributive justice, by policies aimed at redistributing wealth and guaranteeing access to basic goods and services.[23]

The objectives of the Australian Consumer Law (ACL), which were drawn from a 2008 Productivity Commission report,[24] are essentially 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

[18] Department for Digital, Culture, Media & Sport (DDCMS) (UK), Secure by Design: Improving the cyber security of consumer Internet of Things Report (2018).
[19] J. Margolis et al, 'An In-Depth Analysis of the Mirai Botnet', International Conference on Software Security and Assistance, 2017.
[20] J. Winn, 'Information Technology Standards as a Form of Consumer Protection Law' in J. Winn (ed), Consumer Protection in the Age of the 'Information Economy' (Routledge, London, 2006).
[21] Hans-W Micklitz, Lucia A Reich & 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.
[22] Gretchen Larsen & 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, 2016).
[23] United Nations Conference on Trade and Development (UNCTAD), Manual on Consumer Protection (United Nations, 2016).
[24] See Productivity Commission, Review of Australia's Consumer Policy Framework, Final Report, Vol. 1, Canberra, 2008.

mandatory standards (the 'consumer guarantees') to address the information asymmetry between consumers and suppliers.[25] Nevertheless, elements of the regime can be regarded as aimed at enhancing consumer rights.

While consumer IoT 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 section of the report identifies the specific challenges posed by IoT consumer 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 IoT devices. Many of the challenges relate to the complexity of IoT 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 service providers significant ongoing power over the devices.[26]

- *Hybrid nature of consumer IoT devices*

IoT consumer devices are complex products, which may consist of hardware, software, data and service components.[27] Moreover, the extent to which the functions of the devices depend upon software, which may be automatically updated by AI 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.[28] The complex nature of IoT devices may even mean that it is difficult to determine what is meant by the 'product' covered by a consumer contract with a supplier.[29]

- *Opacity of IoT devices*

IoT devices are subject to software upgrades, which are necessary to ensure the security of the devices but may result in significant changes to the 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 changes in the way in which devices work. Consumers therefore often have imperfect information about the nature of the product they are purchasing, about how it might be changed and about how it works.[30]

[25] 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.
[26] N. Tusikov, 'Regulation through "bricking": private ordering in the "Internet of Things"' (2019) 8(2) Internet Policy Review 1.
[27] Consumers International, The Internet of Things and challenges for consumer protection (Consumers International, London, 2016) p.33.
[28] Guido Noto La Diega & Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 7(2) European Journal of Law and Technology 1, 4.
[29] 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, 8.
[30] Consumers International, The Internet of Things and challenges for consumer protection (Consumers International, London, 2016) pp. 28-29.

- *'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 IoT devices on software upgrades, including security upgrades, 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'.[31]

- *Complexity of legal liability*

The complex nature of IoT devices, and the complex nature of 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.[32] Moreover, IoT devices are often subject to multi-layered contracts with, for example, separate contracts relating to device hardware and software services.[33] The complexity of IoT 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.

- *Complexity of ownership*

The hybrid nature of IoT 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 a EULA, with ownership remaining in the software provider. This split in ownership means that, amongst other things, 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.

- *Obstacles to repairing devices*

As noted previously, the complex nature of IoT devices may make it difficult to determine what has gone wrong with a device where there is a fault or defect. Furthermore, as IoT devices are controlled by software, consumers may encounter obstacles in having devices repaired. For example, the software may be subject to a technological protection measure (TPM), such as encryption, which can inhibit or prevent repair.[34]

[31] N. Tusikov, 'Regulation through "bricking": private ordering in the "Internet of Things"' (2019) 8(2) Internet Policy Review 1.

[32] Consumers International, The Internet of Things and challenges for consumer protection (Consumers International, London, 2016) p. 29.

[33] Guido Noto La Diega & Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 7(2) European Journal of Law and Technology 1.

[34] Consumers International, The Internet of Things and challenges for consumer protection (Consumers International, London, 2016) p. 34.

- *Consumer lock-in*

The complex nature of consumer IoT 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 IoT 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.[35]

- *Jurisdictional issues*

Some of the multiple parties involved in supplying consumer IoT 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.[36]

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.[37] The objectives of the *Privacy Act* include both consequentialist and rights-based considerations.[38]

The main features of consumer IoT devices that challenge data privacy laws are as follows:[39]

- *Mass, undifferentiated data collection.* IoT devices are characterised by a variety of sensor technologies, including video cameras, microphones and infrared detectors. These devices may

[35] Consumers International, The Internet of Things and challenges for consumer protection (Consumers International, London, 2016) pp. 37-39.
[36] Guido Noto La Diega & Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 7(2) European Journal of Law and Technology 1, 13-14.
[37] 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 (New South Publishing, Sydney, 2020).
[38] Privacy Act 1988 (Cth), s. 2A.
[39] See generally: Internet Society, Internet Society Policy Brief: IoT Privacy for Policymakers (September 2019); Gilad Rosner & Erin Kenneally, Clearly Opaque: Privacy Risks of the Internet of Things (May 2018).

be 'always on', resulting in continuous sensing, watching or listening to activities in the home. Even if the devices are not 'always on', however, and the sensors need to be activated, they can result in dragnet collection of data that can be linked to individuals.[40] Once linked to an individual, this data can reveal a considerable amount about a person and can, for example, be used to build a profile.

- *Data matching to draw inferences.* Data collected from IoT devices may be combined with other data, including data from other IoT sensors, in a process known as 'sensor fusion',[41] to draw highly revelatory inferences about individuals and their behaviour. As Richardson et al point out, '… the 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…'.[42] In general, the fusion of data across devices is poorly disclosed by IoT businesses, and poorly understood by consumers.[43]
- *Blurring of boundaries.* Traditionally the home has been regarded as a 'private sphere', immune from monitoring and surveillance. By facilitating ubiquitous data collection and monitoring, however, consumer IoT 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.[44]
- *Opaque data collection.* Many IoT devices, which can have 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 is 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.
- *Difficulties in getting informed consent.* Following from the extent to which IoT devices may collect data about a person without that person knowing, it is difficult or impossible to get consent of people, such as household members and visitors to a home, for the collection of data.

[40] Scott R. Peppet, 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85.
[41] Scott R. Peppet, 'Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85.
[42] Megan Richardson, Damian Clifford, Karin Clark & Rachelle Bosua, '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.
[43] Gilad Rosner & Erin Kenneally, Clearly Opaque: Privacy Risks of the Internet of Things (May 2018), p. 42.
[44] Helen Nissenbaum, Privacy in Context (Stanford University Press, 2009).

- *Increased possibility of consumer manipulation.* By extending online models of the collection and use of data into the offline world, the IoT 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".[45]
- *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,[46] 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.

[45] Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books Ltd, London, 2019) p. 293.

[46] 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

A. Ring Doorbell

B. Roomba

C. Google Nest

D. Vtech Smartwatch

E. August Smartlock

F. Tapo Smartbulb

A. Ring Doorbell Case Study

Product Overview

Ring is a 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").

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, and
- Other terms and conditions as may be posted on the Ring website.[47]

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.

Contract Formation

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.[48] 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 at the installation time (although purchasers must then have the right to return the product for

[47] 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.'

[48] 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. *'

'change of mind'). However, it seems impractical to suggest that users are aware of the Terms of Service before purchase and that purchase of Products or Services constitutes agreement to the Terms of Service.

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 raises questions as to the certainty of 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.com website or some other means, rather than by a direct communication to the user.

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 any recourse.

Data Storage and Use

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.[49] 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.[50] Ring encrypts communication between Ring devices and cloud storage (AWS) (both in transit and at rest). According to the Ring website, '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

[49] Ring, 'End-to-End Encryption White Paper' (January 2021) 3, footnote 2 <https://assets.ctfassets.net/a3peezndovsu/7bwgu7ybi1XoyH61pDraYT/94e4bab9347d4abe07f8d843fdfd4bd4/Ring_Encryption_Whitepaper_FINAL.pdf>.

[50] Ring, 'End-to-End Encryption White Paper' (January 2021).

between Ring devices using AES encryption, TLS and SRTP (Secure Real Time Protocol).'[51] From January 2021, end-to-end encryption is 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.[52] 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.

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.

Consumer Protection Issues

Application of Australian Consumer Law

The 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, 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 Australian Consumer Law.

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 'convenient and peace of mind are always at your fingertips whether you're home or away.'

[51] Ring, 'Your Privacy with Ring' (Web Page) <https://support.ring.com/hc/en-us/articles/360043469371-Your-Privacy-with-Ring>.
[52] Ring, 'End-to-End Encryption White Paper' (January 2021).

B. Roomba Case Study

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.

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[53] (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 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 local IXL Terms and Conditions of Purchase and IXL Privacy Policy. However, the mobile application that controls Roomba products is provided by iRobot and is governed by iRobot Terms of Service, iRobot End User Licensing Agreement (EULA) and the iRobot Privacy Policy 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 United States or the laws of Massachusetts whereas the IXL Home terms and conditions refers to the laws of Victoria Australia.

[53] https://www.shopirobot.com.au/terms-and-conditions/

Contract Formation

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.[54] 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.'[55] It may be possible to insist that users not use the mobile application if they do not agree to the iRobot Terms of Service where the terms are made available prior to purchase or installation however it seems impractical to suggest that users may not browse the Services (including the website global.irobot.com) or that users are deemed to have accepted the Terms of Service upon browsing or accessing the website. Browsing the website is necessary to even locate the terms and conditions in some cases. 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.

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 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. The iRobot Terms of Service provide a URL that will contain the current version of the Terms of Service however the URL directs the user to a blank page. The iRobot Privacy Policy states that the policy may be updated from time to time and the website will be amended to reflect the new version date. 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.

[54] Service are defined as the Site (global.irobot.com), the Web App and Mobile Apps.

[55] iRobot Terms of Service, 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

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 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 defense-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'.[56] 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 states that while the companies will take steps to secure personal information, security systems may not be entirely secure and that there are no guarantees as to the security of systems.

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 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 whereas the iRobot EULA states that the user should not connect their product to the internet.

Furthermore, the iRobot Terms of Service advises 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.'

[56] https://webapi.irobot.com/Legal/Documents/Asia-Pacific/Australia/Legal-Documents/Data-Security.aspx?sc_lang=eu-GB

C. Google Nest Case Study

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. The case study was prepared based on purchase of a Google Nest Hub 2nd generation.

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 and the only document that establishes any order of precedence is the Google Nest Terms of Service. The status of information published on webpages, including the ability of Google to change or update this information, is unclear even where the information is cross referenced in legal terms and conditions.

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.' Users are advised to remove their content and stop using the services in the event that they don't 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 Google '[w]ill not reduce your rights under this Privacy Policy without your explicit consent.'

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. 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 to turn the microphone off.

The Google Nest Terms of Service provide 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. "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."

Data Security

The Google Safety Center provides a wealth of publicly available information on security and privacy of Google products.[57] Users are advised that Google uses 'multiple lawyers 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 with 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 Centre, Google commits to release security updates for a minimum of 5 years from the first date of sale on the Google Store.[58] Furthermore, Google has products externally reviewed and validated by external third parties. 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 has been published online.[59]

Google provides monetary rewards and public recognition for security researchers who identify security vulnerabilities as part of its Google Vulnerability Reward Programme.[60]

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, responding to legal requirements or addressing security and operability issues.' The Terms of Service

[57] See https://safety.google/security-privacy/; https://safety.google/security/built-in-protection/ https://safety.google/authentication/
[58] https://support.google.com/product-documentation/answer/10231940#
[59] https://support.google.com/product-documentation/answer/10231940#
[60] bughunters.google.com

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 changed without notice or recourse.

D. Vtech Smartwatch Case Study

Product Overview

The VTech Smart Watch DX device is marketed towards 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 in 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 download of software from the Learning Lodge App is not necessary for the watch to function, certain features advertised on the device packaging are dependent on download of the software.

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. Australia users of Learning Lodge software are bound by two Australian Agreements: the VTech Australia Consolidated Terms and Conditions regarding the Learning Lodge for Installation and Use ("Vtech Australia Learning Lodge Terms") and the VTech Australia Privacy Policy. 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").[61]

Contract Formation

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. 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 European Agreements. There is no explicit reference to the contracts from

[61] On 31 March 2020, a customer service representative of Vtech Australia confirmed in response to an email enquiry that Australian products that use the Learning Lodge application are subject to European terms and conditions.

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' is defined as the VTech Australia Learning Lodge Terms and no reference is made to the European Agreements that consumers 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.

Forum and choice of law

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

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'.

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 some 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 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'.

Software Updates

The Vtech Australia Learning Lodge Terms provides 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 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 states that updates may be provided and users shall follow instructions and download updates, disclaiming liability for loss or damage resulting from failure to follow instructions.

Consumer Protection Issues

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 webpage entitled Consumer Guarantees that provides summarised information about those guarantees. An Australian warranty is provided in the Device packaging. However, the Consumer Guarantees webpage states that warranties are limited to goods sold by authorised retailers (eBay is excluded) and warranties cannot be transferred. A consumer may infer from this that consumer guarantees do not apply to these types of purchases.

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

E. August Smart Lock Pro Case Study

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.com.au from US-based sellers, pursuant to the Amazon Global Store Conditions of Sale that apply to US Imports. The August Terms of Service provides that the August Services include the August website, the App, all related software provided by August, together with services provided via the site.

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. The August End User Agreement explicitly incorporates the hyperlinked August Privacy Policy 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 entitled Cookie Policy, Warranty, AVR 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 United States and Canada. 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 create onerous obligations on users.

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 United States or Canada can return the hardware for a refund if they are unhappy with end user licence 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 terms of the end user licence agreement.

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 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.

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/EEA 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 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 United States 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 ("Invitees"). This can be highly sensitive data to the individual. Users who choose the Auto-Unlock function will 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.'

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 and be provided with limited services.

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) provides that its terms are not intended to exclude, restrict or modify Australian Consumer Law yet determining how 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 guarantees of fitness for purpose or acceptable quality. The Amazon GSCS provides that the purchaser of goods from the Global Store is the importer. There is no place of business for the manufacturer of the August Smart Lock Pro in Australia.

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, 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 purpose where limitations on warranties are permitted.

Security

August encourages the disclosure of vulnerabilities, particularly by security researchers and 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'. It discourages 'premature' disclosure of vulnerabilities.[62]

[62] August, 'Security Center' https://august.com/pages/security-center

F. Tapo Smart Light Bulb Case Study

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 certain times for lights to be on. It is possible to control the device using the Tapo app or in conjunction with Google Assistant and Alexa. The device is sold in mainstream Australian retailers. Smart Light Bulbs are frequently identified as an example of home internet of things 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.

The Nest of Agreements

The Tapo User Agreement and Tapo Privacy Policy are available on the Australian web page. Users accept both agreements so that they can use the Tapo app, entering into agreement 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, mobile app software and subscription services that can be accessed using the Web Apps and Mobile Apps.

Contract Formation

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

Data Storage and Use

There is no reference to Australian legal standards 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. 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 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.

Software Updates

Any use of the provided 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 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 remedy for consumer not agreeing to automatic software updates is to terminate the account and stop using the software and products.

Consumer Protection Issues

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 Australian Consumer Law. The separate Tapo Terms of Use provides 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.'

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 become inoperable. The Tapo Terms of Use provide that termination of Tapo Service 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.'

Security

The user is responsible for the security of any username and password and 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.

3. Legal Challenges arising in relation to consumer IoT devices

Part I: Data security and consumer IoT devices

Part II: Consumer protection and consumer IoT devices

Part III: Privacy law and consumer IoT devices

Part I: Data security and consumer IoT devices

Introduction

This part of the draft report has two sections: the first focuses on the role of regulation in promoting the security of consumer IoT devices, while the second section addresses the potential for labelling schemes to improve device security.

The first part briefly sets out the current state of play in regulating the security of consumer IoT devices, focusing on policy developments in Australia and the UK. After that, it makes recommendations for improving the regulation of the security of consumer IoT devices and explains the reasons for the recommendations. In summary, the report recommends introducing legislation to mandate security standards for consumer IoT devices.

The second part introduces IoT security labelling schemes, focusing on schemes that have been developed in Singapore and Finland. Following that, this part 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, with provision for monitoring and auditing IoT devices and sanctions for non-compliance.

