Strengthening Australia's cyber security regulations and incentives

Submission by:

Dr Evana Wright, Faculty of Law, University of Technology Sydney
Professor David Lindsay, Faculty of Law, University of Technology Sydney
Dr Genevieve Wilkinson, Faculty of Law, University of Technology Sydney
Dr Henry Fraser, Queensland University of Technology
Neva Collings, Faculty of Law, University of Technology Sydney

UTS CRICOS 00099F

Introduction

This submission was prepared by: Dr Evana Wright, Professor David Lindsay, Dr Genevieve Wilkinson and Neva Collings from the Faculty of Law, University of Technology Sydney; and Dr Henry Fraser, Queensland University of Technology and ARC Centre of Excellence for Automated Decision Making and Society.

The submission builds on research completed for a project entitled “Regulating to Protect Security and Privacy in the Internet of Things (IoT)”, which is 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*. The project focusses on developing recommendations for best practice regulation to promote security, privacy and consumer protection in relation to consumer IoT devices.

The researchers appreciate the opportunity provided by the discussion paper to give feedback on how the Australian Government can incentivise businesses to invest in cyber security, including through possible regulatory changes. Given the focus of the research project, this submission does not attempt to address every issue raised by the discussion paper but concentrates on providing feedback on those questions that are most relevant to enhancing the security of consumer IoT devices. The submission therefore does not seek to provide feedback on governance standards for large businesses (Chapter 4) or health checks for small businesses (Chapter 9). Nevertheless, as the broader regulatory environment for promoting cyber security must be taken into account in developing proposals for improving the security of consumer IoT devices, this submission includes recommendations relating to reforms aimed at enhancing cyber security more broadly.

Chapter 2: Why should the government take action?

Question 1. What are the factors preventing the adoption of cyber security best practice in Australia?

Question 2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

Concerns that regulation may inhibit innovation, particularly security enhancing innovation, has limited the adoption of measures to ensure cyber security best practice. The Australian approach to date has been to rely on industry self-regulation and the use of 'soft law', such as voluntary codes.[1] However, voluntary measures such as industry codes tend to only work best where the incentives for industry participants, such as manufacturers or suppliers, to comply align with the public interest in minimising harm.[2] These 'soft law' mechanisms however tend not to work well in situations where private incentives and public benefit conflict.[3] As noted in the Home Affairs Discussion Paper, there are 'weak commercial incentives' for businesses to invest in cyber security.[4] Therefore, manufacturers and suppliers are unlikely to act in the absence of regulation. This market failure requires government intervention to remedy and ensure that best practice cyber security measures are adopted in Australia.

Consumers do not have sufficient information to make informed choices regarding security. Information asymmetries mean that consumers are unable to satisfactorily determine whether a product or service is secure or presents a risk. While measures to educate consumers or provide further guidance on cyber security may go some way to addressing the risk presented by information asymmetries, this is insufficient. Manufacturers and suppliers of products, such as consumer IoT devices, are best placed to address cyber security risks that arise from use of their products and associated services and regulation is necessary to secure the participation of manufacturers and suppliers in adopting best practice cyber security measures.

The cost of cyber security breaches to consumers and society in general reinforces the need to take action. This is particularly true for consumer IoT devices, also known as smart devices, where cyber security vulnerabilities not only result in individual harm but also create system-wide risks of attacks that may be launched by networks of insecure devices.[5]

[1] 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.
[2] OECD, *Industry Self-Regulation: Role and Use in Support Consumer Interests*, DSTI/CP(2014)4/FINAL (OECD, 23 March 2015) 20-23. <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2014)4/FINAL&docLanguage=En>.
[3] Ibid.
[4] Australian Government, Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: A call for views* (2021) 10.
[5] UK Government, Department for Digital, Culture, Media & Sport (DDCMS), *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (2018).

Chapter 3: The current regulatory framework

Question 4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

Cyber security regulation

The regulatory challenges posed by consumer IoT devices cut across many of the most pressing issues relating to reform of Australian data security, consumer and privacy laws. It is our submission that Australia should develop, in consultation with stakeholders, a comprehensive and holistic cyber security regime which incorporates a set of principles aimed at improving cyber security. While enhancing the security of consumer IoT devices is a priority, this cannot be achieved in isolation from the broader cyber security environment and a holistic approach is called for.

Comprehensive cyber security legislation could establish mandatory minimum security standards or principles. While the relevant security standards will differ across industries or sectors it is important that cyber security regulation not be limited to one area such as consumer IoT devices. Cyber security risk is clearly not confined to one industry or use case and a comprehensive approach to addressing vulnerabilities across networks and devices could operate to reduce overall cyber security risk.

It addition, it is imperative to maintain coherence and consistency across the various regimes that apply to the regulation of cyber security. In addition to omnibus cyber security legislation, enhanced privacy laws and consumer protections are critical to ensuring comprehensive protection against cyber security risks. For example, consumer protections under the Australian Consumer Law (ACL) and privacy protections relating to data security under the Australian Privacy Principles (APPs) could be linked to security standards established under cyber security legislation.

In summary, we therefore recommend the following regulatory reforms to incentivise business to improve cyber security standards:

1. Our preference is for the introduction of general cyber security legislation aimed at enhancing cyber security standards across business sectors. This would extend beyond legislation, such as that proposed in the UK, aimed specifically at enhancing the security of consumer IoT devices and potentially extend, for example, to regulating industrial IoT. 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. Omnibus cyber security legislation could establish baseline standards that could be used to enhance coherency and consistency across regulatory regimes, including the privacy and consumer protection regimes. Consideration would, however, need to be given to determining which regulator might be best placed to have responsibility for such a regime.

2. In the absence of omnibus cyber security regulation, legislation – such as that proposed in the UK – should be introduced aimed specifically at enhancing the cyber security of consumer IoT devices. This legislation should, at a minimum, establish the regulatory framework for mandating minimum security standards, such as by mandating compliance with a Code of Practice, and regulating a labelling scheme. As with the

recommendation for a more general regime, consideration needs to be given to determining an appropriate regulatory authority.

3. Regardless of whether the above two proposals are introduced, attention is needed to improve coherency and consistency across current regulatory silos. As the discussion paper emphasises, security can be enhanced by improving industry certainty about what is required for regulatory compliance. As this submission explains, there are areas of considerable uncertainty about how our current regimes – including the data privacy and consumer protection laws – apply to consumer IoT devices. Measures, such as those identified in this submission, are therefore required to improve the clarity and consistency of existing laws.

Some of the regulatory measures that we suggest should be introduced as part of a comprehensive cyber security regime are summarised below and are discussed in greater detail throughout this submission.

Mandatory security standards for consumer IoT devices

The considerations supporting the introduction of mandatory security standards for consumer IoT devices in place of a voluntary code are explained in our responses to Chapter 2 and Chapter 6. In implementing the proposed mandatory standards, we submit that Australia should not adopt the ETSI standard wholesale. Instead, Australia should:

- draw lessons from the ETSI standard and other globally recognised sources of best practice;
- make improvements to the current Code of Practice;
- flesh out guidance on the principles set out in the Code of Practice; and then
- mandate all of the principles in the Code of Practice in a staged process.

Consumer product labelling

This submission recommends the introduction of a mandatory consumer labelling or trust mark scheme as part of either a comprehensive regime to regulate cyber security or a specific law dealing with security of consumer IoT devices.

In the absence of comprehensive cyber security regulation, consumer labelling should be introduced in conjunction with mandatory security standards for consumer IoT devices (as outlined in our responses to Chapter 6).