Regulation of IoT data security

Given the importance of securing IoT devices, the first steps in IoT-specific regulation have, unsurprisingly, been aimed at enhancing security. To date, outside of standard-setting activities by the International Organization for Standardization (ISO),[63] which have a technical focus, there have been few international initiatives. In July 2019, however, the "Five Eyes" countries – Australia, Canada, New Zealand, the UK and the U.S. – issued a joint communique, which affirmed an intention to promote 'security by design' in IoT devices by the respective governments collaborating with industry and standards bodies.[64]

[63] See, for example, ISO/IEC 30141: 2018 (en), Internet of Things (IoT) – Reference Architecture, https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en (last visited on 13 April 2020);

[64] FIVE COUNTRY MINISTERIAL COMMUNIQUÉS, Statement of Intent regarding the security of the Internet of Things, 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 (last visited on 13 April 2020).

The approach taken to governance or regulation of the security of IoT devices in Australia has been influenced by developments in the UK. After a policy development process, which included input from the National Cyber Security Centre (NCSC), the UK introduced a voluntary code of practice for consumer IoT security in October 2018.[65] The UK Code incorporated 13 security principles, which were arranged in order of importance.

The UK government published a table mapping the Code's guidelines against other national and international guidance and regulations relating to IoT security.[66] The table indicated considerable international alignment of the basic security principles, but with some differences in implementation or recommended implementation. In October 2021, this project was re-oriented to map global IoT security and privacy standards to the ETSI standard for the *Cyber Security for Consumer Internet of Things: Baseline Requirements* (EN 303 645), which arguably has become a de facto global standard.[67]

Following a further review of the IoT 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.[68] In November 2021, the government introduced a Bill to implement the April 2021 decision, which this report analyses following an explanation of the Australian policy developments. The Bill mandates compliance with the top three guidelines from the UK Code of practice, which require: (1) IoT device passwords to be unique; (2) manufacturers to provide a public point of contact as part of a vulnerability disclosures policy; and (3) software components in IoT devices to be securely updateable.

Regulation of IoT data security in Australia

The Australian response to securing IoT 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.[69] In December 2019 the Australian Government initiated a consultation on a voluntary draft Code of Practice for consumer IoT devices.[70] Following the

[65] Department for Digital, Culture, Media & Sport (2018), Code of Practice for Consumer IoT Security, <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security> accessed 9 September 2020.
[66] <https://iotsecuritymapping.uk/>
[67] <https://iotsecuritymapping.com/>
[68] Department for Digital, Culture, Media & Sport, 'Government response to the call for views on consumer connected product cyber security legislation', 21 April 2021, *Government response to the call for views on consumer connected product cyber security legislation - GOV.UK (www.gov.uk)*, accessed 21 May 2021.
[69] Australian Government, Australia's Cyber Security Strategy, Canberra, 2016; Australian Government, Australia's Cyber Security Strategy 2020, Canberra, 2020.
[70] Department of Home Affairs, Australian Signals Directorate & ACSC, Securing the Internet of Things for Consumers: Draft Code of Practice, 2019.

consultation, the government released the final version of the Code of Practice, without change to the principles, in September 2020.[71] The Australian code essentially adopted the 13 principles from the UK *Code of Practice,* but restated them, with the consultation document indicating that it 'builds upon' the UK guidelines.[72]

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
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 prepared by the Department of Home Affairs.[73] The discussion paper included options for setting cyber security expectations, increasing transparency and protecting consumer rights, including for smart IoT devices. The paper 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.

[71] Department of Home Affairs, Australian Signals Directorate & ACSC, Code of Practice: Securing the Internet of Things for Consumers, 2020.
[72] Ibid., p. 2.
[73] Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021.

- Products sold at the lower end of the market can have less reputation to protect and thus less incentive for high cyber security.[74]

Following from this research, the discussion paper 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.[75] In relation to the possible mandatory standard, the discussion paper 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 discussion paper 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.[76]

The discussion paper also canvassed options for introducing labelling for smart devices, identifying the following three options:[77]

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

The relative merits of these options are evaluated below in the section of this report dealing with our recommendations relating to product labelling.

Regulation of IoT data security in the UK

This section of the report explains policy developments in the UK, which have resulted in legislation mandating minimum security standards for connected consumer IoT devices.

In May 2019, the UK government initiated a public consultation on regulatory options for making aspects of the UK voluntary code legally enforceable.[78] The consultation indicated that the increase in threats associated with the growth of consumer IoT resulted in an 'urgent need' for security

[74] Ibid. p. 31.
[75] Ibid. pp. 32-3.
[76] Ibid. pp. 33-4.
[77] Ibid. pp. 37-41.
[78] Department for Digital, Culture, Media & Sport, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, 1 May 2019.

safeguards set out in the voluntary Code to be mandated.[79] However, on the basis that implementing the 13 guidelines in the UK Code in full would dampen innovation, the 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.[80] 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.[81]

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 Product Security and Telecommunications Infrastructure Bill 2021 (UK) (the 'PS&TI Bill) was introduced to the House of Commons. The Bill which, in accordance with the April 2021 announcement, introduces mandatory security standards for 'connected devices', is explained and analysed immediately below.

Product Security and Telecommunications Infrastructure Bill 2021 (UK)

Part I of the Product Security and Telecommunications Infrastructure Bill 2021 (UK) (the 'PS&TI Bill') establishes a regulatory framework for the security of connected devices.[82] More specifically, it establishes an enforceable regulatory regime imposing minimum security obligations on 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 regulations.

[79] Ibid. 14.
[80] Ibid. 7, 11.
[81] Department for Digital, Culture, Media & Sport, 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.
[82] Part II of the Bill is intended to support the Electronic Communications Code by introducing measures to enhance the development of digital telecommunications infrastructure.

Clause 1 of the Bill provides the Secretary of State 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; and
- **Security Requirement 3:** Provide transparency about the length of time for which a product will receive security updates.[83]

The security requirements must relate to consumer 'connectable products' of manufacturers, importers or distributors. Under clause 4 of the 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'.[84] 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.[85] The Secretary of State, however, has the ability to designate excepted products, which will include products that might otherwise be subject to double regulation, such as smart metering devices, medical devices and road vehicles.[86]

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

[83] Product Security and Telecommunications Infrastructure Bill, Explanatory Notes, Bill 199-EN, para [19].
[84] Product Security and Telecommunications Infrastructure Bill, cl 5.
[85] Department for Digital, Culture, Media & Sport, The Product Security and Telecommunications Infrastructure (PTSI) Bill – product security factsheet, *The Product Security and Telecommunications Infrastructure (PSTI) Bill - factsheets - GOV.UK (www.gov.uk)*.
[86] Product Security and Telecommunications Infrastructure Bill, Explanatory Notes, Bill 199-EN, para [51].

- the product is or has been made available in the UK to customers who are not consumers where identical products are or have been made available to consumers in the UK.

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 the following table.

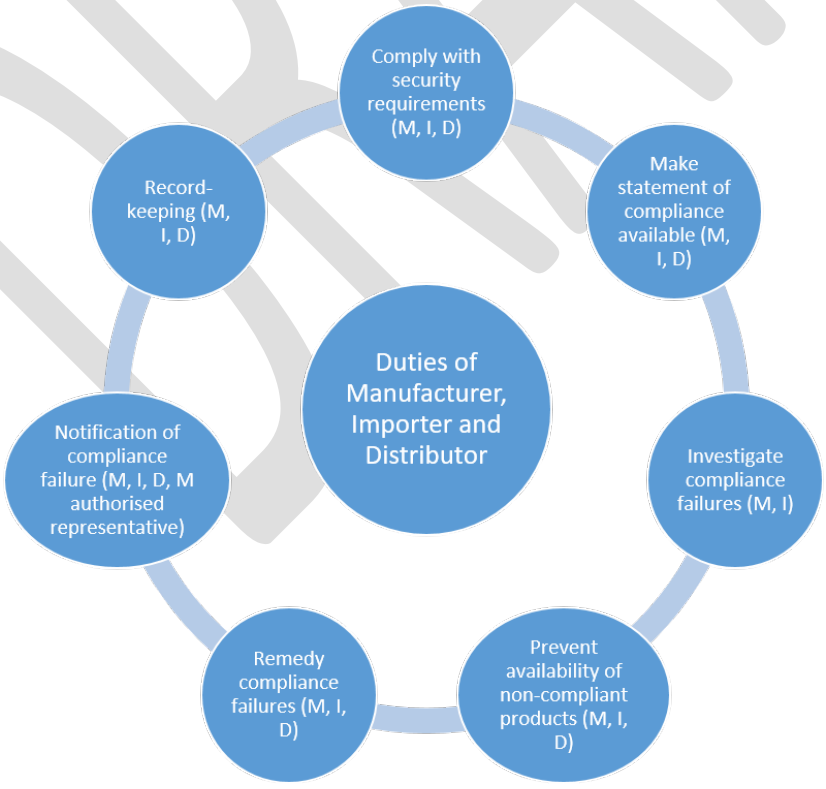

Figure 1: Duties of Manufacturers, Importers and Distributors under Product Security and Telecommunications Infrastructure Bill 2021 (UK)

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: • 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
	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 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 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
	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

The 'enforcement authority' responsible for enforcing Part I of the PS&TI Bill is the Secretary of State for the Department of Digital, Culture, Media and Sport, or a delegate of the Secretary of State. The Bill provides that the enforcement authority has the powers of investigation set out in Schedule 5 of the *Consumer Rights Act 2015* (UK).

Part I of the PS&TI Bill establishes a tiered enforcement regime which provides for the enforcement authority to issue the following enforcement notices to relevant persons (namely, manufacturers, importers or distributors):

- **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, the Secretary of State may, on the satisfaction of certain conditions, apply to the court for an order for the forfeiture of products.

Recommendations

Recommendation 1

General cyber security legislation should be introduced, following a public consultation process, to enhance cyber security standards across business sectors. General cyber security legislation could establish the framework for regulatory measures in particular industry sectors, such as mandating standards or the development of codes of practice, or mandating labelling schemes.

Recommendation 2

In the absence of general cyber security regulation (as described in Recommendation 1) legislation should be introduced to regulate the security of consumer IoT devices. The legislation should impose mandatory minimum obligations on relevant entities, such as manufacturers, importers and distributors of IoT consumer devices. The minimum obligations should require compliance with security principles set out in the Australian code and/or designated technical standards.

This report recommends that Australia develop, in consultation with stakeholders, a comprehensive and holistic cyber security regime which incorporates a set of general principles aimed at improving cyber security across industry sectors. While enhancing the security of consumer IoT devices is a priority, this cannot be achieved in isolation from the broader cyber security environment and, consequently, a holistic approach is called for. Moreover, there are some commonalities to the challenges faced across industry sectors, such as the vulnerability of devices to ransomware attacks and other cyber breaches, which have become increasingly prevalent.

We therefore support the introduction of general cyber security legislation aimed at enhancing security across all industry sectors. This would be broader than the approach taken by the UK PS&TI

Bill, in that it could extend, for example, to IoT in sectors such as energy, finance, building, education and agriculture. Acknowledging the different considerations that apply to different industry sectors, the legislation would establish a general framework, which could then be adapted to particular industry sectors through flexible instruments, such as industry codes of practice.

In the absence of omnibus cyber security legislation, we support the introduction of legislation similar to the UK PS&TI Bill which would provide for mandatory, minimum standards for consumer IoT devices. Such legislation should, at a minimum, establish a framework for mandating compliance with minimum security standards but, as explained below, we also consider there is a case for introducing a mandatory labelling scheme. The reasons for supporting a mandatory labelling scheme are explained later in this section of the report, while the reasons for supporting mandatory standards are explained immediately below.

As the discussion paper on strengthening Australia's cyber security released by the Department of Home Affairs in July 2021 reported, government research conducted after the release of the voluntary Code of Practice has indicated that it is not working effectively to ensure the security of consumer IoT devices.[87] The reason for this is that, unaided, markets fail to provide sufficient incentives for suppliers to adequately secure IoT 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.[88] Secondly, decisions by business not to invest in security may result in costs that are borne not by itself but by others, resulting in a negative externality.[89] 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 against legislatively mandating minimum security standards are that IoT technologies are moving too rapidly for regulation to catch up and, in any case, the diversity of IoT devices means that a 'one size fits all' standard would be unlikely to be successful.[90] 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

[87] Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021, Annex A.

[88] 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.

[89] Ross Anderson and Tyler Moore, 'The Economics of Information Security' (2006) 314 Science 610; Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021, p. 10.

[90] IoTAA, Submission to Department of Home Affairs consultation on "Securing the Internet of Things for Consumers" Draft Code of Practice, 1 March 2020; IoTAA, Response to Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper, 26 August 2021.

information about the technology, but once a technology has achieved mass penetration it is difficult or impossible to effectively control.[91] 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.[92] Accordingly, the first objection is more about how to regulate than it is about whether or not there is a case to regulate. The UK PS&TI Bill addresses this issue by confining itself to framing legislation with details, including minimum standards, spelt out in regulations. A similar, flexible approach could be taken in Australia.

The second objection should also be seen as raising questions 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 apply to a diverse range of consumer IoT devices; and technical standards, such as EN 303 645, while more detailed, 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 be supplemented by guidelines explaining how the rules apply in particular circumstances. Moreover, as is the case under the *Privacy Act 1988* (Cth), provision could be made for the development of codes of practice for industry sectors, which would allow for general standards to be customised to particular circumstances. As this circumstance reminds us, the data security principle in APP 11 (and analogous data privacy laws) applies to a much greater variety of circumstances than security standards applying to consumer IoT devices, but we are not aware of any credible arguments for removing this principle.

Should Australia adopt ETSI EN 303 645?

As explained above, in the Department of Home Affairs' discussion paper on strengthening Australia's cyber security, the option of introducing a mandatory security standard for smart devices was canvassed, with the paper proposing that Australia consider adopting ETSI EN 303 645.[93] The discussion paper suggested that adopting the ETSI standard would ensure international consistency and encourage best practice. Moreover, the discussion paper 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. While the ETSI standard has

[91] David Collingridge, The Social Control of Technology (1980, Pinter, London).

[92] Ryan Hagemann, Jennifer Huddlestone Skees & 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, December 2020.

[93] Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021, p. 32.

strengths, however, there would be disadvantages in adopting the standard wholesale, which we suggest weigh against following this path in Australia.

The ETSI standard is more detailed that either the UK or Australian Codes of Practice; and it has achieved a degree of international recognition.[94] Nevertheless, ETSI is a Europe-based organisation, which was originally established in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT), following a proposal from the European Commission.[95] Furthermore, as one of the three European Standards Organisations (ESOs), ETSI has a special role in Europe, supporting European legislation and regulations.[96] 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, seems to assume the existence of the GDPR. Therefore, the ETSI standard does not need to emphasise privacy protection as much as an Australian instrument, as the GDPR already affords much stronger and more widely applicable privacy protection than is available in Australia.

In addition, the ETSI standard has not been universally adopted. For example, the U.S. *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.'[97] The *Security of Connected Devices* legislation in California requires manufacturers of connected devices, such as consumer IoT devices, to equip devices 'with a reasonable security feature or features.'[98] Similarly, the Oregon House Bill 2395 requires that manufacturers implement 'reasonable security features'.[99] 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).[100] 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

[94] See: Copper Horse Ltd, Mapping Security & Privacy in the Internet of Things, <https://iotsecuritymapping.com/>.
[95] https://www.etsi.org/about/about-us.
[96] https://www.etsi.org/about/about-us.
[97] H.R. 1668 – 116th Congress Public Law No. 116-207 Internet of Things Cybersecurity Improvement Act of 2020, Sec 4(a)(1). <https://www.congress.gov/bill/116th-congress/house-bill/1668>.
[98] California Civil Code, Title 1.81.26 Security of Connected Devices, 1798.91.04(a).
[99] Oregon House Bill (HB) 2395 Relating to security measures required for devices that connect to the Internet; creating new provisions; and amending ORS 646.607 Section 1(2).
[100] California Department of Justice, California Data Breach Report 2012-2015 (2016) v, 30-31; See, e.g., Center for Internet Security, CIS Controls v 7.1 (2019).

of the U.S. market, and the fact that many consumer IoT devices are developed by U.S. companies, the NIST standards may well become significant across the industry as a whole.[101]

At this stage, it is unclear whether the ETSI standard will become globally influential or widely adopted to the extent that Australia obtains a meaningful advantage by adopting it, rather than alternatives. For example, according to the UK's mapping of cyber security standards globally, there are more than 100 global standards, and among them there are many candidates for a standard that might be adopted.[102] NIST standards on IoT cyber security are highly referenced, as are standards from NGOs, such as GSMA, IETF and IEEE.[103] A decision to adopt a standard ought, therefore, at least consider other promising candidates and, given the disconnect between the Australian and European regulatory contexts, assess their suitability for Australia.

We therefore recommend that Australia should draw lessons from the ETSI standard, as well as other globally applicable standards, but should refrain from mandating any particular technical standard. Instead, in implementing mandatory standards, we recommend focussing attention on making improvements to the current Australian Code of Practice.[104]

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 Security Pledge and Google has published the full report online.[105]

The ioXt Security Pledge has eight principles[106]:

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

[101] Draft NIST SP 800/213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (December 2020) <https://doi.org/10.6028/NIST.SP.800-213-draft>; NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline (May 2020) <https://doi.org/10.6028/NIST.IR.8259A>; Draft NISTIR 8259B IoT Non-Technical Supporting Capability Core Baseline (December 2020) <https://doi.org/10.6028/NIST.IR.8259B-draft>; Draft NISTIR 8259C Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline (December 2020) <https://doi.org/10.6028/NIST.IR.8259C-draft>, Draft NISTIR 8259D Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government (December 2020) <https://doi.org/10.6028/NIST.IR.8259D-draft>.

[102] https://iotsecuritymapping.com/.

[103] Copper Horse Ltd, Mapping Security & Privacy in the Internet of Things, <https://iotsecuritymapping.com/>.

[104] See Evana Wright, David Lindsay, Genevieve Wilkinson, Henry Fraser and Neva Collings, Submission to Strengthening Australia's cyber security regulations and incentives (2021) < https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/wright-lindsay-wilkinson-fraser-and-collings.pdf>

[105] *Google, Security updates and third-party assessments for Google Nest devices* https://support.google.com/product-documentation/answer/10231940#

[106] ioXt: internet of secure things, *ioXt Security Pledge* https://www.ioxtalliance.org/the-pledge

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.

Security labelling schemes

This section of the report addresses issues relating to the potential for security labelling schemes to enhance the security of consumer IoT devices.

As this report has explained, a major reason for insecure consumer IoT 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 indicated complacency on the part of consumers to seek out such security and privacy information.[107] This complacency points to the need for regulators to introduce measures that facilitate informed decision making amongst 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.[108] One mechanism proposed for addressing this information deficit is to establish a security labelling scheme. The July 2021 discussion paper on strengthening cyber security released by the Department of Home Affairs

[107] Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings, 3.

[108] 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) Information, Communication & Society 1-20. 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 (August 2021) 6 <https://accan.org.au/files/Grants/2021%20Deakin%20IoT/Deakin%20grants%20report_v5_web.pdf>.

suggested that, based on evidence that consumers think cyber security is an important purchasing consideration, 'a cyber security[109]

As explained above, the Home Affairs discussion paper canvassed proposals for introducing labelling for smart devices and, in doing so, identified the following three options:[110]

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

This section of the report analyses the merits of these options (in explaining our recommendations), following an explanation of existing government-led labelling schemes in Singapore and Finland. To date, Singapore and Finland are the only two countries to have introduced consumer IoT security labelling schemes.

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.[111] 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'.[112] It offers and supports the use of the CLS to provide assurance to customers that IoT products have been objectively assessed for cybersecurity by adopting a 'security by-design approach'.[113]

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.[114] Relatedly, it is intended to incentivise manufacturers to develop more secure products and, by doing so, differentiate their

[109] Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021, p. 36.
[110] Ibid. pp. 37-41.
[111] Cybersecurity Labelling Scheme (CLS), https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls.
[112] See: https://www.csa.gov.sg/Who-We-Are/Our-Organisation.
[113] Cyber Security Agency (Singapore), Cybersecurity Certification Guide (2021), p. 1.
[114] Ibid. p. 5.

products from those of competitors.[115] 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 consumer IoT devices, including IP cameras, smart door locks, smart lights and smart printers.[116]

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:[117]

- **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

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.

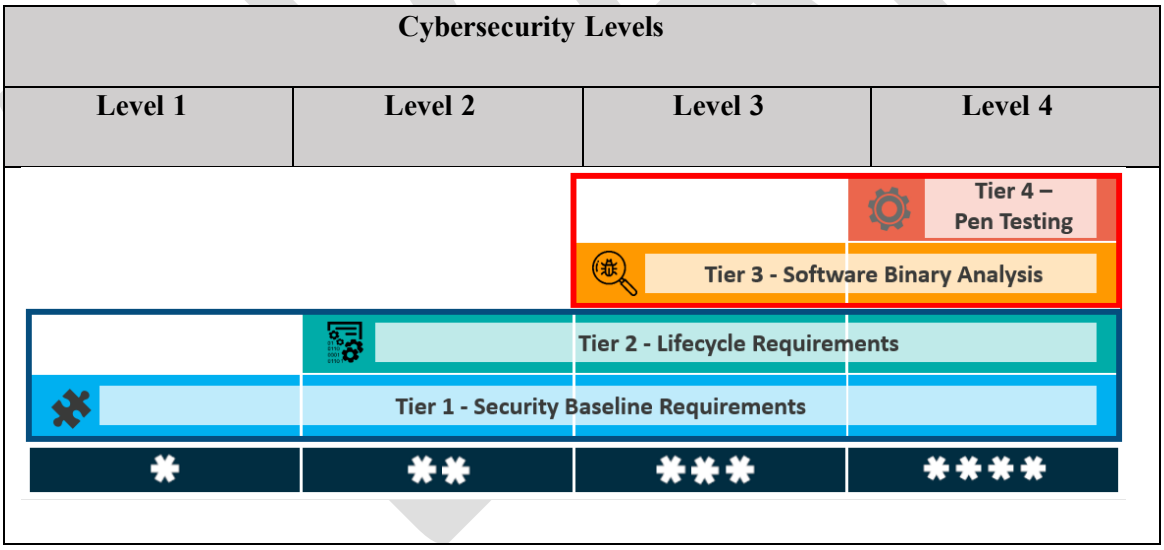

Figure 2: Singapore Cybersecurity Labelling Scheme Tiers

[115] Cybersecurity Labelling Scheme (CLS), https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls.

[116] Ibid.

[117] Cyber Security Agency (Singapore), Cybersecurity Certification Guide (2021), p. 7.

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 IoT 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. Compliance with these requirements, however, depends upon the checklist submitted by the developer, and no independent testing is required for this assessment tier.

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).[118] The Security Guide incorporates the following four IoT security design principles: 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.

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 an IoT 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.

[118] Info-Communications Media Development Authority, Internet of Things (IoT) Cyber Security Guide, v. 1, March 2020.

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*.[119] 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. To date only one product has been assessed for this level under the CLS.

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 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

[119] Cyber Security Agency (CSA) of Singapore, Cybersecurity Labelling Scheme (CLS): Minimum Test Specifications and Methodology for Tier 4, v. 1.1, April 2021.

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.

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.[120] The Traficom terms and conditions stipulate how the CL can be used, including duration, visibility and monitoring.[121]

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.

[120] Statement of Compliance, Traficom. <https://tietoturvamerkki.fi/files/statement-of-compliance-for-the-cybersecurity-label.pdf>
[121] Traficom, Terms of Use – Cybersecurity label for IoT consumer devices, 11 November 2019, https://tietoturvamerkki.fi/files/iot-ttm-tems-of-use.pdf.

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.[122] The application process takes between 5 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.[123] Once approved the label is valid for three years and fee of 350 Euros is payable with a further annual fee of 350 Euros for each annual review.[124]

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 and services and used in marketing and communication channels.[125] Approved devices are published on the Traficom website, which includes the product's *Statement of Compliance.* To date, nine products have been listed, including a contact tracing app, home hubs, intelligent lighting, fitness watches, and a smart heating adjuster.[126] The use of the label is monitored primarily by means of spot checks and feedback.[127] Labelled products or services are reviewed annually to take into account possible changes on information security that may have arisen thereby ensure continuous security.[128]

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

[122] Inspection, <*https://tietoturvamerkki.fi/en/inspection/*>.
[123] Applying for the Label, <*https://tietoturvamerkki.fi/en/apply-for-the-label/*>
[124] Cybersecurity Label: Help your customers make secure choices, <*https://tietoturvamerkki.fi/files/cybersecurity-label-infopack-for-companies.pdf*>
[125] Traficom, The Finnish Cybersecurity Label, <*https://tietoturvamerkki.fi/files/cybersecurity_label_presentation-280920.pdf*>
[126] Products, <*https://tietoturvamerkki.fi/en/products/*>.
[127] Traficom, Terms of Use – Cybersecurity label for IoT consumer devices, 11 November 2019, https://tietoturvamerkki.fi/files/iot-ttm-tems-of-use.pdf.
[128] Inspection, <*https://tietoturvamerkki.fi/en/inspection/*>.

agree on a schedule for corrective action, with problems expected to be rectified within a maximum of 90 days.

Singapore-Finland MoU

A Memorandum of Understanding (MoU) has been signed between Singapore and Finland that mutually recognises the respective cybersecurity labels for consumer IoT products issued in each country. [129] The MoU is the first bilateral agreement whereby products under either scheme can meet the requirements of both the Finnish CL and Singapore's CLS with a single application process.[130] 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.'[131] The uniform requirements facilitated by the MoU is intended to allow products or services to be placed on the market in both countries that meet the security criteria of both labels.

Recommendations

Recommendation 3

A mandatory labelling scheme should be introduced as part of an IoT security regulatory regime. Any mandatory labelling scheme must be properly resourced to ensure satisfactory testing, certification and enforcement. As part of the regime, a government entity should be responsible for evaluating products according to criteria that assist consumers with exercising informed choices concerning security risks.

Recommendation 4

In the absence of a mandatory labelling scheme, a voluntary scheme with government backing, such as Singapore's CLS, should be introduced and properly resourced. This should incorporate an obligation on relevant persons to include a Statement of Compliance and an authoritative list of labelled products.

To date, no jurisdiction has introduced a mandatory labelling scheme for the security of consumer IoT devices. Moreover, the July 2021 discussion paper on strengthening cyber security released by the

[129] Cybersecurity Labelling Scheme (CLS), <https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls>; David Koh, Commissioner of Cybersecurity and Chief Executive of The Cyber Security Agency of Singapore, Speech delivered to Opening of the 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>; 'Singapore and Finland sign agreement to mutually recognise IoT security labels', ScandAsia: Nordic News and Business Promotion in Asia, 9 October 2021, <https://scandasia.com/singapore-and-finland-sign-agreement-to-mutually-recognize-iot-security-labels/>

[130] Eileen Yu, 'Singapore inks pact with Finland to mutually recognise IoT security labels', ZDNet, 7 October 2021, <https://www.zdnet.com/article/singapore-inks-pact-with-finland-to-mutually-recognise-iot-security-labels/>

[131] Cybersecurity Labelling Scheme (CLS), <https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls>.

Department of Home Affairs did not expressly canvas the option of introducing a mandatory regime, confining itself to the options of introducing a voluntary star rating labelling scheme or a mandatory expiry date label.

Nevertheless, the Home Affairs discussion paper refers to evidence produced by the UK Department for Digital, Culture, Media & Sport in a 2019 analysis of policy options for enhancing the security of consumer IoT products, which supported mandatory labelling.[132] The UK impact assessment suggested that, over a 10 year period, 15% 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%. As this section of the report explains, it seems likely that even if a voluntary scheme were to be introduced, it will need to eventually be mandated in order to ensure its effectiveness. Furthermore, in the absence of comprehensive cyber security regulation, consumer labelling should be introduced in conjunction with minimum security standards for consumer IoT devices. Both consumer labelling and security standards are required to address the information asymmetries and market failure discussed above. As observed by Warren, Mann and Harkin in their 2021 report on 'Enhancing Consumer Awareness of Privacy and the Internet of Things', "[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."[133] It is likely that this holds true for both privacy and security concerns.

The Home Affairs discussion paper 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.[134] 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 to become competitive.[135] The difficulty with this argument mirrors the difficulties 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 label their products. And this would be the case largely regardless of the level of uptake of a voluntary scheme. That said, the discussion paper does implicitly raise the most important objections to a mandatory regime.

[132] UK Department for Digital, Culture, Media and Sport 2019, Mandating security requirements for consumer 'IoT' products: Consultation stage impact assessment, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf.

[133] Ian Warren, Monique Mann and Diarmaid Harkin, Enhancing Consumer Awareness of Privacy and the Internet of Things (August 2021) 4 <https://accan.org.au/files/Grants/2021%20Deakin%20IoT/Deakin%20grants%20report_v5_web.pdf>.

[134] Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021, p. 38.

[135] Ibid.

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. These costs are 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 a degree of government involvement, and associated costs incurred by government. Over and above these costs, a mandatory regime would include some additional regulatory costs incurred by government. In relation to cost, 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 mandatory labelling. 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 can be minimised by leveraging existing government expertise, including expertise at the Australian Cyber Security Centre (ACSC).

While the 2019 UK policy impact statement referred to earlier favoured 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 consumer IoT devices, the UK government explained that requiring a specific label to be mandated would create supply chain management issues that could result in potential disruption to business.[136] 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 Home Affairs discussion paper 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.[137] Although the discussion paper 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.[138]

While true that IoT 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

[136] UK Government, Government response to the "Regulatory proposals for consumer Internet of Things (IoT) security" consultation, January 2020, pp. 14-15.

[137] Australian Government, Strengthening Australia's cyber security regulations and incentives, Canberra, 13 July 2021, p. 40.

[138] 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 Home Affairs discussion paper, consumers viewing a mandatory expiry label might be misled into believing that it guaranteed device security: IoTAA, Response to Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper, 26 August 2021.

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 would need to be allocated to entities responsible for placing IoT devices on the market in Australia, which might be importers or retailers. Although this would impose costs in determining the security of products, this should be regarded, in the same way as minimum health and safety standards, as a necessary cost of doing business in Australia. Furthermore, while difficulties certainly arise from the extent to which IoT devices may be directly sourced from outside of Australia, the 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 Home Affairs discussion paper, 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 consumer IoT devices.

The Home Affairs discussion paper posed the question of whether, before deciding upon a labelling scheme, it might be best to await evidence from regimes that have implemented security labelling, namely Singapore and Finland.[139] This directly raises the issue of the timing of regulatory intervention. Ideally, given the extent to which consumer IoT devices may be sourced across national boundaries, there would be a degree of cross-border consistency in 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'.[140] 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 impose costs on all jurisdictions.

In Australia, the IoTAA has been proposing a voluntary industry-led Security Trust Mark since 2017. From its submission to the Home Affairs discussion paper, it seems that the IoTAA opposes mandatory, government-imposed labelling on the basis that it may be inflexible and deter innovation. As this submission 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 may be a case for a staged implementation of device labelling, with evidence

[139] Ibid. p. 41.

[140] Cybersecurity Labelling Scheme (CLS) Publication No. 1: Overview of the Scheme, p. 2.

acquired in the initial stages of implementation being used to refine and improve the scheme. Therefore, in the absence of a mandatory regime, we support a voluntary scheme, such as that which has been implemented in Singapore or Finland. However, as indicated by the experience in Singapore and Finland, a comprehensive voluntary scheme depends upon the active involvement of government. For example, assuming that the regime includes a star rating scheme, government would have a role in certifying bodies and in enforcing compliance. To assist with enforcement, we suggest that, if a voluntary regime were to be introduced, it could effectively be supported by an obligation to provide a statement of compliance, such as that required under the UK PS&TI Bill, which would mean that a misrepresentation could amount to misleading or deceptive conduct under the Australian Consumer Law. 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 list of labelled products, with misrepresentations resulting in removal of a device from the list.

Part II: Consumer protection and consumer IoT devices

Introduction

This section of the draft report introduces recommendations relating to the reform of Australian consumer protection law aimed at improving the protection of consumers who purchase IoT devices for the home. The recommendations focus on reforms to the provisions of the Australian Consumer Law (ACL) that relate to consumer guarantees, disclosure of pre-contractual information, the regulation of unfair contracts and the product liability provisions.

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 consumer IoT devices.

The objectives of Australian consumer protection law and policy are set out in the 2009 *Intergovernmental Agreement for the Australian Consumer Law* (the 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.[141]

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

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

[141] Productivity Commission, Review of Australia's Consumer Policy Framework, Final Report, Vol. 1, Canberra, 2008, pp. 12-13.

- 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 draft 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.

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.[142]

[142] ACL, s. 3 (definition of 'consumer' (1)(b)).

Of the statutory guarantees established under the ACL, the following are the most relevant to the supply of consumer IoT 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.

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.