Strengthening the Privacy Act

The following reforms to the *Privacy Act 1988* (Cth) should be adopted in line with the recommendations of the Digital Platforms Inquiry:

- amend the statutory definition of 'personal information' to extend to technical data and other online identifiers; and
- strengthen the notice and consent provisions to meet 'best practice standards'.

The Australian government should also adopt more substantial reforms to the Privacy Act such as introducing a direct right to bring actions for interferences with privacy under the Privacy Act, including for breaches of privacy codes, as well as an enforceable principle of privacy by design and by default, such as that incorporated in article 25 of the GDPR.

We also support the introduction of cyber security codes under the Privacy Act with different codes established for industry sectors such as: network providers, including telecommunications carriers and ISPs; consumer smart device manufacturers and

suppliers; entities in the financial industry, including banks and credit providers; and educational service providers, including universities.

Reforming the Australian Consumer Law

The following reforms to the ACL should be considered:

- a new *sui generis* category for digital products, distinct from 'goods' and 'services', should be introduced. This new category would allow for consumer guarantees to be specifically tailored to reflect the expectations that consumers might reasonably have for hybrid, connected devices. A new category would also reduce uncertainties in determining whether a consumer IoT device, or elements of the device, are 'goods' or 'services'.
- amendments to the ACL to clarify that the statutory product safety regime applies to protect against insecure products. Legislative amendments could include amendments to the definition of a 'safety defect' and amendments to relevant defences, such as the 'no defect at time of supply' defence.

Furthermore, a new general consumer safeguard should be included to the ACL in the form of a general prohibition of unfair trading, which could provide recourse against some predatory and manipulative conduct associated with data-driven business models.

Chapter 5: Minimum Standards for personal information

Question 8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

Under Part IIIB of the Privacy Act, the Australian Information Commissioner can approve and register codes that are developed by APP entities at their own initiative or on request from the Commissioner. The main purpose of a code is to provide guidance as to how one or more of the APPs is to be complied with.[6] A code may, however, impose requirements over and above those specified in the APPs, and may cover exemptions from the Privacy Act. Therefore a code can incorporate standards that are higher than those required by the Privacy Act.

The Privacy Act establishes minimum standards for data security in APP 11. APP 11 requires an APP entity that holds personal information to take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. The standard set by APP 11 therefore relates to 'personal information security'.

One advantage of a code is the ability to draw on the experience and knowledge of industry to ensure that data security rules are appropriate and adapted to current industry practice. Codes can provide greater certainty to industry as to how to comply with the APPs. In addition, privacy codes can provide higher levels of protection to personal information than the APPs. We therefore consider there is a case for the Information Commissioner to request industry sectors to develop privacy codes aimed at enhancing cyber security (noting that a request cannot require a code to deal with exempt acts or practices).[7]

There are, nevertheless, limits to how effective privacy codes may be in promoting the uptake of cyber security standards in isolation from other measures. While the Privacy Act (and especially APP 11) is concerned with protecting personal information security, promoting cyber security extends well beyond this to include the security of devices and network security. In addition, a code may not apply to small business operators. As explained in our response to Chapter 3, we therefore consider there is a case for introducing broader cyber security legislation, which would address gaps in the current regulatory regime. Such legislation could include provision for cyber security codes.

Given the different security requirements in different industry sectors, it is doubtful whether a single privacy code will be sufficiently specific to provide the required certainty. If it is considered advisable to use codes under the Privacy Act as a means for improving cyber security, we therefore suggest that codes be developed for specific industry sectors.

As we are recommending the development of a comprehensive and holistic cyber security regime, it is important that laws regulating cyber security be coherent and

[6] Office of the Australian Information Commissioner (OAIC), *Guidelines for Developing Codes,* Issued under Part IIIB of the Privacy Act 1988, [1.11].
[7] *Privacy Act 1988* (Cth), s 26E(6).

consistent. Ensuring consistency across relevant laws may well require some additions to the APPs, or amendments to APP 11.

The introduction of cyber security codes under the Privacy Act would extend the OAIC's role in promoting cyber security. For this arrangement to be effective, it is necessary for the OAIC to be effectively resourced. Similarly, the effectiveness of cyber security codes depends upon the effectiveness of an enforcement regime. As explained in our response to Chapter 10, we support the introduction of a direct right of action for breaches of the Privacy Act, including for breaches of privacy codes.

Question 9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

Industry requires certainty about how to comply with regulations aimed at improving cyber security. It is evident that APP 11, even when combined with guidance on securing personal information from the OAIC,[8] is not currently providing sufficient certainty on steps to take to enhance cyber security.

As explained in our responses to Chapter 3, our preference is for the introduction of an omnibus cyber security law, which incorporates a set of principles aimed at improving cyber security. Cyber security principles alone, however, do not provide sufficient certainty on how the principles should be implemented in practice. One way of increasing certainty is to link laws or regulations to relevant technical standards. That said, the process for developing (and amending) technical standards is different to the process for developing legislation, including delegated legislation.

We therefore suggest that compliance with mandated cyber security principles could be satisfied by compliance with either nominated technical standards or delegated legislation, such as regulations (see responses to Chapter 6 below). If, however, compliance with specific technical standards were to be mandated, some regulatory mechanism must be established for determining the applicable standard or standards, and ensuring that it is adequate.

Question 10. What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

As explained above, we consider the security requirements in different industry sectors are sufficiently distinctive to require the development of codes for particular industry sectors. Without attempting to be exhaustive, the industry sectors that may require distinct cyber security obligations may include: network providers, including telecommunications carriers and ISPs; consumer smart device manufacturers and suppliers; entities in the financial industry, including banks and credit providers; and educational service providers, including universities.

[8] Office of the Australian Information Commissioner, *Guide to securing personal information: 'Reasonable steps' to protect personal information,* June 2018 (currently under review).

Chapter 6: Standards for smart devices

Question 11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

It is our submission that legislation should be introduced to regulate the security of consumer IoT devices (or smart devices) either as part of a comprehensive cyber security regime or as standalone legislation. In relation to smart devices, this legislation should:

- impose mandatory minimum obligations requiring compliance with security principles set out in the Code of Practice and/or designated technical standards; and
- require compliance with all principles set out in the Code of Practice (or standards) or alternatively, implement the requirements in phases with the first phase requiring compliance with the top 3 principles with other principles becoming mandatory in later phases (in order of priority).

The current experience in Australia has demonstrated that the voluntary Code of Practice is insufficient to ensure best practice approaches to cyber security and privacy. As set out in the Discussion Paper, research indicates that IoT providers 'find it difficult to implement voluntary, principles-based guidance.'[9] This experience is not unique to Australia. The United Kingdom also found limited uptake or compliance with the voluntary Code of Practice introduced in 2018 and will move to introduce legislation that will mandate compliance with certain security principles.[10] In addition to the United Kingdom, a number of other jurisdictions have led the way in regulating IoT cyber security including the United States of America (federally and in the states of California and Oregon) and Singapore.

Why legislation?

As observed above, voluntary measures work best where incentives for industry participants, such as IoT manufacturers or suppliers, to comply align with the public interest in minimising harm. Generally, these 'soft law' mechanisms do not work well in situations where private incentives and public benefit conflict.[11] The cost to society and, in particular, consumers is sufficient to warrant action in this area and the introduction of legislation will facilitate compliance by providing a framework of minimum standards. Given the weak incentives for consumer IoT device manufacturers to invest in cyber security, government intervention is necessary to address the market failure. This is reflected in the reasons given by the UK government for introducing legislation to mandate security requirements in relation to consumer IoT devices.[12] As Bellman and van Oorschot put it:

---

[9] Department of Home Affairs, *Voluntary Code of Practice: Securing the Internet of Things for Consumers* (Web Page, 13 July 2021) <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice>.

[10] UK Government, 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>.

[11] OECD, *Industry Self-Regulation: Role and Use in Supporting Consumer Interests,* DSTI/CP(2014)4/FINAL (OECD, 2015).

[12] UK Government, 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>.

> It seems quite apparent that self-regulation of the IoT industry has been largely unsuccessful; this falls against the backdrop of a grand success of the overall software industry in disclaiming all liability for software flaws, despite itself falling far short of delivering products without security vulnerabilities.[13]

The cost to society and, in particular, consumers is sufficient to warrant action in this area and the introduction of legislation will facilitate compliance by providing a framework of minimum standards.

It is, nevertheless, important to be careful to ensure that regulation does not impede innovation. This may be achieved through the introduction of a flexible regulatory regime that appropriately balances cyber security protection and the need to promote technological innovation. For example, as proposed by the UK government, elements of the regulatory regime may be flexibly specified using tools such as delegated legislation.[14]

Australian cyber security legislation for IoT devices should therefore impose mandatory minimum obligations on relevant entities including manufacturers, distributors and suppliers of consumer IoT devices. These minimum obligations should require compliance with security principles set out in the Australian Code of Practice and/or equivalent designated technical standards (see discussion regarding mandatory standards below). Ideally, the legislation should require compliance with all 13 principles set out in the Code of Practice; however, a flexible approach to regulation may be to include a staged introduction of mandated security principles in order of priority starting with the first 3 principles, as proposed by the UK government.

Appropriate enforcement is critical to success.

The objectives of a regulatory regime aimed at enhancing the security of consumer IoT devices can be achieved only if it is accompanied by an appropriate enforcement regime. Therefore, in addition to introducing mandatory security standards, the Australian Government should also implement an appropriate enforcement regime. This enforcement regime should include arrangements for post-market investigation, monitoring and security auditing, as well as sanctions.

In designing an enforcement regime, it may be possible to draw on the approach being pursued in the UK. As proposed in the June 2020 UK government consultation on proposals for regulating the security of consumer IoT devices, an effective enforcement regime should include a tiered suite of enforcement and compliance measures, such as education and compliance guidance, compliance warnings, enforcement undertakings, enforceable notices and pecuniary penalties.[15] As the consultation document further acknowledged, the enforcement regime should be accompanied by appropriate investigatory and enforcement powers, including powers to test and monitor products, purchase and test products, enter and search premises and obtain search warrants.

---

[13] Christopher Bellman and Paul C. van Oorschot, 'Best Practices for IoT Security: What Even Does it Mean?' arXiv:2004.12179v1 [cs.CR] submitted 25 April 2020 <https://arxiv.org/pdf/2004.12179.pdf>.

[14] UK Government, 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>.

[15] UK Government, Department for Digital, Culture, Media & Sport, P*roposals for regulating consumer smart product cyber security – call for views* (6 June 2020) <https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views>.

Mandatory Standards (Option 2)

Question 12: Would ETSI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices?

There is much about ETSI EN 303 645 (the ***ETSI standard***) to recommend it. On balance, however, we submit that Australia should not adopt the ETSI standard wholesale. Instead, Australia should:

- draw lessons from the ETSI standard and other globally recognised sources of best practice
- make improvements to the current Code of Practice;
- flesh out guidance on the principles set out in the Code of Practice; and then
- mandate all of the principles set out in the Code of Practice in a staged process.

This part of the submission addresses some of the advantages of the ETSI standard, but gives reasons why each advantage does not clearly favour adopting the ETSI standard. Then, it explains some of the weaknesses of the Code of Practice and makes some recommendations to strengthen the Code.

The ETSI standard is built on European expertise, but adopting the standard is not a cheap shortcut

It is tempting to assume that adopting the ETSI standard would be an inexpensive way to leverage the policy analysis and experience of respected European regulators, and leapfrog straight to global best practice. That assumption is wrong. The Code of Practice was developed in a different regulatory context. European Standards are designed to 'support European legislation'[16] and the ETSI standard presumes the operation of overlapping and supporting regulations that are simply absent in the Australian context. For example, the ETSI standard does not need to emphasise privacy to the same extent as the Australian Code of Practice, because Europe's General Data Protection Regulation (***GDPR***) already affords much stronger and more widely applicable privacy protection than is available in Australia.

Accordingly, the Australian Code of Practice places greater emphasis on principles relating to data protection, with principle 5 dealing with the protection of personal data. The ETSI Standard defers discussion of data protection until provisions 5.8 and 6 and the UK Code of Practice deals with the subject in principle 8. The lesser emphasis on data protection in the ETSI standard and UK Code of Practice may be attributed to the more developed data privacy framework that may be relied upon in Europe. The European GDPR, while not beyond criticism, is a substantially more developed and rigorous privacy framework than that of the Australian *Privacy Act 1988* (Cth). Importantly, the ETSI standard relies upon additional rights arising under the GDPR, such as the right to erasure, that do not have an equivalent under Australian privacy law. For example, provision 5.11-2 of the ETSI standard deals with the ability to remove personal data from services and sets out the expectation that 'such functionality is compliant to applicable data protection law, including the GDPR'. Australia cannot rely on the strong privacy protections afforded by the GDPR, such as the right to erasure, and therefore needs to establish a Code of Practice that provides protections in relation to data protection over and above those provided under the Privacy Act.

[16] ETSI, *About ETSI* (Web Page) <https://www.etsi.org/about>.

Simply adopting ETSI wholesale, without developing Australian privacy law in parallel would therefore result in insufficient privacy protection. That said, as addressed in our responses to Chapter 10, there is currently a privacy law reform process underway in Australia.[17] It may conceivably be possible to align that reform in such a way as to make the ETSI standard work in the Australian context. But that would be no easy feat. Moreover, it should always be borne in mind that the GDPR assumes the background of the EU rights-based legal regime, which expressly recognises a right to data privacy.

The wholesale adoption of the ETSI standards would therefore pose significant challenges. We therefore support the development of a response that is better tailored to Australian circumstances, including the Australian legal and regulatory framework.

The ETSI standard is internationally recognised, but it is not the only internationally recognised standard

According to the discussion paper, participants in research on the effectiveness of the Code of Practice preferred that Government communicate its expectations of industry through internationally recognised standards. Certainly the ETSI standard is internationally recognised. The advantage of adopting the ETSI standards is that IoT providers who supply services or devices to the European market could be assured of no additional compliance cost in entering the Australian market. Australian consumers would benefit from any consequent marginal increase in supply or choice, or decrease in cost, of IoT devices.

While the ETSI standard has been adopted by the United Kingdom, other standards or frameworks have been adopted in other jurisdictions such as the United States. 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.'[18] 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.'[19] Similarly, the Oregon House Bill 2395 requires that manufacturers implement 'reasonable security features'.[20] 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).[21] It is likely that the NIST 'minimum security requirements' would also inform interpretation of 'reasonable security features' in the California and Oregon legislation. Given the size of the U.S. market and the fact that many consumer IoT devices are developed by U.S. companies the NIST standards may become significant across the industry as a whole.[22]

---

[17] The authors acknowledge that the Attorney General's Department is currently conducting a review of the *Privacy Act 1988* and this may result in Australia incorporating some of the additional rights that arise under the GDPR – such as the right to data portability, right to erasure, and the capacity to challenge automated decisions - into Australian privacy law. See Attorney-General's Department, *Privacy Act Review,* Issues Paper (October 2020).

[18] 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>.

[19] California Civil Code, Title 1.81.26 *Security of Connected Devices*, 1798.91.04(a).