The 2017 ACL Review Final 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'.[143] While acknowledging that UK consumer law expressly addresses the unique characteristics of digital content - such as software, e-books and other content - the 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'.[144]

This draft report recommends changes to the consumer guarantees in order to take into account the distinctive features of consumer IoT devices and other digital products. In doing so, the report reviews

[143] ACL Review Final Report, p. 96.
[144] Ibid.

and assesses relevant recommendations relating to the consumer guarantees made by the Productivity Commission in its final report on the *Right to Repair,* which was released in October 2021.[145]

Recommendations

Recommendation 5

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

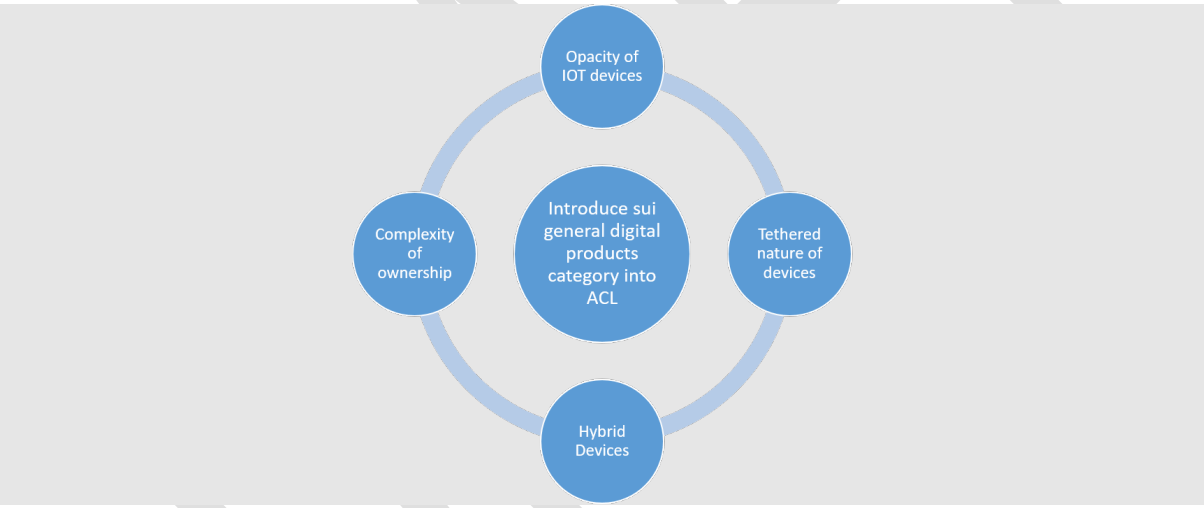

Figure 5 Elements of proposed sui generis category of digital products

As Hayward has pointed out, the historical controversy of whether software should be categorised as a good, which has largely been resolved, has been replaced by the question of how to categorise a broader category of digital products, including digital content.[146] This has been dealt with under UK and EU law by introducing a new *sui generis* category of 'digital content'. This raises the question of whether a new category of product, distinct from 'goods' and 'services', should be introduced to the ACL. This would effectively address the issue identified by the Productivity Commission in its report

[145] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021.
[146] Benjamin Hayward, 'What's In A Name? Software, Digital Products and Sale of Goods' (2016) 38 Sydney Law Review 441, 443.

on the *Right to Repair,* that 'the consumer guarantees do not explicitly specify obligations relating to software embedded in products and any associated updates',[147] but would go beyond this to address other issues arising from connected products.

CASE STUDY: Ring Doorbell

The language in the Ring Doorbell Terms of Service demonstrates the case for consumer IoT devices falling within a new *sui generis* category of digital products. The divide between goods and services is not clear cut and the supply of the goods (in this case, the doorbell) is inextricably linked with the services (the application, the web service, etc). Without use of the services, the good does not function properly. While Ring defines its software as a 'Service', it is considered a 'good' for the purpose of the Australian Consumer Law.[148] Therefore, the consumer guarantees applicable to 'goods' will apply to both the Products (as they are defined in the Ring Terms of Service) and the software, but not to 'service' elements of the product. Creating a *sui generis* category of 'digital goods' would avoid the need to distinguish between elements of a consumer IoT device that constitute a 'good' as opposed to a 'service' particularly where such an approach is artificial given the nature of the devices involved whereby the good is often inseparable from or non-functional without associated services.

There are benefits and disadvantages in introducing a new *sui generis* category for digital products. The benefits are, first, that a new category would have the potential to reduce the uncertainties in determining whether a complex product, or an element of a complex product, is a good or a service. Secondly, a new category for digital products would allow for the consumer guarantees to be tailored to account for the particular characteristics of these products and to address gaps in how the existing guarantees apply to connected digital products. The disadvantages are that, first, given the diversity of products that might be characterised as digital products, there are difficulties in satisfactorily defining a new category. Secondly, introducing a new *sui generis* category could create additional uncertainties in determining how to categorise products.

From the perspectives of both consumers and suppliers, 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, as much as possible, be tailored to the characteristics of the product. In both the UK and the EU, digital products have been considered to be sufficiently different from traditional goods and services to merit the introduction of a new category

[147] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 95.

[148] See ACL, s 2 (definition of 'goods').

of ‘digital content’. This category was, however, introduced largely to deal with products such as music, films or games that are not supplied in a tangible form; and the definitions in the UK and EU laws reflect this concern.

While there is a case for introducing a new category for digital products, given the rapid growth in IoT consumer devices, consideration should be given to developing a definition that more clearly applies to these devices than the current UK and EU definitions, as well as potentially encompassing other consumer products, such as ‘disembodied’ music, films or games. The introduction of a new category of consumer product would, of necessity, 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 example, be the case with some apps that are separately downloaded to a consumer IoT device. Although this could result in some uncertainty, whenever legislation draws boundaries between technologies or products some penumbral ambiguity can arise. This uncertainty could, however, be minimised by a combination of careful legislative drafting and guidance provided on the application of the categories to particular products.

In any case, the advantages of applying a uniform set of guarantees that are specifically tailored to digital products would seem to outweigh the demarcation problems of determining which category a product, or an element of a product, falls within; and which may arise only in a minority of borderline cases.

Recommendation 6

In association with the introduction of a new category of digital products, a set of consumer obligations should be developed that are specifically tailored to such products, including consumer IoT devices. The obligations should include requirements for: any software elements to be up to date and regularly updated; the devices to be reasonably secure; and for the elements of hybrid devices (including hardware, software and data elements) to be properly integrated.

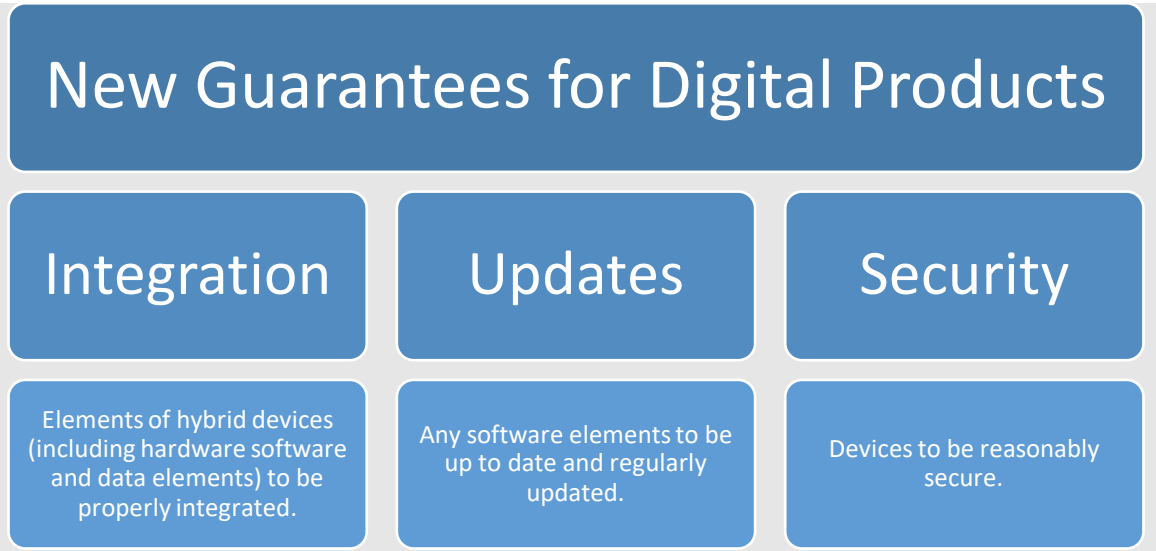

Figure 6 Elements of new guarantees for digital products: Integration, Updates and Security

Two EU Directives - the Sale of Goods Directive (SGD) and Digital Content Directive (DCD) - impose obligations on suppliers that are specifically tailored to digital products. The rationale for a uniform set of rights and obligations for digital products is set out in Recital (6) to the DCD, which states that:

> Consumers should benefit from harmonised rights for the supply of digital content and digital services that provide a high level of protection. They should have clear mandatory rights when they receive or access digital content or digital services from anywhere in the Union. Having such rights should increase their confidence in acquiring digital content or digital services. It should also contribute to reducing the detriment consumers currently suffer, since there would be a set of clear rights that will enable them to address problems they face with digital content or digital services.

While the obligations imposed by the EU directives are not necessarily exhaustive, they are illustrative of the sorts of expectations that consumers might reasonably have for hybrid connected IoT devices. 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 different elements of a hybrid device, including software and hardware, should be properly integrated.

Therefore, if a new category of digital products were to be introduced into the ACL, the specific obligations imposed in relation to digital products under the EU directives could provide the core for a set of bespoke consumer guarantees that are tailored for digital products. Moreover, introducing a

set of obligations specifically designed to apply to digital products would remove the uncertainties about how the generic obligations under the ACL apply to consumer IoT devices identified below.

A Guarantee of 'Reasonable Security'?

The fundamental purpose of the consumer guarantees law in the ACL is to ensure minimum mandatory standards of quality apply to products that are supplied to consumers. From the perspective of a consumer, a key feature of a consumer IoT device is the extent to which it is secure from potential intrusions. As it is impossible to give an absolute guarantee of device security, and as the consumer guarantees are designed to balance consumer expectations and manufacturer obligations, a bespoke provision would need to guarantee 'reasonable security'.

CASE STUDY: Ring Doorbell

Compliance with industry standards or relevant codes of practice may assist in securing consumer protections by ensuring that consumer IoT 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.[149] However, there are a number of examples where Ring services have been compromised resulting in authorised 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.[150] Hackers have also been able to intercept WiFi passwords due to insecure transmission of details during device configuration.[151] A number of these cases have proceeded to litigation in the United States of America.

The vulnerability of Ring devices in 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 is mandatory. From January 2021, end-to-end encryption is 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

[149] Ring End to End Encryption White Paper page 3 footnote 2

[150] 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>; Paul Black, 'Ring hacked: doorbell and camera security issues' NordVPN (Blog Post, 4 June 2020) <https://nordvpn.com/blog/ring-doorbell-hack/>

[151] 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/>

user features and therefore requires a trade-off between security and product features.[152] Videos that are end-to-end encrypted are automatically excluded from any requests made by law enforcement.[153] The use of two factor authentication and end to end encryption is consistent with industry standards for IoT 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.

As the Productivity Commission's *Right to Repair* report points out, '(c)yber security is an important broader policy issue extending beyond consumer law and the ability to 'repair' products via software updates'.[154] Introducing a reasonable security guarantee under the ACL would raise the prospect of inconsistency between the ACL and other laws regulating data security, including any law establishing minimum security standards for consumer IoT devices resulting from the current policy process aimed at strengthening cyber security or the data security principle in APP 11 of the Privacy Act. The potential for inconsistent standards could, however, be minimised by expressly linking a guarantee of device security to other laws. For example, a guarantee of reasonable security could be deemed to be satisfied if a device complies with the minimum standards mandated by a consumer IoT security law, or if the device complies with a security ratings label. While it is important to avoid unnecessary legislative duplication, introducing a guarantee of reasonable security to the ACL would have the advantage of providing an additional avenue for enforcing security standards. As indicated previously, this project is investigating additional measures that might better promote 'joined-up regulation'.

Recommendation 7

In the absence of a more fundamental reform, a deeming provision should be introduced to the ACL to provide that the consumer guarantees apply to software embedded in integrated products and to internet-connected products as a whole.

In *ACCC v Apple (No 4),*[155] the Federal Court held that the consumer guarantees apply to a software fault in iPhones and iPads. As explained below, however, there are remaining uncertainties in how, if at all, the existing consumer guarantees apply to consumer IoT devices. Moreover, in its inquiry into

[152] Ring, 'End-to-End Encryption White Paper' (January 2021) https://assets.ctfassets.net/a3peezndovsu/7bwgu7ybi1XoyH61pDraYT/94e4bab9347d4abe07f8d843fdfd4bd4/Ring_Encryption_Whitepaper_FINAL.pdf

[153] ing, 'End-to-End Encryption White Paper' (January 2021) 12 https://assets.ctfassets.net/a3peezndovsu/7bwgu7ybi1XoyH61pDraYT/94e4bab9347d4abe07f8d843fdfd4bd4/Ring_Encryption_Whitepaper_FINAL.pdf

[154] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 98.

[155] [2018] FCA 953.

the *Right to Repair,* the Productivity Commission received evidence about the difficulties experienced by consumers in addressing faulty software embedded in devices.[156] Short of introducing a new category of consumer product, one way to address this would be to introduce an appropriately drafted general provision deeming that the consumer guarantees apply, to the greatest extent possible, to software embedded in integrated products and to internet-connected products as a whole. This would go beyond the Productivity Commission's recommendation, introduced immediately below, to introduce a new consumer guarantee to provide reasonable software updates for a reasonable time period, as it would provide statutory guidance about the application of all relevant consumer guarantees. As explained further below, however, it would need to be accompanied by other, more specific, amendments to the consumer guarantees.

Recommendation 8

In the absence of more fundamental reforms, as recommended by the Productivity Commission, the ACL should be amended to include a new consumer guarantee to provide reasonable software updates for a reasonable time.

The Productivity Commission's *Right to Repair* report concluded that the consumer guarantees in the ACL are 'reasonably comprehensive and generally work well',[157] but made some recommendations for improving the guarantees. Of particular relevance to consumer IoT devices, the PC identified concerns with the uncertainty over a 'reasonable' period of product durability and a lack of clarity about whether software updates are covered by the guarantees. The report proposed a number of measures to deal with uncertainty about the 'reasonable durability' of products, including enabling consumer bodies to lodge 'super complaints', which are addressed further below. In relation to software updates, the PC 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.[158]

As the PC pointed out, it is unclear whether the consumer guarantees, and especially the guarantee of spare parts and repair in s. 58 of the ACL, impose an obligation to provide upgrades for embedded software – and they likely do not. Nevertheless, software updates may be necessary to correct faults,

[156] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 96.
[157] Ibid. p. 79.
[158] Ibid. p. 98.

address security vulnerabilities, maintain functionality, and add new features or improvements.[159] In making the recommendation, the PC explained the purpose of the proposed new guarantee as 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'.[160] While the PC 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'.[161] On this issue, the PC report also flagged the possibility of manufacturers being required to inform consumers at the point-of-sale about the minimum period they will provide essential software updates, such as through a labelling scheme. Issues relating to pre-contractual disclosures of information are dealt with in this report further below.

As explained above, this report recommends more fundamental reform to the consumer guarantees to account for the distinctive features of connected devices than merely introducing a new guarantee. While we support a new guarantee relating to software updates, we also support a guarantee of reasonable device security and a guarantee that elements of complex, hybrid devices are properly integrated. There may be additional guarantees that could apply to connected devices and/or digital content.

The PC recommendations were confined by the terms of reference to issues relating to the 'right to repair' in the Australian context, including the legislative arrangements that govern repairs of goods and services. Accordingly, in assessing the consumer guarantees, the PC report did not consider broader issues, such as difficulties in applying the distinction between goods and services to hybrid, connected devices and potential problems in ensuring that device components are properly integrated. This, as well as the extent to which the PC inquiry was not specifically focused on connected devices, may explain the limited nature of some of the PC recommendations. Moreover, in considering the relationship between the recommendation to introduce a guarantee relating to software updates and more general security obligations, the PC acknowledged that 'to fully achieve broader cyber security objectives additional measures may be needed beyond the Commission's recommended consumer policy changes'.[162]

This report has previously pointed to the potential problems that may arise from potential inconsistency in security obligations imposed by different statutory regimes but has suggested ways

[159] Ibid. p. 96.
[160] Ibid. p. 98.
[161] Ibid.
[162] Ibid. p. 98.

of dealing with this. On balance, we consider that the benefits of including an express consumer guarantee of device security in the ACL outweighs any potential disadvantages. We therefore support the PC recommendation to introduce a new consumer guarantee of reasonable software updates but consider that a broader range of guarantees specifically adapted to connected devices and digital content to be preferable. In either case, legislative reform would be needed to define the products to which the new guarantees would apply.

Uncertainties in the Application of Existing Guarantees

This section of the report identifies and explains uncertainties in how the most relevant consumer guarantees apply to consumer IoT devices. As indicated previously, the three most relevant 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.