[20] 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).

[21] 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).

[22] 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>.

On the other hand, the global response to Europe's GDPR, and Europe's potential leadership in developing regulation for artificial intelligence, indicates that Europe can be a global standard setter. Europe is certainly a sufficiently large and wealthy market that providers of IoT devices have a strong incentive to meet European standards as a matter of course.

Nonetheless, at this stage it is not clear that the ETSI standard will become globally influential or widely adopted to the extent that Australia obtains a meaningful advantage by adopting them, rather than other standards. 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 standards to follow. NIST standards on IoT cyber security are very highly referenced, as are standards from the non-governmental organisations, including GSMA, IETF and IEEE.[23] 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.

The ETSI standard is more detailed than the Code of Practice, but the Code of Practice could be supplemented by more detail and guidance

The discussion paper indicates that '[m]any firms are aware of the Code of Practice, but [have] found it difficult to implement high-level principles.'[24] One reason the ETSI standard might be preferred to the Code of Practice is that the ETSI standard provides more (and better) detail and guidance. The compliance checklist that accompanies the standard is a particularly useful tool. Even so, the ETSI standard is by no means comprehensive. It is, for example, certainly less detailed than other highly respected sources of cyber security guidance, such as the CIS Controls.[25]

We suggest that the best way of dealing with the difficulties experienced by firms in implementing the high level principles in the Code of Practice is to directly address the problem by issuing better guidance on implementation. This submission therefore makes recommendations on the guidance that might be provided immediately below.

Improving the Code of Practice

It is our submission that, Australia should mandate an improved version of the current Code of Practice, with additional guidance provided on implementation. Through this mechanism, many of the advantages of the ETSI standard might be realised without adopting the standard wholesale, simply by making some improvements to the Code of Practice and its guidance. We briefly set out below some key improvements that we suggest would help bring the existing Code of Practice principles in line with the ETSI standard and other internationally recognised sources of guidance. These recommendations are not meant to be exhaustive but, in our view, they address some of the main shortcomings of the current Code.

Improving the presentation and availability of the Code of Practice

The first step in improving the Code of Practice and its guidance has more to do with its presentation and ease of use, than its content. Unfortunately, the Code of Practice and guidelines are not easy to find and their presentation lacks coherence. The Australian Cyber Security Centre (ACSC) and the Department of Home Affairs are not fully

[23] Copper House, *Mapping Security & Privacy in the Internet of Things: Making sense of global IoT recommendations and standards and mapping them to the UK's Code of Practice for Consumer IoT Security* <https://iotsecuritymapping.uk/by-sector-and-body/>.
[24] Australian Government, *Strengthening Australia's cyber security regulations and incentives: A call for views* (2021) ('Discussion Paper') 31.
[25] Center for Internet Security, *CIS Controls v 8* (May 2021).

coordinated in providing information about the Code. A person wishing to access the Code and relevant guidance currently has to exercise considerable initiative to seek them out. The ACSC guidance is also presented without including the Code of Practice principles themselves. It assumes that a person who has found the guidance already has the principles to hand, which may not be the case. The 'friction' inherent in having to search online for the principles may deter stakeholders from giving them careful consideration side by side with the ACSC guidance.

Moreover, the guidance provided by the ACSC is very sparse and does not provide much detail. Take, for example, Principle 4 – Securely store credentials. The ETSI standard and other sources of guidance provide much more detail than the ACSC guidance on the kinds of credentials that require secure storage, and on appropriate storage mechanisms. Guidance for this principle should be improved to follow suit. To take another example, Principle 8 – Ensure software integrity also includes substantially less guidance on implementation than does the corresponding ETSI standard.

More generally speaking, a key advantage of the ETSI standard over the Australian Code of Practice is (as mentioned above) that the former includes a relatively detailed implementation checklist. A checklist of this kind, suitably adapted to the Australian Code, would assist stakeholders to comply with the Code of Practice.

Moreover, as noted above, the ETSI standard itself is not exhaustive in its detail. More detailed guidelines, of a kind similar to the APP guidelines issued by the Office of the Australian Privacy Commissioner,[26] have the potential to give stakeholders further assurance and clarity.

To remedy these problems, we recommend the following:

- The Department of Home Affairs and Australian Cyber Security Centre should collaborate to set up a dedicated website for the Code of Practice, aggregating all relevant government materials on the Code.
- The Code of Practice should be consolidated with the Australian Cyber Security Centre's guidance for manufacturers on 'How to Implement the IoT Code of Practice' and presented as a single document.
- The Department of Home Affairs and Australian Cyber Security Centre should develop more detailed guidance on the Code of Practice, similar in nature and level of detail to the OAICs APP Guidelines.
- Guidance on the Code of Practice should also include a checklist similar to the one included at the end of the ETSI standard.

Recommendation: Improving Principle 2 – Implement a vulnerability disclosure policy

The biggest shortcoming of the Australian Code of Practice principles is the insufficiency of requirements in relation to vulnerability disclosure in Principle 2. Principle 2 differs from the corresponding principle in the ETSI standard, and in the UK Code of Practice, in two main ways.

Firstly, the Australian principle fails to specify that vulnerability disclosure practices should include disclosure of vulnerabilities *by* IoT providers to affected persons and relevant authorities. Instead it emphasises measures that permit IoT users to report vulnerabilities to providers, such as bug bounties. The corresponding principle in the UK Code of Practice and in the ETSI standard (Provision 5.2-3) provide for both notification *by* users of vulnerabilities, and notification *of* users and authorities about vulnerabilities discovered by IoT manufacturers and service providers. The ETSI standard, as well as

[26] OAIC, *Australian Privacy Principles Guidelines,* July 2019.

guidance from ENISA, the US DHS and GSMA, suggests that best practice for such outward facing disclosure is 'Co-ordinated disclosure' with shared disclosure programs, and formal coordination between developers, manufacturers and service providers built on effective information sharing practices and platforms.[27]

Secondly, the corresponding parts of the ETSI standard, the UK Code of Practice, and other authoritative sources of guidance such as the CIS Controls situate vulnerability disclosure responsibilities within a broader obligation to continually monitor for, identify and rectify security vulnerabilities.[28] This element is missing from the Australian principle.

Principle 2 should therefore be amended to include the following language, taken from the UK Code of Practice:

> Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Vulnerabilities should be reported directly to the affected stakeholders in the first instance.[29]

Guidance connected with the principle should recommend co-ordinated vulnerability disclosure, as contemplated by the ETSI standard.

Recommendation: Code of Practice Principle 9 – Make systems resilient to outages

Principle 9 should be updated to include additional guidance that IoT devices and systems should, where reasonably possible, notify users of outages of power, network or associated services. This would reflect the guidance in ETSI, and ensure that users, especially users who rely on devices for health or similarly significant reasons, are able to appropriately manage risks posed to them by outages.

Recommendation: Code of Practice Principle 12 - Make installation and maintenance of devices easy.

Principle 12 refers to external documents in footnotes however it is not easy locate these documents. This is particularly the case for the referenced 'Accessibility and Inclusivity Guide'. Principle 12 should be updated to remove the footnotes. Instead, the Department of Home Affairs should add two sentences to the body of the principle, to the following effect:

> Australian Government best practice on security is set out in the Australian Cyber Security Centre's 'IoT Code of Practice: Guidance for Manufacturers', available at [insert URL]. Australian Government best practice on accessibility is set out in [insert agency name]'s [insert document name], available at [insert URL].

---

[27] ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements* (v2.1.1 2020-06) Provision 5.2; ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* (20 November 2017) <https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot>, GP-OP-06 'Coordinated disclosure of vulnerabilities' and GP-OP-07 'Participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about cyber threats and vulnerabilities from public and private partners.'; U.S. Department of Homeland Security, *Strategic Principles for Securing the Internet of Things* (Version 1.0, 15 November 2016) 7; *GSMA Coordinated Vulnerability Disclosure (CVD) Programme* <https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/>.

[28] ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements* (v2.1.1 2020-06) Provision 5.2-3; UK Government, Department of Digital, Culture, Media and Sport, *Code of Practice for Consumer IoT Security* (October 2018) Principle 2; Center for Internet Security, *CIS Controls v8* (May 2021) Control 7: Continuous Vulnerability Management.

[29] UK *Code of Practice for Consumer IoT Security* (October 2018), Principle 2.

Chapter 7: Labelling for smart devices

Question 16. What is the best approach to encouraging consumers to purchase secure smart devices? Why?

As explained in our responses to Chapter 2, under current regulatory settings there is little incentive for businesses to invest in cyber security and businesses are unlikely to act to address security risks in the absence of legislation. However, there are measures that may be adopted to encourage consumers to purchase secure smart devices. This submission recommends the introduction of a consumer labelling or trust mark scheme as an element of any comprehensive regime to regulate cyber security or of a specific law dealing with security of consumer IoT devices.

Consumer awareness of security vulnerabilities

As discussed in response to questions 1 and 2 above, information asymmetries mean that consumers are unable to determine whether a product or service is secure or not. Thus, consumers may unknowingly purchase or use products that pose cyber security risks.[30] The functionality and security of data accessed by smart devices can be intercepted and compromised or impeded. Such breaches of security and privacy can lead to identity theft and crime, physical harm if devices are caused to fail, and loss of privacy.

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.[31] 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.[32]

The lack of consumer awareness of security and privacy features of smart devices limits commercial incentives for manufacturers to compete on cyber security.[33] It is important to ensure that consumers are aware of the cyber security risks associated with smart devices because consumer confidence is critical to ensure the uptake of smart devices. Consequently, ensuring that consumers have sufficient information to make better informed decisions is of utmost importance.

Value of product labelling

Product labelling may promote consumer awareness of the safety and security issues with products and facilitate the exercise of a 'more informed' choice by consumers. Surveys conducted in the UK demonstrate people are significantly more likely to select

[30] Australian Government, Department of Home Affairs, *Strengthening Australia's cyber-security regulations and incentives: a call for views* (2021) 30.
[31] Harris Interactive, *Consumer Internet of Things Security Labelling Survey Research Findings,* 3.
[32] 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>.
[33] Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T. W. Wong, 'The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay' (2020) 15(1) *PLoS One* 1, 2.

a device that carries a label than one that does not, with the obvious exception of a label that implies weak security.[34] A survey commissioned by the Finnish Transport and Communications Agency found that 'approximately 80% of consumers in Finland would be influenced by a well-known and reliable information security label.'[35] Another recent study suggests that, after controlling for price and functionality, security labels can have a positive effect on consumer choices and that consumers are willing to pay more for devices with a security label.[36]

Voluntary or mandatory labelling?

As observed in the Discussion Paper, voluntary labelling schemes are currently in operation or being developed in a number of jurisdictions including Singapore,[37] Finland,[38] the United Kingdom[39] and the U.S.[40] However, as discussed above in relation to security standards (see responses to Chapter 2 and Chapter 6), voluntary schemes are less effective in environments where there is conflict between public and private interests. In the absence of requirements or incentives to build security into the design of smart devices, security may not be considered a high priority for manufacturers and smart devices are frequently deployed without basic in-built security.[41]

The introduction of a regulatory regime that promotes safety, security and privacy of smart devices is required beyond current standards under existing consumer laws, privacy law, and voluntary codes of practice. Minimum standards are needed to ensure devices are safe, secure and protect privacy by design (see responses to Chapter 6 and Chapter 10 above). Part of this regulatory regime should include a consumer labelling or trust mark scheme where industry and consumers are engaged in developing the standards and certification processes together with targeted consumer and industry education.

It is our submission, to address problems such as industry compliance, that a labelling scheme should be a mandatory element of a regulatory regime. Any mandatory labelling scheme must also be properly resourced to ensure satisfactory testing, certification and enforcement. This could include a role for an independent body such as that established in Singapore and proposed for the UK, which evaluates and rates products according to criteria that assist consumers with exercising informed choices concerning risk.

[34] Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T. W. Wong, 'The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay' (2020) 15(1) *PLoS One* 1, 1, 6.
[35] Tietoturva (Cybersecurity), *Research on consumer views on cybersecurity* (Web Page) < https://tietoturvamerkki.fi/en/for-companies/>.
[36] Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T. W. Wong, 'The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay' (2020) 15(1) *PLoS One* 1, 2.
[37] See CSA Singapore, *Cybersecurity Labelling Scheme (CLS)* (Web Page) < https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls>
[38] See Finnish Transport and Communications Agency (TRAFICOM) National Cyber Security Centre Finland (NSCS-FI), *Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products* (Web Page, 26 November 2019) < https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label>. See also, Tietoturva (Cybersecurity), *What is the Finnish Cybersecurity Label?* (Web Page) < https://tietoturvamerkki.fi/en/>.
[39] See the following voluntary certification schemes: *Internet of Toys Certification Scheme* <https://iotoys.org.uk/#:~:text=The%20scheme%20is%20intended%20for,of%20vulnerabilities%20in%20children's%20toys.>; *SafeShark - Cyber security certification* < https://safeshark.co.uk/>; *IASME IoT Security Assured* <https://iasme.co.uk/internet-of-things/>.
[40] See The White House, *Executive Order on Improving the Nations Cybersecurity* (Presidential Actions, 12 May 2021) Sec 4 Enhancing Software Supply Chain Security paras (s)-(u).
[41] Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T. W. Wong, 'The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay' (2020) 15(1) *PLoS One* 1, 2.

Question 17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

Labels are unlikely to be sufficient to address security concerns in the absence of additional regulatory reform. Even the most effective consumer labelling scheme can only have some effect on improving consumer decision-making[42] and therefore, in our submission, a consumer labelling or trust mark scheme should form one part of a broader suite of cyber security regulation (as outlined in responses to Chapter 3 above).

In the absence of comprehensive cyber security regulation, consumer labelling should be introduced in conjunction with mandatory security standards for smart devices (as outlined in responses to Chapter 6 above). Both consumer labelling and security standards are required to address the information asymmetries and market failure identified above (see responses to questions 1 and 2). 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.'[43] It is likely that this holds true for both privacy and security concerns.

Question 18: Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?

Issues with voluntary schemes

In our view, it is unlikely that there will be sufficient industry uptake of a voluntary label for smart devices. The voluntary Code of Practice: Securing the Internet of Things for Consumers provides a useful comparator here. As set out in the Discussion Paper, the voluntary Code of Practice has had little impact on the lower-cost end of the market for smart devices and, while many firms are aware of the Code, implementation of the principles into practice is limited.[44] Similarly in the United Kingdom, despite having a voluntary Code of Practice in place since 2018, the UK Government has recently moved to introduce mandatory security requirements stating, '…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.'[45] Manufacturers of consumer IoT devices are more likely to compete on price and other features rather than security[46] and thus, there is less incentive to participate in a voluntary labelling scheme. As observed by Bellman and van Oorschot, '[i]t seems quite apparent that self-regulation of the IoT industry has been largely unsuccessful.'[47]

---

[42] Elise Golan, Fred Kuchler, Lorraine Mitchell, Cathy Greene and Amber Jessup, 'Economics of Food Labeling' (2001) 24(2) *Journal of Consumer Policy* 117.
[43] 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>.
[44] Australian Government, *Strengthening Australia's cyber security regulations and incentives: A call for views* (2021) 31.
[45] UK Government, 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>.
[46] Australian Government, *Strengthening Australia's cyber security regulations and incentives: A call for views* (2021) 11, 30.
[47] Christopher Bellman & Paul C. van Oorschot, 'Best Practices for IoT Security: What Even Does it Mean?' arXiv:2004.12179v1 [cs.CR] submitted on 25 April 2020 <https://arxiv.org/pdf/2004.12179.pdf>.