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).[163] To add certainty to the standard, the ACL introduced a definition of 'acceptable quality' that is more expansive than the definition of 'merchantable quality' under the TPA. Under s. 54(2) of the ACL, goods will be of 'acceptable quality' if they are:

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

(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

[163] TPA, s. 71.

hidden defects) would regard as acceptable having regard to a number of listed statutory matters. The statutory matters that must 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.[164]

The guarantee of acceptable quality is not an absolute guarantee that goods will be free from any defect, completely safe or of unlimited durability – which would be impractical. The guarantee is therefore subject to the 'reasonable consumer' test.

There are, however, difficulties in applying the 'reasonable consumer' test, and particular difficulties in applying the test to consumer IoT devices. Consumer IoT devices may be relatively opaque to consumers: the functions and nature of the device may change due to software upgrades and the hybrid mix of software, data and hardware may make it difficult for consumers to understand how a device works. Arising from these features, IoT devices raise novel issues for the application of the guarantee of acceptable quality. For example, security vulnerabilities in consumer IoT 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 DDoS attacks. 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. Moreover, 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.[165] This raises questions about the application of the 'reasonable consumer' test where defects or other flaws result from 'upgrades' to devices that are difficult or impossible for a consumer to be aware of or to predict.

The ACL Review Final 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.[166] In relation to guidance about product safety, the Report specifically recommended that guidance should clarify how

[164] ACL, s. 54(3).
[165] See, for example, Freestone Auto Sales Pty Ltd v Musulin [2015] NSW CA 100.
[166] ACL Review Final Report, p. 14.

the guarantee should apply where a safety issue may not eventuate for some time or render the good as a whole unsafe.[167] In relation to reasonable durability, the 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'.[168] Following the recommendations in the Final Report, and public consultation on draft guidance, specific guidance on how the consumer guarantee of acceptable quality applies to the safety and durability of goods has been produced by relevant stakeholders, including state and territory consumer affairs and fair trading offices.[169]

While the consumer guidance provides a gloss on the guarantee of acceptable quality, the practical examples provided are confined mainly to traditional consumer products. The guidance therefore provides limited assistance in determining how the guarantee may apply to consumer IoT devices, which are more complex than most other products, where the functions of the product may change over time, and which may be relatively opaque to consumers. Therefore, although the ACL Review Final Report referred to the need for specific guidance about how the guarantee applies to smart or hybrid products, the published guidance has not met this need.

The PC report on the *Right to Repair* identified general uncertainties in determining what amounts to 'reasonable durability' in applying the guarantee of acceptable quality and considered proposals for addressing these uncertainties by introducing additional regulatory guidance.[170] While acknowledging that there might be some benefits in providing guidance, on balance, the PC concluded that the potential disadvantages outweighed any benefits. Instead, the PC supported proposals for enhancing the enforcement of existing guarantees, including the introduction of a 'super complaints' mechanism, as a means for addressing regulatory uncertainties. The merits of providing regulatory guidance and the proposed 'super complaints' mechanism are assessed further below.

Meanwhile, as explained previously, uncertainties in the application of the existing consumer guarantees to consumer IoT devices could potentially be addressed by a general deeming or interpretative provision, which might need to be accompanied by amendments to specific guarantees. In relation to the guarantee of acceptable quality we suggest that, at a minimum, there is a need to

[167] Ibid. p. 18.
[168] Ibid. p. 23.
[169] Australian Consumer Law, Guidance on the consumer guarantee as to acceptable quality and 'safe'; Australian Consumer Law, Guidance on the consumer guarantee as to acceptable quality and 'durability'.
[170] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, pp. 87-91.

address the extent to which the guarantee is limited to the quality of a product at the time of supply, so that the guarantee can capture defects that may arise as a result of software updates.

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 ss. 55 and 56 of the ACL, suppliers of goods guarantee that they are reasonably fit for purposes disclosed by or to the consumer. Under s. 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 s. 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.[171] The duty imposed on suppliers by the s. 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'.[172] This seems to necessarily follow from the requirement to meet the standard in accordance with the purpose disclosed by a consumer.

Under s. 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 s. 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 IoT consumer devices for the guarantees in ss. 55 and 56 relates to the extent to which IoT products, and the operation of the products, may change over time as a result of software upgrades 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, an IoT 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 IoT devices, there are questions in relation to the s. 55 guarantee about when a device might be 'reasonably' fit for a disclosed purpose.

[171] Jeanie Marie Paterson, Corones' Australian Consumer Law (4th ed, Thomson Reuters, 2019) p. 391.
[172] Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010, Explanatory Memorandum, [7.43].

As with the guarantee of acceptable quality, if a general deeming provision were to be introduced to ensure that the guarantees apply to consumer IoT devices, this may need to be supplemented by amendments to ss. 55 and 56 to ensure that they apply to devices that have been modified after the point-of-sale by software updates.

Guarantee of Spare Parts and Repair Facilities

Under s. 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 s. 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. Moreover, what is 'reasonable' is determined from the manufacturer's point of view, meaning that the question is 'whether it is reasonable for the manufacturer to place the consumer in a position in which repairs or spare parts are not available'.[173] Consumer guidance on the guarantees makes it clear that what is 'reasonable' depends upon the nature of the goods, with the following examples being given:

- it would be reasonable to expect that tyres for a new car will be available for many years after its purchase;
- it may not be reasonable to expect that spare parts for an inexpensive children's toy are available at all.[174]

Consumer IoT devices are complex products, with their operation commonly opaque to consumers. The increasing complexity of consumer products, especially arising from the incorporation of software into products, has given rise to economy-wide concerns about the increasing difficulties facing consumers in effectively repairing products, which formed part of the background to the PC inquiry into the *Right to Repair.*

One of the issues considered by the PC inquiry was the rationale for 'opt out' clauses for the provision of spare parts and repair facilities. Under s. 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 in relation to the goods or will only be available for a specified time. In its final report, the PC indicated that it had not seen evidence of widespread use of the 'opt-out' clause, and therefore did not make any recommendation for removing or amending s. 58(2). Nevertheless, in supporting the introduction

[173] Jeanie Marie Paterson, Corones' Australian Consumer Law (4th ed, Thomson Reuters, 2019) p. 401.
[174] Consumer Guarantees: A Guide for Business and Legal Practitioners (Commonwealth of Australia, 2016) p. 17.

of a new guarantee for reasonable software updates, the PC recommended that it not be subject to an 'opt-out' clause similar to that in s. 58(2). The reason given for this distinction was that, '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'.[175]

Consumer IoT devices are complex products, involving the interaction of software, hardware and service elements. Moreover, the supply chain for IoT products may be complex, with multiple parties being responsible for different elements of a product. Consumers confronted with these complex products that may require rectification may be unable to determine the source of the problem or to determine which entity is responsible for the product. While we support a new guarantee of reasonable software updates, we do not think that this alone is sufficient to address the problems facing consumers where IoT devices are not performing as they should or need repairs. In this report, we therefore support additional bespoke guarantees, such as a guarantee that elements of a complex product, such as an IoT device, are properly integrated. Moreover, while the PC report recommends that the proposed new guarantee of reasonable software updates apply to 'manufacturers', in implementing the proposal consideration should be given to whether there is a need to be more specific about the entities responsible for software updates for complex, hybrid products. In addition, if, as suggested in this report, a general deeming provision might assist in ensuring that the existing guarantees apply to consumer IoT devices, consideration may need to be given to how to introduce certainty as to whether the proposed new guarantee or the s. 58 guarantee of repair and spare parts would apply where problems are encountered with IoT devices.

Consumer guarantee enforcement issues

In general, the PC *Right to Repair* report accepted arguments made in some submissions that the certainty and effectiveness of the existing consumer guarantees could be improved by enhanced enforcement. As the PC report put it:

> A well-functioning consumer redress system is essential for the effective operation of the consumer guarantees.[176]

The importance of enhanced enforcement mechanisms was strongly supported in feedback on our preliminary report.

[175] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 98.
[176] Ibid. p. 102.

Overall, the PC 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 report 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.*[177]
- *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.*[178]
- *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 Australian Competition and Consumer Commission (ACCC).*[179]

The ACCC is currently unable to take legal action against suppliers or manufacturers that refuse to provide a remedy that they are entitled to for breach of a consumer guarantee. In December 2021, Treasury commenced a consultation on options for improving the effectiveness of the consumer guarantees under the ACL.[180] The consultation canvassed the option of introducing a prohibition on suppliers failing to provide a remedy for a breach of a consumer guarantee, which would be enforced by a court imposing a civil pecuniary penalty or injunction, or the ACCC issuing civil penalty notices. The consultation, however, proposed that the option should apply only where there is a 'major failure'. 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.[181]

[177] Ibid. Recommendation 3.4, p. 110.
[178] Ibid. Recommendation 3.3, p. 107.
[179] Ibid. Recommendation 3.2, p. 101.
[180] The Treasury, Consultation Regulation Impact Statement, Improving the effectiveness of the consumer guarantee and supplier indemnification provisions under the Australian Consumer Law, December 2021.
[181] Ibid. p. 45.

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, is an overdue reform that can improve the certainty and effectiveness of the consumer guarantees regime. It should, however, be seen as part of a broader range of reforms. Enforcement of the guarantees can only be effective if the guarantees themselves impose obligations that address the most important issues facing consumers. As this report has suggested, there is scope for new guarantees to be introduced to address distinctive issues raised by consumer IoT devices. Furthermore, enhanced enforcement of individual consumer complaints does not necessarily address systemic issues confronting consumers. We therefore support the PC recommendation for introducing a 'super complaints' mechanism. While, as the ACCC has suggested, such a mechanism has the potential to divert resources away from other priorities, we agree with the PC that, if the problem identified by a consumer body is not significant, this would require only the minimum resources needed for an initial investigation.[182]

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 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.[183] The market for connected devices in the home is growing at a considerable rate, and raises some novel consumer protection issues. One systemic issue raised in this draft report is the extent to which, given the complex nature of consumer IoT devices, consumer complaints may cut across regulatory regimes, such as consumer protection and data privacy laws. Although there are clearly resource implications, and potential problems of regulatory duplication, in introducing a new regulatory regime, there may be benefits in establishing a one-stop-shop complaints mechanism for consumer IoT devices, such as a specialised ombudsman. This possibility will be investigated further in the next stage of the project.

Guidance on consumer guarantees?

Submissions to the PC inquiry into the *Right to Repair* supported the production of regulatory guidance by the ACCC on the meaning of 'reasonable durability' under the consumer guarantees.[184] On the other hand, however, in its submission to the PC draft report, the ACCC argued that providing non-

[182] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 100.
[183] Ibid. pp. 104-5.
[184] Ibid. p. 89.

binding guidance on product durability would be both costly and relatively ineffective.[185] On balance, the PC concluded that additional ACCC guidance on reasonable durability of products would not have net benefits; and that enhanced enforcement measures would have a greater impact on improving certainty about the consumer guarantees and improving consumer welfare.[186]

The spectrum of legal and regulatory issues raised by consumer IoT devices that have been identified in this report indicates the importance of a holistic response to the policy challenges. Given the novel issues raised by IoT devices, one of the challenges is increasing certainty about how consumer guarantees apply to these products. As this report explains, we consider that the preferred policy option would be to introduce guarantees that apply specifically to hybrid, connected devices and other digital products and, failing that, to introduce a deeming provision with additional targeted amendments. In the absence of these reforms, however, a range of measures should be pursued to improve regulatory certainty.

While enhanced enforcement, which may over time result in more court decisions, has a role to play, this need not preclude other measures. As with any principles-based regulation, there is an ongoing need for guidance in how principles formulated at a high level of generality may be operationalised. This need can be partially met by regulatory guidance, such as the guidelines produced by the OAIC on the Australian Privacy Principles (APPs).[187] While acknowledging the particular difficulties in formulating meaningful practical guidance about when products are 'reasonably durable' identified by the ACCC in its submission to the PC, this report has identified considerable areas of uncertainty in applying the relevant existing guarantees to consumer IoT devices. Given the growing prevalence of hybrid, connected devices in the homes of many Australians, we do think that, in the absence of substantive reforms to the guarantees, there is a role for greater regulatory guidance on the application of the guarantees, and especially the guarantee of acceptable quality, to consumer IoT devices. It should, however, be borne in mind that, given that any guidance is necessarily non-binding, this is less of a priority than other proposals made in this report.

Pre-contractual Information Disclosure

Recommendation 9

All suppliers of digital products should be required to ensure that clear explanations of prescribed contractual terms, including warranties, are made available to consumers before purchase. The

[185] ACCC, ACCC Submission in response to the Productivity Commission Draft Report, July 2021.
[186] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 91.
[187] Office of the Australian Information Commissioner (OAIC), Australian Privacy Principles Guidelines, July 2019.

contractual terms and conditions should also be publicly available on supplier websites. We recommend that additional proposals be investigated for improving access to terms and conditions for consumer IoT devices, such as requiring that the information about terms and conditions be disclosed to the ACCC to be published on a publicly available register of contracts for digital products with obligations to notify and update any changes or requiring terms and conditions to be lodged with any statement of compliance required to obtain a ratings label.

The limited disclosure of consumer information regarding digital products is a significant issue for consumers and the organisations who represent their interests as well as for the possibility of more meaningful market regulation by government authorities. Advantages of disclosure include transparency in the contracting process as well as disclosure of terms that promote honesty and informed consent by consumers as they determine whether or not to enter a contract.[188] Noto La Diego and Walden argue that transparency is integral to fairness but the need for transparency within a contract will depend on the nature of the provision and is particularly important for unfair terms.[189]

Although there are requirements for pre-contractual disclosure of certain terms in other jurisdictions, the ACL does not currently require pre-contractual disclosure of key terms. 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 IoT products is to purchase the product. Often consumers then download linked software which contains additional terms and conditions of use, which is accessible only after purchase.

CASE STUDY: Tapo Smart Light Bulb

The Tapo Smart Light Bulb is available 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 consumer 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 provides further information not disclosed at purchase 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 could be more expensive than purchasing a new product.

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

[189] Guido Noto La Diega & 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'.

In multiple case studies, consumers were first required to accept terms of use and privacy policies in relation to hardware if they wished to use the relevant IoT products. Consumers were then asked to accept further user agreements and privacy policies containing additional provisions that reflected specific privacy obligations of different international jurisdictions before they were able to use the apps that permitted them to access 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 in relation to other jurisdictions such as the United States or Europe but not for Australia.

CASE STUDY: Vtech Smartwatch

For the DX smartwatch, Australian warranty information is provided within the packaging on purchase of VTech products. 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 wish to accept the additional privacy policy (based on European privacy regulations) terms and terms of use in relation to the Learning Lodge app that permits consumers to access all the features of the DX smartwatch. This includes a requirement that children using the app 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 United States and Canada. When the device is imported 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 only applies to American and Canadian purchasers.

A pre-purchase requirement for disclosure of key terms has recently been introduced into the New South Wales *Fair Trading Act 1987* (NSW).[190] 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.'[191] 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

[190] Fair Trading Legislation Amendment (Reform) Act 2018 (NSW).

[191] Fair Trading Act 1987 (NSW) s47A(1).

data about or from a consumer to a third party.[192] 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.[193]

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 used for specific industries. The New South Wales *Fair Trading Regulation 2019* 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.[194]

This report recommends that a disclosure requirement that is similar to the New South Wales mechanism should be applied to digital products. This should provide 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.[195] The information standards can give further specific guidance about the type of terms that suppliers should provide clear information about to consumers and this can be revised so that it responds to consumer concerns that may emerge in the changing digital environment. If a separate information standard was developed in relation to digital products and adopted federally, the law could require disclosure of certain terms that are directly relevant to problems for consumers identified in this report and its recommendations. Clear explanations of the substance of these prescribed terms should be made available to consumers before purchase in addition to the disclosure on a publicly available website of the full contractual terms and conditions that consumers are expected to agree to as users of the IoT device.[196] These explanations could assist consumers to understand the complexities of interrelated agreements that are frequently characteristic of digital products.[197]

[192] Ibid s 47A(2).
[193] Ibid s 47A(3).
[194] Fair Trading Regulation 2019 (NSW) Part 2, Div 2.
[195] See below discussion that a term allowing unilateral amendments without notice should be regarded as unfair.
[196] 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) Schedule 1.
[197] Noto La Diega and Walden 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': 19.

Although it is not a requirement of the NSW legislation, consumer protection could be strengthened by a further obligation to deposit those terms that are required to be disclosed to consumers prior to purchase on a publicly available register, such as a register maintained by the ACCC. The register would disclose the key terms registered by suppliers, using a standardised format that reflects the requirements of any information standards. The register can clearly notify consumers that publication of those terms is to provide consumers with information but does not reflect endorsement of those terms as being consistent with consumer protection legislation or accurate. An additional obligation to provide the link to a website where suppliers disclose the full contractual terms and conditions that consumers are expected to agree to should be consistent with the current obligations for disclosure in the Australian privacy regime. This approach can reduce the likelihood of constant updates to the register for minor contractual changes and may discourage practices such as unilateral changes to important terms and conditions.