A mandatory labelling scheme is required

A mandatory labelling scheme has the potential to provide necessary information to enable more-informed decision making by consumers and is unlikely to inhibit product innovation or entry of new companies into the market when compared to other regulatory options. By impacting consumer behaviour directly, a labelling scheme also has the potential to incentivise industry to compete. To maximise industry buy-in, we therefore suggest that a co-regulatory labelling scheme should be pursued with industry highly engaged in the development of the scheme. Given that industry has more information about smart devices than a central regulator it is more likely to know what information consumers may need and failure to engage with industry may result in under-compliance. That said, given the heterogeneous nature of manufacturers and sellers of smart devices we see a need for government to be involved to address the coordination and enforcement problems associated with industry self-regulation. As the success of a labelling or trust mark scheme will depend on cooperation and trust between regulators and manufacturers/suppliers of smart devices, we believe that a co-regulation approach would provide the best framework for introducing an effective labelling scheme.

Question 19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

Consumer labelling for smart devices should not be limited to providing information on the expiry of security updates. The proposal to use 'security expiry date labels' relies on the assumption that expiry dates may act as a proxy for security when instead this may be considered a 'tick a box' exercise that does not actually result in any meaningful improvement in security of smart devices. Instead, consumer labelling should provide additional information to allow for comparison between products across a number of features. This should include information on: security standards met by the device; whether there are inbuilt privacy safeguards; what personal information may be collected and how that information may be stored/deleted; how personal data may be shared; as well as information on security update expiry dates.

The purpose of labelling should be to not only convey information to the consumer but also to drive improvement in security and privacy across the Internet of Things by encouraging manufacturers and suppliers to change their business practices in response to consumer demand and competition. As noted in the Discussion Paper, research undertaken in the UK indicated that use of a mandatory trust mark 'would reduce the probability of breaches on smart devices by between 10 and 50 per cent and that 15 per cent of consumers would switch to more secure devices over a 10-year period.'[48]

Question 21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Consumer labelling could include QR codes that can be applied to physical products and link to further detailed information on security and privacy matters. Digital labelling using a QR code alone, however, is unlikely to be sufficient. Research in the United Kingdom has recognised that labels that require additional action by the consumer, such as scanning a QR code, are 'likely to be less effective in communicating security information'.[49] Information therefore should be made available to a consumer on a

[48] Australian Government, *Strengthening Australia's cyber security regulations and incentives: A call for views* (2021) 40.
[49] Harris Interactive, *Consumer Internet of Things Security Labelling Survey Research Findings,* 24.

physical label that does not require the consumer to have access to another device such as a smart phone. This is important to ensure that information is accessible to all consumers. That said, there is clearly a role for the 'layered' presentation of consumer information.

This question directs attention to the central importance of design decisions in ensuring the effectiveness of any labelling scheme. Consumer engagement, such as by surveys, is therefore essential to determine the most appropriate and effective forms of labelling including trust marks and digital labels.

Chapter 8: Responsible disclosure policies

Question 22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

The following considers responsible disclosure policies in relation to consumer IoT (smart) devices and builds upon submissions made in response to the questions in Chapter 6 above. It is our recommendation that responsible disclosure policies should address both inward and outward facing notification of security vulnerabilities, consistent with principles of 'coordinated disclosure' as endorsed by the ETSI standard, the UK Code of Practice, and the CIS Controls.[50] Such requirements should be incorporated as part of the mandatory security standards proposed in our responses to Chapter 6 above.

The Australian Code of Practice currently emphasises inward facing notification of security vulnerabilities with a focus on notice *from* the public to manufacturers, service providers and app providers. In comparison, the UK guidance[51] and the ETSI standard[52] goes beyond the Australian principle by addressing outward facing disclosure: measures that manufacturers, service providers and app developers can take to notify affected stakeholders, national authorities and industry bodies of vulnerabilities. Both kinds of notification – from the public and to the public – are important elements of vulnerability disclosure. Therefore, in our view disclosure policies should cover both inward and outward facing disclosures. The current proposal to focus on responsible disclosure *by* security researchers *to* developers, manufacturers and potentially the government is insufficient to address the risks posed by software vulnerabilities.

The ETSI standard, as well as guidance from ENISA, the U.S. DHS and GSMA, relies on principles of 'coordinated disclosure' with shared disclosure programs, and formal coordination between developers, manufacturers and service providers built upon effective information sharing practices and platforms.[53] Consistent with the ETSI Standard, the UK Code of Practice and the CIS Controls, vulnerability disclosure should form part of a broader set of responsibilities to continually monitor for, identify and rectify security vulnerabilities.[54]

---

[50] ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements* (v2.1.1 2020-06) Provision 5.2-3; UK Government, Department of Digital, Culture, Media and Sport, *Code of Practice for Consumer IoT Security* (October 2018) Principle 2; Center for Internet Security, *CIS Controls v8* (May 2021) Control 7: Continuous Vulnerability Management.

[51] UK Government, Department of Digital, Culture, Media and Sport, *Code of Practice for Consumer IoT Security* (October 2018) Principle 2.

[52] ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements* (v2.1.1 2020-06) Provision 5.2.

[53] ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements* (v2.1.1 2020-06) Provision 5.2; ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* (20 November 2017) <https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot>, GP-OP-06 'Coordinated disclosure of vulnerabilities' and GP-OP-07 'Participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about cyber threats and vulnerabilities from public and private partners.'; U.S. Department of Homeland Security, *Strategic Principles for Securing the Internet of Things* (Version 1.0, 15 November 2016) 7; *GSMA Coordinated Vulnerability Disclosure (CVD) Programme* <https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/>.

[54] ETSI EN 303 645 *Cyber Security for Consumer Internet of Things: Baseline Requirements* (v2.1.1 2020-06) Provision 5.2-3; UK Government, Department of Digital, Culture, Media and Sport, *Code of Practice for Consumer IoT Security* (October 2018) Principle 2; Center for Internet Security, *CIS Controls v8* (May 2021) Control 7: Continuous Vulnerability Management.

Chapter 10: Clear legal remedies for consumers

Question 26. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

As explained in the discussion paper, there are considerable challenges and uncertainties in applying the *Australian Consumer Law* ('ACL') to digital products, such as consumer IoT devices. The challenges arise from the distinctive nature of these products and devices. 'Smart devices', such as consumer IoT devices, are complex hybrid products consisting of hardware, software, data and associated services. As explained further below, there are uncertainties about whether the supply of a device, or elements of a device, amounts to the supply of a 'good' or a 'service'. Moreover, the complexity of the supply chain, with multiple businesses being involved in the supply of elements of a device, can create difficulties in determining who is liable for security defects. In addition, connected devices are subject to change over time due to software upgrades, including security upgrades. The devices may therefore be secure at the point of sale, with security defects only subsequently emerging. Finally, non-technical users encounter difficulties in understanding or determining the source of defects.