There are benefits and disadvantages to this disclosure approach. A mandatory disclosure requirement to consumers of digital products with the registration of disclosed terms could be useful for the regulatory activities of the ACCC and state and territory agencies as it would permit them to more easily monitor contractual terms that are unfair or unconscionable. Mandatory disclosure of warranties for hardware and software, as well as consumer, privacy and security protections, will strengthen other recommendations in this report. It would also permit consumers and consumer organisations to proactively inform consumers about those problematic features of digital product contracts that we identify in this report. This can support competition and market correction for problems such as unfair consumer terms and unilateral contractual changes. Having a central repository for this information in a form guided by information standards would enable consumer organisations to more meaningfully compare the market for digital products based on consumer protection concerns. It would permit consumers to adopt a pro-active approach to identifying suitable products, rather than expecting them to bear the cost of returning digital product hardware after they read the terms and conditions and are informed that product return is their only recourse if they do not agree to comply.

The disadvantages are that this approach would require resources for the ACCC to establish and maintain the website. Resources would also be required to effectively monitor compliance with the disclosure obligation, including ensuring that forms are correctly populated so that correct information is publicly available. In their submission to the PC on the Right to Repair the ACCC noted practical enforcement challenges in relation to consumer guarantees.[198] The proposed legislation

[198] ACCC, Submission in response to Productivity Commission Inquiry into the Right to Repair in Australia Issues Paper, February 2021, 2.

should include enforcement provisions that permit the ACCC to take court action to address compliance failure. The NSW legislation permits NSW Fair Trading to issue penalty notices for breach of standards relating to information standards.[199] In addition to pecuniary penalties, remedies available for breach of the requirement to disclose substantially prejudicial terms following court action include pecuniary penalties and disqualification of persons from managing corporations.[200]

Other proposals that can enhance disclosure of these important terms and conditions should also be investigated. The New South Wales laws do not require deposit of terms and conditions on a publicly available register but use other mechanisms for disclosure to consumers that may include provision of a summary of prejudicial terms or check-boxes linked to the prescribed information that the consumer must acknowledge.[201] It is too soon to comment on compliance with the new obligations as they were introduced in July 2020 and the grace period expired at the beginning of 2021. Other options include requiring terms and conditions to be lodged with any statement of compliance required to be submitted to obtain the ratings label proposed in Recommendation 3. This should also require suppliers to provide that information and regularly update it on a publicly available website. Alternatively, an independent consumer organisation may be willing to maintain a public register for digital products if they are provided funding to do so.

'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.[202]

[199] Fair Trading Act 1987 (NSW) s 47D.
[200] Ibid s 70.
[201] European Union Directives also mandate pre-purchase provision of certain information and do not require registration of this information: see Council Directive 2011/83/EU, On Consumer Rights, 2011 O.J. (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 (OJ L 136, 22.5.2019; 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 (OJ L 136, 22.5.2019).
[202] 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.

As this report has explained, the complexity and hybrid nature of IoT devices presents 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, this is often exacerbated by the way in which suppliers present terms and conditions to consumers. In addition, the supply of consumer IoT devices is rarely a simple 'one-off' supply of a product. Rather, the dependence of most devices upon software upgrades 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, 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.

Statutory Unconscionability

Section 21 of the ACL prohibits conduct in trade or commerce that is, in all the circumstances, unconscionable. The s. 21 prohibition applies to conduct in the supply or acquisition of goods or services, and therefore applies to contracts for the supply of consumer IoT 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. It is unsurprising that giving meaning to, and applying, a broad standard such as statutory unconscionable has been contentious.[203] Feedback received on the preliminary report cast doubt the practicality of proposals for reforming statutory unconscionability to improve certainty about the operation of the standard. Nevertheless, unconscionability remains the most important avenue for redress for procedural unfairness involving vulnerable consumers. Some of these issues will be taken up in the next stage of the project.

Prohibition of 'Unfair Trading' Practices

Recommendation 10

The government should expedite work on producing options for introducing a statutory prohibition of unfair trading, which should be aimed particularly at addressing predatory and manipulative conduct associated with data-driven business models. The boundaries of any prohibition should be carefully calibrated so that it is proportionate and does not extend to legitimate business practices. The prohibition should be regarded as a 'safety net' that forms one element of a layered regulatory regime.

[203] J.M. Paterson, 'Unconscionable Bargains in Equity and Under Statute' (2015) 9 Journal of Equity 188.

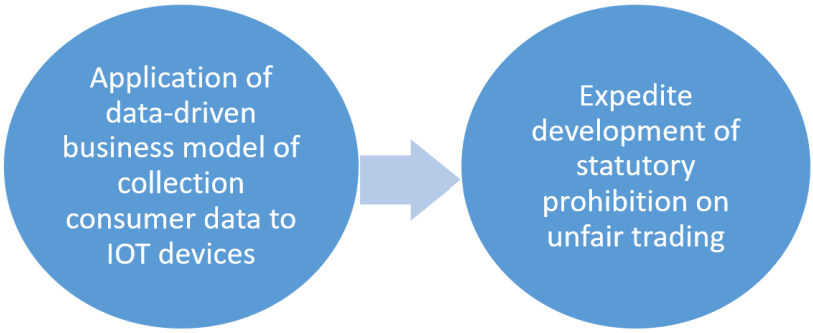

Figure 7 Using data driven business model to expedite development of statutory prohibition on unfair trading

As a 2009 Productivity Commission report pointed out, statutory unconscionability not only lacks clarity, but it is costly and slow to use. Consideration therefore needs to be given to whether there is conduct outside the scope of statutory unconscionability that should be prohibited, or whether there are any alternatives that could assist in dealing with potential procedural unfairness in consumer IoT contracts.

In its *DPI,* 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.[204] 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 IoT providers apply versions of the data-driven business model, the ACCC's analysis is as applicable to the provision of consumer IoT 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'.[205]

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.

[204] Australian Competition and Consumer Commission (ACCC). 2019. Digital Platforms Inquiry, Final Report, June 2019, pp. 498-9.
[205] Ibid. p. 499.

- 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 U.S.[206] In making this recommendation, however, the ACCC noted that the 'scope of such a prohibition should be carefully developed so that it is sufficiently defined and targeted, with appropriate legal safeguards and guidance'.[207] In its submission to the PC *Right to Repair* inquiry, the ACCC argued that a general prohibition on unfair trading could address concerns relating to the 'durability' of products, which may have particular application to consumer IoT devices, 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;
- a business not providing security updates for smart products for a reasonable amount of time, thereby putting sensitive consumer information at risk.[208]

CASE STUDY: August Smart Lock

The type of sensitive information that the August Smart Lock Pro might collect could include the timing and identity of home visitors. August Smart Lock Pro provides that the purpose of its collection of data is 'performance as necessary to support a contract, including fulfilling product orders, enabling the functionality of the website, providing customer support, and notifying you of account or important product updates.' However, the privacy policy also discloses that it enables third-party advertising services to use cookies with website visitors, suggesting that data collection may be not limited to the narrower purposes described.

In its response to the *DPI*, the government 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

[206] Ibid. p. 498.
[207] Ibid.
[208] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 227.

for introducing such a prohibition would be developed in 2020.[209] In its final report on the *Right to Repair,* 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.[210] 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, the government has not produced policy options for addressing the ACCC's recommendation from the *DPI.*

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.[211] While the authors explain the benefits of a calibrated prohibition of unfair trading, they also acknowledge that it should not be seen as a 'magic bullet', but must be part of a layered regulatory regime, which includes bright-line rules as well as broad standards such as a 'safety net' prohibition on unfair trading.[212] 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'.[213] Given the need for a 'layered' or 'holistic' approach to regulating 'unfair' practices in the provision of consumer IoT devices, this report includes further recommendations relating to other elements of a regulatory regime, including possible bright line rules for unfair contracts, immediately below.

[209] Australian Government. 2019. Regulating in the Digital Age, Government Response and Implementation Roadmap for the Digital Platforms Inquiry. 12 December 2019.

[210] Productivity Commission, Right to Repair, Inquiry Report No. 97, 29 October 2021, p. 228.

[211] J.M. Paterson and E. 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; J.M. Paterson and G. 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.

[212] J.M. Paterson and E. 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.

[213] Consumer Policy Research Centre (CPRC), Unfair Trading Practices in Digital Markets – Evidence and Regulatory Gaps, Research and policy briefing, December 2020, 17.

Unfair Contracts

Recommendation 11

Consideration should be given to establishing a more 'layered' regime than the current unfair contract terms law for regulating unfair terms in standard form consumer contracts by introducing a black list of prohibited terms or a grey list of presumptively unfair terms, or a combination of both.

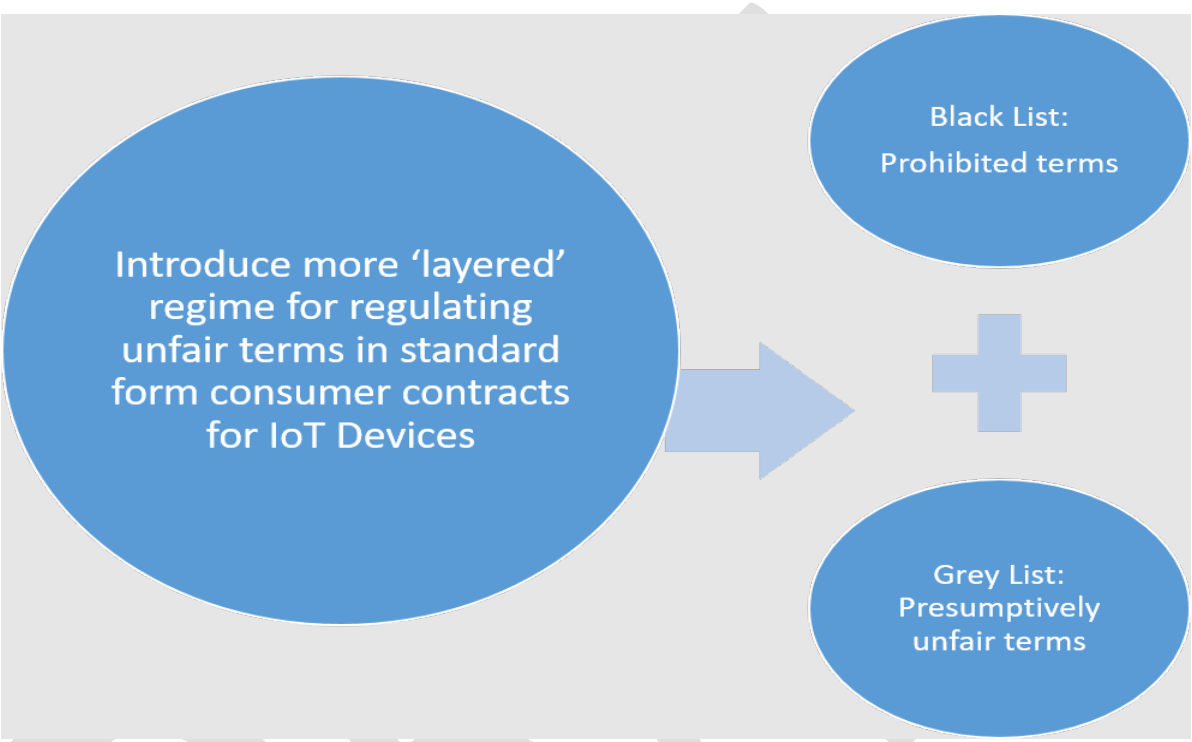

Figure 8 Layered regime for regulating unfair terms: Black and Grey Lists

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 s. 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 s. 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 prepared by one party only, and 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 s. 24(1) 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, and are not prohibited and do not create a presumption that the term is unfair. The examples of unfair terms can therefore be regarded as a 'grey list' rather than a 'black list'.[214] The examples of unfair terms set out in s. 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;

[214] Jeanie Marie Paterson, Corones' Australian Consumer Law (4th ed, Thomson Reuters, 2019) p. 234.

- 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.

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 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.

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. The iRobot Terms of Service provide a URL that will contain the current version of the Terms of Service however the URL directs the user to a blank page.

In its *DPI,* the ACCC recommended amending the unfair contract terms law so that unfair terms are prohibited and not just voidable, and that civil penalties apply to the incorporation of an unfair term in a consumer or small business standard form contract.[215] 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 this would extend to include whether unfair terms should be illegal.[216] 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,

[215] Australian Competition and Consumer Commission (ACCC). 2019. Digital Platforms Inquiry, Final Report, June 2019, p. 497.
[216] Australian Government. 2019. Regulating in the Digital Age, Government Response and Implementation Roadmap for the Digital Platforms Inquiry. 12 December 2019, p. 5.

in November 2020 Commonwealth and state and territory consumer affairs ministers announced they had agreed to amend the unfair contract terms law by:

- 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'.[217]

In August 2021, the Commonwealth released exposure draft legislation aimed at strengthening and clarifying the unfair contracts law.[218] The draft bill includes provisions aimed at strengthening the remedies and enforcement of the unfair contracts regime, expanding the class of contracts covered by the regime, and clarifying and strengthening some of the provisions. In relation to remedies and enforcement, the bill would:

- provide courts with the power to impose a pecuniary penalty for a contravention of the prohibition on proposing, applying or relying on an unfair contract term provision in a standard form contract;
- streamline the powers of a court to make orders to void, vary or refuse to enforce part or all of a contract;
- make 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;
- make clear a court's power to issue injunctions against a respondent with respect to existing or future consumer or small business standard form contracts entered into by a respondent, 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; and
- create a new rebuttable presumption that terms that have been found to be unfair that are subsequently included in relevant contracts in similar circumstances, are unfair.

While the reforms in the draft bill would strengthen the existing regime, especially in relation to enforcement, we consider that there are more fundamental questions about the extent to which the

[217] The Treasury, 'Enhancements to Unfair Contract Term Protections', November 2020, https://consult.treasury.gov.au/consumer-and-corporations-policy-division/enhancements-to-unfair-contract-term-protections/.
[218] Treasury Law Amendment (Measures for a later sitting) Bill 2021: Unfair contract terms reform (Cth).

current law is adequately equipped to deal with the challenges posed by contracts for consumer IoT 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, secondly, whether there are additional regulatory measures that should 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),*[219] which was adopted in 1993, was an important influence on the introduction of the unfair contract terms law in the ACL.[220] However, apart from a 2019 amendment to provide for increasing the effectiveness of penalties and enforcement,[221] the UCTD has not been updated since it was introduced. An independent study, produced for the European Parliament's Committee on Legal Affairs (the JURI Committee), which was specifically aimed at proposing measures for increasing the effectiveness of the UCTD in the regulation of digital services, was released in February 2021.[222]

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 and a 'grey list' of terms that should be presumed to be unfair unless the service provider gives valid reasons for including the term.

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, include 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.

[219] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993, L 095/29.
[220] Jeanie Marie Paterson, Corones' Australian Consumer Law (4th ed, Thomson Reuters, 2019) p. 200.
[221] Council Directive 2019/2161 of 27 November 2019 on better enforcement and modernisation of Union consumer protection rules, OJ 2019, L 328/7.
[222] Marco Loos and Joasia Luzak, Update the Unfair Contract Terms directive for digital services, Study requested by the JURI committee, February 2021.

- 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.
- 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').

We note that a similar proposal, drawing on previous research commissioned by the EU, was made by Professor Malbon, from Griffith Law School, in his submission to the 2019 Treasury consultation.[223]

The introduction of a black list of prohibited terms, or a grey list of presumptively unfair terms, or a combination of both would represent a fundamental shift in the ACL unfair contract terms law in that it would implement a form of *ex ante* regulation rather than the current *ex post* regulation of unfair terms. The prevalence of problematic terms in the IoT consumer contracts in the case studies examined in this report suggests that the current approach, which is confined to an indicative list of potentially unfair terms, is not achieving the objectives of the unfair contract terms law. This conclusion is reinforced by the 2020 Regulatory Impact Statement produced by Treasury, which recommended introducing civil penalties for unfair contract terms, and which observed that:

[223] Justin Malbon, Submission to Treasury Consultation, Regulation Impact Statement, Enhancements to Unfair Contract Terms Protection, December 2019.

> 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.[224]

Moreover, the introduction of bright line rules that would prohibit certain terms, possibly supplemented by a list of terms that are presumptively unfair, would create a more layered regulatory regime, which is likely to be more effective than the current regime, and which would increase certainty and reduce enforcement costs.