The complexity of the law applying to liability for defective products (potentially including security flaws), which in the past has been described as a 'legal morass',[55] can be illustrated by the range of actions that are possible against manufacturers (which can include importers):

- Breach of the ACL for making false or misleading representations about the safety or security of a product.
- Breach of the consumer guarantees of acceptable quality or fitness for purpose.
- An action against the manufacturer (or importer as 'deemed manufacturer') where goods have a 'safety defect', as defined in the product liability regime under the ACL; or
- An action for damages for breach of implied conditions as to merchantable quality or fitness for purpose implied into a contract under the Sale of Goods regime, or a common law claim for negligence.[56]

This submission focusses on the consumer guarantees and the product liability regime and proposes the following reforms to the ACL:

- A new *sui generis* category for digital products, distinct from 'goods' and 'services' should be introduced to the ACL. This new category would allow for consumer guarantees to be specifically tailored to reflect the expectations that consumers might reasonably have for hybrid, connected devices. A new category would also reduce uncertainties in determining whether a consumer IoT device, or elements of the device, are 'goods' or 'services'.

[55] See Luke R. Nottage and Jocelyn Kellam, 'Happy 15th Birthday, Part VA TPA! Australia's Product Liability Morass' (2007) *Competition and Consumer Law Journal* 15; Jocelyn Kellam, Stuart C. Clark, and Mikhail Glavac, 'Theories of product liability and the Australian Consumer Law' (2013) 21 *Competition and Consumer Law Journal* 1.
[56] See Jeannie Marie Paterson, *Corones' Australian Consumer Law* (4th ed, Lawbook Co., 2019) p. 521.

- Introduce amendments to the ACL to clarify that the statutory product safety regime applies to protect against insecure products. Both consumers and manufacturers need greater certainty about how the product safety regime may apply to IoT products. Legislative amendments could include amendments to the definition of a 'safety defect' and amendments to relevant defences, such as the 'no defect at time of supply' defence.

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 apply where a consumer purchases goods and services ordinarily acquired for personal, domestic or household use.[57]

Application of statutory consumer guarantees to consumer IoT devices

Of the statutory guarantees established under the ACL, the following are potentially the most relevant to ensuring the security 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
- a supplier guarantees that services will be rendered with due care and skill.

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'.[58] While acknowledging that UK consumer law 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'.[59]

Given the hybrid nature of consumer IoT devices, difficulties can arise in determining whether a product is a good and/or a service and, accordingly, which guarantees apply.[60] Some of the complexities involved in determining whether a complex digital product is a good or service arose in *Valve (No 3)*.[61] As Edelman J (at first instance) pointed out, the relationship between the definitions of 'goods' and 'services' is dealt with in the definition of 'services', which includes 'any rights (including rights in relation to, and interests in, real or personal property), benefits, privileges or facilities that are, or are to be, provided, granted or conferred in trade or commerce'.[62] However, as the definition specifically excludes 'rights or benefits being the supply of goods or the performance of work under a contract', as Edelman J concluded, a transaction must first be characterised to determine if it is a supply of 'goods'.[63] Moreover, once a transaction has been

[57] ACL s 3 (definition of 'consumer' (1)(b)).
[58] Consumer Affairs Australia and New Zealand (CAANZ), *Australian Consumer Law Review: Final Report* (March 2017) ('ACL Review Final Report') 96.
[59] Ibid.
[60] Benjamin Hayward, 'What's In A Name? Software, Digital Products and Sale of Goods' (2016) 38 *Sydney Law Review* 441.
[61] *Australian Competition and Consumer Commission v Valve Corporation (No 3)* [2016] FCA 196 ('Valve (No 3)').
[62] ACL, s 2 (definition of 'services' (a)).
[63] Valve (No 3) [131].

characterised as a supply of 'goods', the effect of the exception to the definition of 'services' is that the transaction as a whole will not involve the supply of a service.[64]

As the definition of 'goods' includes software, in most cases the supply of a consumer IoT device will be a supply of 'goods', even if the product also includes a mixed supply of software and associated services. That said, there is some continuing uncertainty where goods are incidentally supplied as part of the supply of a service, such as antibiotics supplied as part of the supply of medical services. While transactions such as these were characterised as the supply of services under the *Trade Practices Act 1974* (Cth), in *Valve (No 3)* Edelman J questioned whether, given the exception in the definition of 'services' in the ACL, any 'incidental' supply of goods whatsoever might properly be described as the supply of goods.[65]

Consumer IoT devices and the guarantee of acceptable quality

Apart from uncertainties about whether a product may be categorised as a good or service, there are uncertainties about the application of the guarantees to consumer IoT devices. For example, the guarantee of acceptable quality requires that, among other things, goods must be free from defects and safe. This, however, is subject to the 'reasonable consumer test', so that goods will meet the standard if a reasonable consumer, who is fully acquainted with the state and condition of the goods (including any hidden defects), would regard as acceptable having regard to a number of listed statutory matters. This ensures that unreasonable demands are not placed on suppliers and manufacturers. But there are difficulties in applying the 'reasonable consumer test' to consumer IoT devices.

As noted above, consumer IoT devices may be 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.[66] 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.[67] In relation to guidance about product safety, the Report specifically recommended that guidance should clarify how the guarantee should apply where a safety issue may not eventuate for some time or render the good as a whole unsafe.[68] In relation to reasonable durability, the Report noted consumer uncertainty about how durable a good should be and recommended that guidance be provided for

[64] Valve (No 3) [132].
[65] Valve (No 3) [134].
[66] See, for example, *Freestone Auto Sales Pty Ltd v Musulin* [2015] NSW CA 100.
[67] ACL Review Final Report, 14.
[68] Ibid 18.

specific circumstances and goods, including where 'the good is a 'smart' or hybrid product that combines different functions or blurs traditional product categories'.[69]

A sui generis category for digital products

In the UK and the EU, issues relating to the categorisation of digital products have been dealt with by introducing a new *sui generis* category of 'digital content'.[70] This raises the question of whether a new category of product, distinct from 'goods' and 'services', should be introduced to the ACL.

There would be 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. Thirdly, it may be possible to more clearly specify which entities in complex supply chains should be primarily liable for breach of relevant consumer guarantees. The disadvantages are that, first, given the diversity of products that might be characterised as digital products, there may be 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 consumers, suppliers and manufacturers, it seems preferable for a uniform set of consumer guarantees to apply to a single product, even where that product is a complex hybrid of hardware, software and associated services. 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 the relatively new category 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 relevant definitions reflect that concern. While there is a case for introducing a new category for digital products, it may be that, given the rapid growth in IoT consumer devices, consideration should be given to developing a definition that more clearly applies to these devices, as well as possibly 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 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 combined with 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.

It is our submission that a new category of 'digital products', distinct from 'goods' or 'services', should be introduced to the ACL. A particular advantage of introducing a new category of digital products would be to allow for consumer guarantees to be specifically

[69] Ibid 23.
[70] See *Consumer Rights Act 2015* (Cth); 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 (the 'Digital Content Directive'); 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 (the 'Sale of Goods Directive').

tailored to reflect the expectations that consumers might reasonably have for hybrid, connected devices. The guarantees could, for example, include specific guarantees that: the devices be reasonably secure; that any software elements be up to date and regularly updated; and that elements of hybrid devices be properly integrated.

Product Safety

Part 3-5 of the ACL includes a statutory product liability law which imposes liability on manufacturers (including 'deemed manufacturers' such as, in certain circumstances, importers) where goods have a 'safety defect'. Goods will have a 'safety defect' where 'their safety is not such as persons generally are entitled to expect'.[71] The test for determining whether there is a safety defect is objective, based on the reasonable expectations of the community. This means that the standard is not that goods must be absolutely free from risk, but that the level of safety is that which the community is entitled to expect.