Recommendation 12

The ACCC should be resourced to investigate and potentially design machine learning tools to assist it in the identification of unfair terms in standard form consumer contracts. Such tools may be particularly helpful in enforcing the unfair contract terms law if the law is amended to include black and/or grey lists of categories of unfair terms.

The complexity of standard form contracts, together with the complex nest of contracts that characterise the provision of consumer IoT devices, make it difficult to identify potentially unfair terms. Furthermore, most consumers rationally fail to read, or understand, complex standard form contracts.[225] In addition, even where a consumer may attempt to read contractual terms, problematic terms may be 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, to assist in the analysis of legal documents.[226] 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.[227] 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

[224] The Treasury, Enhancements to Unfair Contract Term Protections, Regulation Impact Statement for Decision, September 2020.
[225] J.A. Obar and A. Oeldorf-Hirsch, 'The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services' (2016), TPRC 44: the 44th research conference on communication, information and internet policy.
[226] Michael Legg and Felicity Bell, Artificial Intelligence and the Legal Profession (Hart Publishing, Oxford, 2020).
[227] Marci Lippi et al, 'CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service' (2019) 27 Artificial Intelligence and Law 117.

in identifying unfair terms, or potentially unfair terms, in complex standard form contracts, we consider there is considerable merit in the investment of public 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 the ACCC in transitioning to more proactive forms of regulatory intervention, which is increasingly required for rapidly evolving technologies, such as IoT devices.[228]

Product Liability

Under the Australian Consumer Law (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[229] or where other goods, land, buildings or fixtures are destroyed or damaged because of the safety defect.[230] 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.[231]

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 and their consumers. 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'[232]. This is particularly true when it comes to consumer IoT 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.'[233]

As discussed above, there is uncertainty as to how the product liability regime applies to consumer IoT devices where harm arises as a consequence of security vulnerabilities. This section will consider the issues that arise when applying the existing product liability regime to consumer IoT devices including the following important questions:

[228] See, for example, World Economic Forum, Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators (December 2020).
[229] ACL s 138(1)
[230] ACL s 140(1), s 141(1)
[231] ACL s 139
[232] The Law Reform Commission, Product Liability (Report No. 51, 1989) 16.
[233] The Law Reform Commission, Product Liability (Report No. 51, 1989) 16.

- Are security vulnerabilities a 'safety defect' under section 9 of the ACL?
- 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?
- Should manufacturers have a continuing duty to monitor security vulnerabilities and provide updates for consumer IoT devices? In such case, could failure to release security updates be considered a 'safety defect'?
- 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 consumer IoT devices.

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.'[234] In making a determination as to the safety of goods under the ACL, the following should 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.

> **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
> (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.

[234] ACL s 9

(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 consumer IoT 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.

Recommendation 13

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

The definition of 'safety defect' is problematic in relation to consumer IoT devices. It is unclear what the 'reasonable expectations' of the community might be in relation to the security of IoT devices. As previously discussed in this Report, there exist information asymmetries between producers/suppliers and consumers. Consumers are often unaware of the security risks posed by consumer IoT devices and are unable to make informed choices regarding security. It is unclear what the reasonable expectations of the community might be in relation to consumer IoT 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.[235]

[235] 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.

The complexity of IoT devices 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.[236] Furthermore, if there is a reasonable expectation as to the presence of certain security features, what security features would be considered so critical that their absence would constitute a safety defect?[237] Reference may be made to a Code of Practice or other industry standards to determine essential security features and there is a potential role for regulators to identify mandatory security principles (see discussion regarding security in Part I above). Consideration should also be given to 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. The continuing relationship between the consumer and the supplier/manufacturer should be sufficient to impose a post-sale duty upon the manufacturer to release updates, as well as monitor and rectify security vulnerabilities.[238]

Recommendation 14

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 may be enacted by introducing a new sub-section under section 142(a): '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.' It is acknowledged that such an approach is contingent upon the introduction of a category of 'digital products' being introduced into the ACL (consistent with recommendation 5 set out above).

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'[239] and it is a defence to a product liability claim under the ACL if the defect arose after the product was put into circulation.

> '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:

[236] Benjamin C. Dean, Strict Products Liability and the Internet of Things, (Center for Democracy and Technology, April 2018) 20.
[237] Benjamin C. Dean, Strict Products Liability and the Internet of Things, (Center for Democracy and Technology, April 2018) 20.
[238] 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, 928*
[239] ACL s 142(a)(ii)

(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.'[240]

There is uncertainty whether such a provision would limit the ability of consumers to make claims for safety defects that arise in relation to consumer IoT 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 consumer IoT 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 extend to cover safety defects that arise as a consequence.

There is similar uncertainty in Europe in relation to the *Directive on Liability for Defective Products* ('Product Liability Directive').[241] The Product Liability Directive is a useful comparator as it forms the basis for the product liability regime established under the ACL. 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.'[242] A recent impact assessment by the European Commission stated that the Directive was 'unclear about who should be liable for defects resulting from changes to products after they are put into circulation.'[243] While the impact assessment

[240] ACL s 142(a)(ii)

[241] Directive on Liability for Defective Products (85/374/EEC)

[242] Directive on Liability for Defective Products (85/374/EEC) art 7(b).

[243] European Commission, Inception Impact Assessment: Adapting liability rules to the digital age and circular economy, Ref.Ares(2021)4266516 – 30/06/2021, pg 2.

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 (e.g. software updates or circular economy activities like product refurbishments)'.[244] 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 15

In the event that a product liability claim involves a consumer IoT device with components, the consumer may bring an action against the ultimate supplier or manufacturer and the burden shall rest with the supplier or manufacturer to reach a determination as to liability between the providers of the component parts.

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 liable for defective goods where a defective component is included in a finished product. The defence effectively excuses 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[245] of the good. As discussed earlier, consumer IoT devices are complex products combining hardware, software and associated services. As observed by Benjamin Dean, 'complex supply chains for the design, manufacture, assemblage, shipping, and sale of these technologies'[246] may complicate the issue of

[244] European Commission, Inception Impact Assessment: Adapting liability rules to the digital age and circular economy, Ref.Ares(2021)4266516 – 30/06/2021, pg 4.
[245] ACL s 7.
[246] Benjamin C. Dean, Strict Products Liability and the Internet of Things, (Center for Democracy and Technology, April 2018) 12-13.

determining and assigning responsibility for defective products. The consumer is unlikely to be aware of, or unable to easily determine, which party in a complex supply chain should be liable for a safety defect and it is unreasonable to place such a burden on a consumer.

Consistent with the principles of good product liability regulation as outlined above, 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 with a consumer only required to bring an action against the ultimate supplier or manufacturer.

Recommendation 16

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 to tangible property or intangible personal property, including data loss.

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. 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.

The loss or damage envisaged under Part 3-5 of the ACL is physical – arising as a consequence of injuries to an individual or damage to physical property such as goods, buildings or land. The nature of digital products 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 consumer IoT 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).

CASE STUDY: Ring Doorbell

There have been several cases in the USA 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.[247] In one case the plaintiff's outdoor camera was hacked with the hacker speaking to the plaintiff's children.[248] In another case hackers obtained access to a camera in a child's room and began speaking to her.[249] Both complaints contain numerous other examples of hacking, including threats and demands for ransoms paid in Bitcoin. The class action complaints allege that Ring has failed to implement basic security measures such as two factor authentication[250] 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 fraud.[251] Such loss or damage would not be covered under existing provisions dealing with liability of manufacturers for safety defects.

[247] See *John Baker Orange on behalf of himself and all others similarly situated,* v Ring LLC and Amazon.com Inc, Case No 2:19-cv-10899; *Ashley LeMay, Dylan Blakely, Tania Amador and Todd Craig v Ring LLC* Case No. 2:20-cv-074

[248] John Baker Orange on behalf of himself and all others similarly situated, v Ring LLC and Amazon.com Inc, Case No 2:19-cv-10899

[249] Ashley LeMay, Dylan Blakely, Tania Amador and Todd Craig v Ring LLC Case No. 2:20-cv-074

[250] Note that two factor authentication has been mandatory for Ring products since 2020.

[251] Ashley LeMay, Dylan Blakely, Tania Amador and Todd Craig v Ring LLC Case No. 2:20-cv-074 [89], [94]

Part III: Privacy law and consumer IoT devices

Introduction

Consumer IoT 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.[252]

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).[253] 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 section of the draft report explains the application of Australian data privacy law to consumer IoT devices for the home and sets out our recommendations.

Australian Data Privacy Law

Australian data privacy laws regulate the collection, use and disclosure of personal information. The most important Act is the *Privacy Act 1988* (Cth), which regulates the collection and processing of personal information by federal government agencies and private sector organisations. 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.

[252] Office of the Victorian Information Commissioner (OVIC), The Internet of Things and Privacy (Issues Paper, February 2020) 11.
[253] https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/#!#18

The scope of the 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 department, or a private sector 'organisation'. Although the Act applies to private businesses, it does not generally apply to small business operators, meaning that it applies to businesses that have an annual turnover of more than $3 million.[254] Under the Act, an APP entity must not engage in an act or practice that breaches an APP.[255] The APPS are 13 principles that regulate the collection, storage, use and disclosure of personal information.[256] For example, the APPs impose requirements to maintain a privacy policy about the management of personal information,[257] not to collect personal information unless it is reasonably necessary,[258] and not to disclose personal information for direct marketing purposes (unless an exception applies).[259] The Act also incorporates important exceptions to the operation of the APPs. For example, under s. 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 Act is confined to interferences with privacy that consist of acts or practices that involve 'personal information'. Under s. 6 of the Act, '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 difficulties, especially in the context of contemporary data processing practices.

Review of the Privacy Act

In the *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 the deficiencies in the law.[260] The recommendations have implications that go beyond the practices of digital platforms and are especially relevant to the

[254] Privacy Act 1988 (Cth) ss 6, 6C, 6D, 6DA.
[255] Privacy Act 1988 (Cth) s 15.
[256] Privacy Act 1988 (Cth), Sch 1.
[257] Privacy Act 1988 (Cth), Sch 1, APP 1.3-1.6.
[258] Privacy Act 1988 (Cth), Sch 1, APP 3.
[259] Privacy Act 1988 (Cth), Sch 1, APP 7.
[260] Australian Competition and Consumer Commission (ACCC). 2019. Digital Platforms Inquiry, Final Report, June 2019 (DPI).

regulation of the data collection and processing practices of consumer IoT 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.

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'.[261]
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'.[262]
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.[263]
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.[264]
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.[265]
6. Increasing maximum penalties under the Privacy Act to mirror the penalties under the ACL.[266]

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 it remains fit for purpose:[267]

1. Reconsider the objectives of the Privacy Act to ensure that consumer privacy is properly protected, including a reconsideration of the balancing 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.

[261] DPI report, Recommendation 16(a), 458.
[262] Ibid. Recommendation 16(b), 461.
[263] Ibid. Recommendation 16(c), 464.
[264] Ibid. Recommendation 16(d), 470.
[265] Ibid. Recommendation 16(e), 473.
[266] Ibid. Recommendation 16(f), 475.
[267] Ibid. Recommendation 17, 476.

3. Review the scope of the Privacy Act, especially the exceptions for small businesses, employee records and registered political parties.
4. Review whether the 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, scheduled to be completed in 2021.[268]

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.[269] 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?*[270]

In October 2021, Attorney-General's released a *Discussion Paper (DP)* which took into account feedback on the *Issues Paper* and proposed reforms for addressing issues identified with the operation of the Privacy Act.[271] At the time of writing this draft report, it was expected that, following feedback, a final report would be released in mid-2022.

Given the extensive scope of the issues raised by the *Discussion Paper,* this analysis addresses only those issues that we have identified as particularly relevant to consumer IoT devices.

[268] Australian Government. 2019. Regulating in the Digital Age, Government Response and Implementation Roadmap for the Digital Platforms Inquiry. 12 December 2019.
[269] Attorney-General's Department, Privacy Act Review, Issues Paper (October 2020).
[270] Attorney-General's Department, Privacy Act Review, Issues Paper (October 2020), Question 34, p. 49.
[271] Attorney-General's Department, Privacy Act Review, Discussion Paper (October 2021) (DP).

A New Regulatory Paradigm?

Recommendation 17

Australian data privacy law should be amended to 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 data processing practices, while allowing for more effective regulatory oversight. Such measures should include targeted privacy impact statements, data protection by default and by design, and targeted monitoring and auditing.*

Data privacy law has always necessarily been linked to technological developments in data processing, and this has resulted in generations of paradigms for the regulation of data privacy.[272] Consumer IoT 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.[273] 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 represents a more recent attempt to adapt data privacy regulation to apply to contemporary data processing practices, it has also been overtaken by events. The first step in reforming the law so that it is adequately adapted to existing practices is to review the regulatory paradigm. In this, lessons can be learned from 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,[274] which built on experience with measures introduced as part of the GDPR to address 'big data' practices. When taken together, it is possible to see 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 regulatory paradigm which attempts to address the challenges of regulating near-

[272] Graham Greenleaf, *Asian Data Privacy Laws* (OUP, 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.

[273] Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books, 2019).

[274] 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.

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 human rights impact assessments, as recommended in relation to AI systems by the Australian Human Rights Commission (AHRC) in its report on *Human Rights and Technology*.[275] 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,

[275] Australian Human Rights Commission, Human Rights and Technology, Final Report (June 2021).

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 below.

Ex ante regulatory measures should be designed, as much as possible, to ensure that privacy protection is embodied in the technologies themselves. However, as software-based technologies, such as AI systems and IoT devices, are subject to fundamental change over time, it is important to apply *ex post* regulatory measures. 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 IoT devices.[276] 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. Moreover, both *ex ante* and *ex post* regulatory measures should be supported by appropriate regulatory powers of investigation and enforcement, including the availability of sanctions.[277]

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 become inoperable. 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.'

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 Commission proposal to regulate AI systems and the AHRC report on *Human Rights and Technology,* is to apply a

[276] Thomas Pasquier et al, 'Data provenance to audit compliance with privacy policy in the Internet of Things' (2018) 22 Personal Ubiquitous Computing 333.

[277] For a similar approach in the context of the regulation of AI systems see: K. Yeung, A. Howes and G. Progebna, 'AI Governance by Human-Rights Centred Design, Deliberation and Oversight: An End to Ethics Washing' in M. Dubber and F. Pasquale (eds), The Oxford Handbook of AI Ethics (OUP, 2019).

'risk-based' approach to regulation. Under this approach, regulation – and regulatory resources – are targeted at technologies that pose the greatest risks.[278] 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, which it also referred to as 'restricted' practices, which are dealt with in more detail below.

Some Problems with 'Privacy by Design'

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'.[279] 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 compliance with other substantive provisions of the GDPR.[280] In addition, even apart from the vague language used in the GDPR, there are a number of competing conceptions of 'privacy by design'.[281]

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 data processing products, such as consumer IoT devices.

The Attorney-General's DP addresses the principle of 'privacy by design' mainly in chapter 10, which deals with 'Organisational Accountability'. Referring to the Explanatory Memorandum to the 2012 amending bill, the DP explains that APP 1 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'.[282]

[278] See, for example, R. Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 3.

[279] Ari Ezra Waldman, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53(1) Cornell International Law Journal 147, 149.

[280] 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, Version 2.0, Adopted on 20 October 2020.

[281] Ibid. 149-151.

[282] DP, p. 150.

APP 1.2 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; but also requires a comprehensive privacy management program which, where appropriate, could require PIAs by independent third parties.

We support the statutory recognition of 'privacy by design' in the Privacy Act, but 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 on the relationship between the principles of DPbDD and what should be the complementary principles of 'security by design and by default'.[283]

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 Attorney-General's DP 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 DP identifies the following two options for reform:[284]

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 which plague the 'privacy self-management' model, and which are referred to later in this section of the report, Option

[283] ENISA, ENISA, Recommendations on shaping technology according to GDPR provisions: Exploring the notion of data protection by default, December 2018.
[284] DP, p. 99.

2 would be unlikely to achieve the objectives of the principle of privacy by default. In general, we consider that the benefits of setting defaults to the most privacy protective – especially in terms of transparency and accountability for data practices - outweigh any inconvenience. We therefore support a statutory codification of the principle of privacy by default.

That said, there is much to be said for the concern expressed by some submissions to the *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 general case for confining the principle 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, as explained below, that the principle is applied more restrictively to high risk acts and practices. Subsequently, in this section of the report, we make recommendations about how the principle may apply in the particular context of consumer IoT devices in the home which engage in ubiquitous data collection.

Advantages and Limitations of 'Risk-based' Regulation

Some submissions on the Attorney-General's *Issues Paper* proposed that certain collections, uses or disclosures of personal information presented such high risks that they should be more tightly regulated or prohibited entirely.[285] The Attorney-General's *DP* 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 *DP* were as follows:

Option 1[286]

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;*
- *The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software;*

[285] DP, p. 94.
[286] Ibid. p. 95.

- *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[287]

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 *DP* 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.[288]

As explained subsequently in this section of the report, we are sceptical of the extent to which privacy self-management, by means of improvements to the 'notice and consent' model, can effectively prevent privacy harms. We therefore do not consider that Option 2, as identified in the *DP,* is a feasible alternative for dealing with high risk acts or practices. We do, however, consider that, in order to deal with the challenges of regulating contemporary data practices at scale, there is potential in 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, we suggest that there is a case for imposing a tiered system of regulation, similar to that in the EC's proposed AI Regulation, for example:

[287] Ibid. p. 96.
[288] Ibid.

- 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;
- 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 focussing regulatory resources, a more highly calibrated or tiered approach to regulation could address issues arising from the removal of the current exceptions in the PA. For example, in considering the case for removing the small business exception, the DP examines the option of retaining the exception, but prescribing further high risk acts and practices.[289] While the flexibly embedded in a principles-based approach, such as the APPs, already arguably embodies a 'risk-based' approach, more expressly recognising this would alleviate potential concerns about the costs of removing the small business exception, while ensuring that high risk acts and practices engaged in by small business do not escape regulation.

Acknowledging the limitations of privacy self-management, in chapter 10 the DP 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'.[290]As explained subsequently in this report, there is a good case for implementing a new 'fair and reasonable' test. The test, however, 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 them shifts to the App entity.

In our consideration of the unfair contract terms law, we have supported the introduction of a black list of prohibited terms and a grey list of terms that are presumptively unfair, as a means for improving regulatory certainty. In a similar way to our proposal for enhancing certainty in determining whether contractual terms are 'fair', we suggest that the proposed broad 'fair and reasonable' standard might be supported by a black list of practices that would be prohibited and a grey list of factors that would be presumptively unfair. It is conceivable that this could be based on 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, and therefore prohibited; processing which poses high

[289] DP, pp. 46-7.
[290] DP, Proposal 10.1, p. 85.

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 which is deemed to be low risk. While the list of acts or practices identified by the *DP* in Option 1 is a reasonable starting point, more nuance would clearly be needed in distinguishing 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 uses, or uses in certain contexts, might be thought to 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 people might be regarded as unacceptably risky.

While we believe 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, it is always important to bear in mind the limitations and problems with applying purely risk-based approaches. For example, risk-based regulation can easily degenerate into a form of cost-benefit analysis, which fails to give due consideration to all risks, including unpredictable and systemic risks.[291] In addition, what amounts to a 'risk' necessarily embodies choices about social and political values.[292] Moreover, 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.

Definition of 'personal information'

Recommendation 18

As proposed by the Attorney-General's Discussion Paper (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, including the definition of 'personal data' under the GDPR.*

Recommendation 19

The amendments proposed by the DP 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

[291] See D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (2018) 37(1) Yearbook of European Law 130.

[292] See, for example, Robert Baldwin & 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.

'reasonably identifiable', and an amended definition of 'collection' that covers inferred information, should also be introduced.

Recommendation 20

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 processing at scale. This could, for example, lead to some re-formulation of the APPs.*

In the *DPI,* the ACCC recommended amending the definition of personal information to clarify that it captures technical data, such as 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.[293] 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, firstly, technical and, secondly, 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.*[294]

In addition, the *DP* proposed the following amendments to support the new definition:

- a non-exhaustive list of the types of information capable of falling within the new definition of personal information

[293] Attorney-General's Department, Privacy Act Review, Issues Paper (October 2020), Question 34, p. 18.
[294] DP, p. 26.

- 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 serious problems arising from the *Telstra* decision,[295] and ensure that the Privacy Act is better equipped to address contemporary data practices. It would also make the Australian Act more consistent with data privacy laws in comparable jurisdictions, including the GDPR. As the *DP* 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.[296]

While we support the suite of changes to the definition of ‘personal information’ proposed in the *DP,* in our view they do not resolve all issues relating to application of data privacy laws to contemporary processes involving the collection and processing of data, including data collected by IoT devices.

CASE STUDY: Google Nest Hub

The Google Privacy Policy highlights the diverse range of information that may be captured by consumer IoT 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
- User activity: such as search terms, content viewed, voice and audio information, purchase activity, browsing history

[295] Privacy Commissioner v Telstra Corporation Ltd (2017) 249 FCR 24.
[296] Ibid.

- 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 is 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'.[297] 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 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 there is only a remote risk of identification.[298] 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.[299] In Australia, the

[297] 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.
[298] 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.
[299] Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4(4) International Data Privacy Law 250.

Australian Computer Society (ACS) has released white papers which propose a framework for assessing the risk of identifiability of data, based on a modified version of the 'Five Safes' framework.[300] 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.[301] This suggests the need for a broad scope for data privacy laws and, accordingly, as proposed in the Attorney-General's *DP,* a broad definition of personal data or personal information. On the other hand, a broad definition raises the problem of scalability, including the social 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.[302] In Australia, the privacy safeguards under the 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.[303] The instrument designating the banking sector, for example, specifies information that goes beyond personal information to include information about financial products and uses of products.[304]

Against this, Schwartz and Solove have argued in favour of retaining the concept of 'personal information' as it serves to confine the scope of privacy regulation, and avoids the prospect of all data needing to be subject to a risk assessment.[305] 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 useful.

[300] See Ian Opperman (ed), Privacy Preserving Data Sharing Frameworks, Australian Computing Society, 9 August 2019.
[301] 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, 73.
[302] 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, 80. See also Omer Tene, 'Privacy: The new generations' (2011) 1(1) International Data Privacy Law 15.
[303] Competition and Consumer Protection Act 2010 (Cth) s. 56AI(1).
[304] Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (Cth).
[305] 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, 1866.

Policy discussions relating to the concept of 'personal information', such as the Attorney-General's *DP,* commonly focus on the 'risks' of *identifying* individuals, directly or indirectly, from the information.[306] Moreover, data privacy laws have long distinguished 'sensitive information' from other 'personal information'. 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, referred to previously in this report. To date, 'identifiability' has effectively been used as a proxy for broader privacy 'risks' to individuals. Given contemporary data practices, however, information or data may pose 'risks' to individuals regardless of the extent to which an individual is identifiable from the information or data.

In its consideration of whether or not to remove the current small business exemption, the Attorney General's *DP* canvassed the possibility of retaining the exemption, but extending the operation of the Act to a broader range of high-risk acts and practices engaged in by small businesses.[307] In examining this option, the *DP* referred to a list of 'high risk' practices set out in guidelines adopted by the UK ICO for data protection impact assessments, which 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.[308] This is a good example of the potential for regulation to be targeted in accordance with the risk of data practices. However, as explained above, we consider that there is broader potential for the Privacy Act, including the APPs, to be re-formulated so that it is better calibrated to contemporary high risk data practices.

We therefore suggest that there is a case for resources to 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 all data falling with an amended definition of 'personal information' at scale. At the same time, as explained previously, it is important to bear in mind that 'risk-based' approaches are not a panacea, and that there are significant limitations and dangers with regulatory approaches centred purely on 'risk'.

[306] See also Raphael Gellert, 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5(1) International Data Privacy Law 3.
[307] Attorney-General's Department, Privacy Act Review, Discussion Paper (October 2021), p. 47.
[308] UK ICO, Examples of processing 'likely to result in high risk'.

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.

Notice and consent

Recommendation 21

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.*

Recommendation 22

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.*

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.[309] 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

[309] See DP, p. 80.

there is no alternative but to consent in order to acquire a product or service. As the ACCC concluded in the *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 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.[310]

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'.[311] First, behavioural science research reveals that individuals often do not make rational choices about the processing of their personal data. Secondly, 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 when taken together are significant.[312]

As currently defined in the *Privacy Act,* consent means 'express consent or implied consent',[313] which sets a low consent threshold.[314] This can be compared with the definition in the GDPR which, in Article 4(11), defines consent to mean:

> any 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 the *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.[315] In the current

[310] DIP, p. 478.
[311] Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880, 1880.
[312] Ibid. 1880-1881.
[313] Privacy Act 1988 (Cth), s. 6(1).
[314] Damian Clifford & Jeannie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94(10) Australian Law Journal 741.
[315] DPI report, p. 466.

round of consultations on reforms, the Attorney General's *DP* 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.[316]
- 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.[317]
- 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*.[318]
- Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.[319]
- 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.[320]

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'.[321] Secondly, 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.[322] 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

[316] DP, p. 69.
[317] Ibid. p. 71.
[318] Ibid. p. 73.
[319] Ibid. p. 78.
[320] Ibid. p. 79.
[321] Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' 1894.
[322] Ibid. 1885.

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; and this can be done, in part, by enhancing the regulatory requirements for notice and consent. The Attorney-General's *DP* 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 *DP* cautioned that 'it is likely to be impractical to develop consent templates, icons or phrases across all sectors'.[323]

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.[324] Warren, Mann and Harkin have recently 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.[325] That said, it may be that properly designed systems aimed at simplifying information provided to consumers can have an effect at the margins, but only when combined with other regulatory measures.

This section of the draft report essentially endorses the proposals for strengthening notice and consent in the Attorney-General's *DP.* Nevertheless, it cautions that the proposed measures may effect only marginal improvements, to the extent they remain embedded in the privacy self-management model. To be effective, they should be matched by additional reforms which strengthen the protections in the Privacy Act, which are explained immediately below.

Additional Protections

Recommendation 23

As proposed in the Attorney-General's DP, 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 any inconsistencies, should prevail. As further proposed in the DP, the principle should be supplemented by a list of non-exhaustive statutory factors. Consideration should

[323] DP, p. 79.

[324] L. F. Cranor, 'Informing California Privacy Regulations with Evidence from Research', (2021) 63(3) Communications of the ACM 29-32, https://cacm.acm.org/magazines/2021/3/250700-informing-california-privacy-regulations-with-evidence-from-research/fulltext.

[325] Ian Warren, Monique Mann and Diarmaid Harkin, Enhancing Consumer Awareness of Privacy and the Internet of Things, August 2021.

be given to whether the statutory factors proposed in the DP could be improved, such as by ensuring that an objective standard is applied in assessing the risk of data processing.

Recommendation 24

Consideration should be given to whether certainty could be improved by introducing elements of a risk-based approach to the collection, use or disclosure of personal information. This could involve drawing distinctions between data processing which poses unacceptable risks, which would be prohibited, processing which poses high risks, which might be presumed to be unfair or unreasonable unless they are justified, and processing which is deemed to be low risk.

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'.[326] 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 Attorney-General's *DP* proposed that additional protections be introduced to ensure minimum acceptable standards for the processing of personal information. In particular, the *DP* proposed that:

> A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.[327]

In formulating this proposal, the *DP* 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 very different Australian legal context. Nevertheless, the test proposed in the *DP* draws on standards in other data privacy laws, such as 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 *DP* is obviously a flexible standard and, as such, requires guidance as to how it would apply in practice. To address this, the *DP* proposed introducing a non-

[326] DP, p. 82.
[327] Ibid. p. 85.

exhaustive list of legislative factors to be taken into account in determining whether processing of personal information is fair and reasonable. The factors proposed by the *DP* are as follows:

- 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;
- 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.[328]

To illustrate the potential operation of the proposed 'fair and reasonable' test, the *DP* 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.

[328] DP, p. 89.

> 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. [329]

The Attorney-General's *Issues Paper* sought specific feedback on how the personal information of individuals may be protected where consumer IoT 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, rely on the dragnet collection of ambient data for their functionality. As such devices indiscriminately collect data, they can clearly collect highly personal information from third parties without their consent.

CASE STUDIES: Collection of highly personal information

A number of the cases 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.[330] 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 personalization but may use data from Google Assistant for ad personalization. These settings may be managed by the user in settings.

The proposed 'fair and reasonable' test, as supplemented by legislative factors and as illustrated by the case study, would go some way to addressing legitimate concerns about the potential

[329] Ibid. p. 90.

[330] Google, Hey Google: Privacy Notice for Audio Collection from Children's Features on Google Assistant, https://assistant.google.com/privacy-notice-childrens-features/?hl=en_GB

unconstrained collection of personal information by IoT devices. For example, in elaborating on the 'reasonable expectations' factor, the *DP* explained that:

> 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.[331]

We further note that the factors identified in the *DP* include 'whether an individual is at foreseeable risk of unjustified adverse impacts or harm'. This raises the issue of whether the risks of data processing should be regulated regardless of whether or not they are foreseeable or the potential harms justifiable. We therefore suggest 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, this could entail distinctions being drawn between: data processing which poses unacceptable risks, which would be prohibited; processing which poses high risks, which might be presumed to be unfair or unreasonable unless the practices are justified or the risks mitigated; and processing which is deemed to be low risk.

Additional Safeguards for Consumer IoT Devices

Recommendation 25

Except where data processing is essential for the functioning of a consumer IoT device, default settings allowing for data processing by means of such devices should be pre-selected to 'off'.

As referred to above, the Attorney-General's *Issues Paper* sought feedback on how the personal information of individuals may be protected where consumer IoT 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 IoT devices installed in the home, are high risk.[332] This is, at least in part, due to the highly sensitive personal information that may be collected in a domestic context. We therefore consider that, over and above the general 'fair and reasonable'

[331] Ibid. p. 86.

[332] See DP, p. 47, citing European Data Protection Board, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020.

standard referred to above, 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.[333]

Many purchasers and users of IoT devices installed in the home are 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 differs from Option 1 identified in the Attorney-General's DP for implementing 'privacy by default', as that canvasses pre-selecting privacy settings to the most restrictive, whereas our recommendation is to set 'functionality' to 'off'. This proposal might be implemented either as a particular application of a general 'privacy by design' principle or as a specific provision requiring that, to the maximum extent possible, default settings for data processing by consumer IoT devices in the home be set to 'off'.

Data security

Recommendation 26

To minimise the possibility of inconsistency across regulatory regimes, the principle of 'joined-up regulation' should be applied across regimes that regulate device security, including any sui generis *security law, consumer protection law and data privacy law. At a minimum, the data security principle in APP 11.1 should be expressly linked to mandatory minimum security standards introduced by* sui

[333] ENISA, Recommendations on shaping technology according to GDPR provisions: Exploring the notion of data protection by default, December 2018, p. 7.

generis *legislation that applies to IoT devices and to any proposed new consumer guarantee of 'reasonable security' for digital products.*

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 unauthorized access, modification or disclosure. While the Attorney-General's *DP* supported retaining a principles-based and technology security principle, it canvassed proposals for increasing the certainty of the 'reasonable steps' test. In particular, the *DP* included the following proposals:

- Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.
- Include a list of factors that indicate what reasonable steps may be required.[334]

We support the proposals for introducing amendments to increase the certainty of the 'reasonable steps' test. However, given the importance of enhancing data security, especially in relation to IoT devices, we consider that it is important to ensure that security requirements imposed by distinct legal regimes are coherent and cohesive. To address the problems of regulatory inconsistency regulating new technologies, the World Economic Form (WEF) has recommended applying the concept of 'joined-up regulation'. As the WEF puts it:

> While individual regulations may be designed and administered in a proportionate way, gaps and overlaps with other regulations may lead to worse policy outcomes, while creating unnecessary complexity, cost and delay. The use of common analytical approaches and models for all regulatory impact assessments can support a better understanding of the cumulative impacts of different regulations.[335]

The techniques recommended by the WEF for implementing 'joined-up regulation' include conducting joint horizon scanning, developing machine-consumable regulation or integrating common standards into regulations.[336]

This report has recommended introducing mandatory minimum security standards for consumer IoT devices either by general cyber security legislation or by legislation introduced to regulate the security of consumer IoT devices (see Recommendations 1 and 2 above). The report has also proposed introduced a new consumer guarantee of reasonable security for digital products (see

[334] DP, p. 146.
[335] World Economic Forum (WEF), Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators (December 2020), p. 40.
[336] Ibid.

Recommendation 6 above). In doing so, we suggested that the potential for inconsistency could be minimised by expressly linking a guarantee of reasonable security of IoT devices to a *sui generis* law introducing mandatory security standards for such devices. Similarly, in relation to the application of APP 11.1, certainty could be enhanced by expressly linking the data security principle to both minimum mandatory standards under a *sui generis* law and a consumer guarantee of reasonable security. In any case, we recommend that the principle of 'joined-up regulation' should be applied to data security for consumer IoT devices by, for example, including references to common technical standards across regulatory regimes.