The liability of manufacturers for safety defects is subject to defences, including that:

- the alleged defect did not exist at the time the product was supplied by the manufacturer;[72] and
- the defect could not have been discovered in the light of the state of scientific and technical knowledge at the time the goods were supplied.[73]

Application of product safety regime to consumer IoT devices.

There is no relevant case law on the application of the product safety regime to products with cyber security vulnerabilities. As with the consumer guarantees, however, there are considerable uncertainties about the way in which the product safety regime may apply to consumer products with security vulnerabilities. For example, it is unclear what the 'reasonable expectations' of the community might be in relation to the security of IoT devices. Moreover, a product might be supplied with no hardware vulnerabilities, but vulnerabilities may subsequently emerge, potentially due to software upgrades. Where different entities are responsible for different elements of an IoT product, such as hardware or software elements, there may also be difficulties in applying what is known as the 'component defence'. While manufacturers of a component of a complex product may be liable to compensate consumers for losses incurred from defective components, section 142(d) of the ACL establishes a defence where the defect is due to the actions of the ultimate manufacturer of the finished product, such as a failure to ensure proper integration of components. With consumer IoT devices, there may be difficulties in determining the source of a security defect and, moreover, it may be difficult to determine who is ultimately responsible.

We believe that, given the extent to which security is a fundamental element – if not the most important element - of the safety of consumer IoT devices, the product safety regime under the ACL should clearly apply to protect against insecure products. As with the consumer guarantees, however, consumers and manufacturers need greater certainty about how the product safety regime may apply to IoT products. Ideally, we suggest that this could involve legislative amendments, such as amendments to the definition of a 'safety defect' and amendments to relevant defences, such as the 'no defect at time of supply' defence.

[71] ACL s 9(1).
[72] ACL s 142(a).
[73] ACL s 142(c).

Product safety and technical standards

A particular area of difficulty concerns the relationship between the product safety regime and applicable technical standards. Recognising that standards may lag behind technological developments, section 9(4) of the ACL provides that an inference of a safety defect is not to be drawn merely because of compliance with a Commonwealth mandatory standard that is not the safest possible standard given the latest state of scientific and technical knowledge at the time the product is supplied. This reinforces the importance of ensuring that relevant technical standards remain up to date, but also raises the question of the relationship between the product safety regime and technical standards. As this submission has emphasised, it is important to maintain coherence and consistency across the various regimes that apply to the regulation of cyber security. One potential way for ensuring this may be to more explicitly linking consumer protections under the ACL to security standards, provided that there are mechanisms in place to ensure that relevant standards are adequate and kept up to date.

27. Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

In its report on *Digital Platforms* (the 'DPI Report'), the ACCC made it clear that Australian data privacy law has not kept pace with contemporary data practices and made recommendations for addressing deficiencies in the law.[74] The DPI report included specific recommendations to strengthen the protections available under the Privacy Act, as well as issues that the ACCC recommended should be subject to further review.

The Commonwealth Government's response to the DPI Report, released in December 2019, indicated that it would consult on legislation to amend the Privacy Act.[75] In particular, the response indicated that the government supported the following three ACCC recommendations in principle:

- amending the definition of 'personal information' to extend to technical data and other online identifiers;
- strengthening notice and consent requirements to meet 'best practice standards'; and
- introducing a direct right for individuals to bring actions for interferences with privacy under the Privacy Act.

Subsequently, the Commonwealth Attorney-General's Department initiated a fundamental review of the Privacy Act, releasing an *Issues Paper* seeking public submissions on 68 questions.[76]

Strengthening the Privacy Act

This submission focuses on those aspects of the review of the Privacy Act that are most relevant to protecting and promoting cyber security. The protection of personal information and cyber security protection have a symbiotic relationship: cyber security is necessary to ensure that personal information is not collected, disclosed or stored without consent; and adequately protecting personal information can protect devices

[74] Australian Competition and Consumer Commission (ACCC). *Digital Platforms Inquiry* (Final Report, June 2019).
[75] Australian Government. *Regulating in the Digital Age*: *Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (12 December 2019).
[76] Attorney-General's Department, *Privacy Act Review,* Issues Paper (October 2020).

against security intrusions. The strengthening of the Privacy Act to ensure that it is reasonably adapted and appropriate to apply to contemporary data practices can therefore play an important role in assisting to ensure and promote cyber security.

We therefore support necessary reforms such as extending the statutory definition of 'personal information' and strengthening the notice and consent provisions. We also support introducing a direct right to bring actions for interferences with privacy under the Privacy Act, which can provide an important additional avenue for enforcing the Act, assist in conserving the scarce resources of the OAIC and provide direct recourse for affected individuals.

As explained in our responses to Chapter 5, ensuring appropriate coherency and consistency across laws relating to cyber security may require some additions to the APPs, or amendments to APP 11.

Privacy by design and by default

Over and above reforms that are directed at addressing existing gaps in the Privacy Act, however, there is a need to re-evaluate the adequacy of the paradigm underpinning the Act. The Privacy Act is essentially based on 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. To an extent, this paradigm still applies to data privacy laws, such as the EU's GDPR. 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. 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.[77]

This suggests a need for more holistic approaches to protecting the security of personal information that impose clear obligations on data collectors and data processors. For example, the well-known limits to the ability to enhance notice and consent, such as 'notice fatigue' and 'consent fatigue', direct attention to the ways in which systems for collecting and processing data are designed.

We therefore support the introduction of an enforceable principle of privacy by design and by default, such as that incorporated in article 25 of the GDPR. In addition, in relation to devices that pose considerable security risks, there may be a role for the Information Commissioner (or a relevant regulator) to have the power to require pre-market privacy/security impact assessments. Finally, especially given the degree to which the nature of connected devices may be changed by software upgrades, there is a need for appropriate powers for post-market regulation and enforcement, including appropriate monitoring and auditing powers.

Enforcement

As explained in the Discussion Paper, Treasury is developing options for giving the ACCC the right to bring civil proceedings for failures to comply with the consumer guarantees. We believe this is an overdue reform, and believe it will help in ensuring

[77] DPI Report, 478.

greater compliance with the consumer guarantees and clarifying liability for failure to comply with the guarantees. In general, we consider that there is no justification for the enforcement regime, and the available remedies, relating to a failure to comply with the consumer guarantees to provide any less protection than that available for breaches of other parts of the ACL. That said, enforcement and remedial regimes can only be effective if the substantive provisions of the ACL are fit for purpose. That is why this submission emphasises the importance of ensuring that substantive provisions of the ACL, such as the consumer guarantees and product safety regimes, are able to satisfactorily protect consumers against cyber security risks.

Prohibition of unfair trading

Apart from amendments to the consumer guarantees and product safety regime, we consider there is a case for introducing an additional consumer safeguard, which could potentially assist in enhancing cyber security. Data-driven business models, which can facilitate fine-grained targeting of individual consumers, can allow businesses to manipulate consumer preferences, including the preferences of vulnerable consumers.[78] The extent to which consumers may be subject to manipulative practices, including automated forms of manipulation, can pose cyber security risks. To address this problem, we support proposals, such as that made by the ACCC in its DPI Report,[79] for introducing a new consumer safeguard in the form of a general prohibition of unfair trading, which could provide recourse against certain predatory and manipulative conduct associated with data-driven business models.

[78] 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; Kayleen Manwaring, 'Will emerging information technologies outpace consumer protection law? – The case of digital consumer manipulation' (2018) 26 *Competition and Consumer Law Journal* 141.
[79] DPI Report, p. 498.