27 August 2021

Department of Home Affairs
Via website

Submission on Australia's cyber security regulations and incentives

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('**UNSW Allens Hub**') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The Australian Society for Computers and Law ('**AUSCL**') is an interdisciplinary network of IT and Legal professionals and academics focussed on issues arising at the intersection of law, technology, and society. It is a registered Australian charity with a charter to advance education and advocacy. AUSCL was officially launched in July 2020 by its patron, the Hon. Justice Michael Kirby. The Society has a proud history, with its member societies being established as early as 1982. AUSCL provides a forum for learned discussion and debate through its Policy Lab, Working Groups and Events Program attracting support and engagement across Australia and globally.

The UNSW Institute for Cyber Security ('**IFCYBER**') is a multidisciplinary Institute which focuses on research, education, innovation and commercialisation that has 'real world impact'. The Institute has over 60 members across each of our faculties. We are ambitious (achieving international impact), scholarly, collaborative and inclusive (acknowledging that cyber security is a new and developing field and seeking opportunities to broaden our understandings of the field by welcoming a broad range of disciplines), entrepreneurial (seeking opportunities to empower academics to be creative), diverse (embracing multidisciplinary and working as thought leaders), and generous and supportive (helping to develop and mentor early career academics, recognising vulnerable groups in society).

The Security Engineering Capability Network ('**SECedu'**) is a partnership of cyber security and security engineering academics and educators and industry experts working to advance Australia's digital security engineering capability through education, training, and professional development. It is a partnership between UNSW and the Commonwealth Bank of Australia. More information about SECedu can be found at https://sec.edu.au

Policy context

This call for submissions takes place in an evolving policy space. It intersects with other policy initiatives including changes in critical infrastructure legislation, a review of the *Privacy Act 1988* (Cth), development of an Australian Data Strategy, and others. Because ideas being considered by other policy units, such as eliminating some restrictions on privacy-related litigation, impact on this policy process, our comments and recommendations are often based on assumptions about existing policy settings that may cease to be true. Our submission therefore needs to be read in that light and we encourage strong links among the various policy development processes across government.

It is also important to ensure that any policy work is conducted in the context of the existing legal landscape. While the Call for Views highlights many relevant laws and policy developments, possibilities such as breach of contract (where the contract contains promises with respect to secrecy or security) could also be relevant in some circumstances. For a helpful "work in progress" map of law relating to cyber security, we recommend Austlii's Cyber Law Map.

About this Submission

We appreciate the engaged consultation approach of the Department and, in particular, the opportunity to discuss our ideas at the roundtable on 16 August 2021, which we found very useful in guiding us in this submission. We endorse the Department's willingness to consider bold policy reform.

This submission is not intended as a comprehensive response to all the issues raised in the Call for Views, but rather focuses on topics on which our research and experience can shed light. Our responses on the questions thus make particular points (as follows) but may not deal with all aspects of the questions.

Question 1: What are the factors preventing the adoption of cyber security best practices in Australia?
The lack of agreement in industry around cyber security and diversity of strategies to measure and manage risk make it difficult for organisations to identify best practices. What is best practice is often in dispute and evolves over time and varies from organisation to organisation depending on their particular risk characteristics, assets, and attackers.

Question 2: Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?
We encourage Government to provide resources and incentives for the development and adoption of cyber security standards and best practices.

Question 3: What are the strengths and limitations of Australia's current regulatory framework for cyber security?
CPS 234 sets a good example of how standards can improve cyber security; outside the contexts in which it applies, the vagueness of the *Privacy Act 1988* (Cth) APP 11 creates challenges not only for compliance, but also for subsequent criticism of and liability for poor practices.

Question 4: How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements
Standards (technical, governance, management) have a number of advantages in terms of specificity, clarity and coverage, but also some important limitations and challenges. Some of these limitations and challenges can be mitigated through resourcing standards development and access to standards, allowing regulated entities to choose among acceptable standards, and funding research that creates an evidence base for better standards.

Question 5: What is the best approach to strengthening corporate governance of cyber security risk? Why?
We prefer option 2 and make some suggestions as to how identified challenges can be managed.

Question 6: What cyber security support, if any, should be provided to directors of small and medium companies?
In addition to information and guidance, small and medium enterprises should be given financial incentives and practical support to take additional cyber security measures.

Question 7: Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?
Relevant and high-quality education initiatives are required to support business leaders to prioritise investment in cyber security and to bring about the adoption of security culture across organisations from the top, in the same way the adoption of safety culture by leadership has uplifted transport and occupational safety.

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?
It is a viable option to include a cyber security code under the Privacy Act and give concrete criteria for APP 11, but there are issues to consider and address should this be the preferred approach. Note that the 'cyber security code' could be a requirement to comply with internationally recognised standards.

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)?
While we make some specific suggestions here, our preference is for adoption of international standards. In that context, our suggestions could be factored into a broader standards development process.

Question 11: What is the best approach to strengthening the cyber security of smart devices in Australia? Why?
The status quo is inadequate; we suggest a better approach.

Question 12 Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices
The Department should consider a choice of standards, including but additional to ETSI EN 303 645. Additionally, the Department should consider the appropriateness of network-level security standards.

Question 14: What would be the costs of a mandatory standard for smart devices for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?
When considering this question, associated costs should be levelled against the prospect and scale of future harms.

Question 16: What is the best approach to encouraging consumers to purchase secure smart devices? Why?
Labelling may be helpful in encouraging consumers to become aware of cyber security in relation to smart devices, and consequently improving their purchasing choices in this area, but this is only a small part of a solution.

Question 17: Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?
Labels and standards are unlikely to be sufficient in themselves without some form of mandatory implementation.

Question 20: Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?
There should be some form of regulated minimum cyber security standard for smartphones.

Question 21: Would it be beneficial for manufacturers to label smart devices both physically and digitally? Why or why not?
Physical labels will be necessary in some contexts but will need to be updatable in ways that prevent updating "at will".

Question 26: What issues have arisen to demonstrate any gaps in the ACL in terms of its application to digital products and cyber security risk?
We set out some examples in which the application of the ACL is uncertain in its application to digital products and cyber security risks.

Question 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?
Reforms being considered to the *Privacy Act* will not adequately cover the field in relation to smart devices. Some reforms being considered for the ACL are useful. Other reforms such as strengthening protection against unfair contract terms are also relevant.

Question 28: What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights [of] consumers?
Other policies to consider include a strict liability regime, international harmonisation and learning from overseas jurisdictions.

Further detail on these responses follow.

Question 1

What are the factors preventing the adoption of cyber security best practices in Australia?

Identifying what are the best practices can be challenging for less mature organisations. What is best practice is often in dispute, evolves over time and varies from organisation to organisation depending on their particular risks characteristics, assets, and attackers. Further, even with full understanding and agreement of best practice for a particular organisation at a particular time, there is a significant national shortage of human capability to properly implement and operate best practice. There is not only a shortage of technical security expertise, but also a lack of general understanding and cyber security mindset amongst all staff across the organisation. Understanding needs to extend beyond simple awareness. Furthermore, without a sufficiently mature understanding of cyber security and cyber security risk, key individuals in organisations are not equipped to make appropriate decisions about cyber practices relevant to their role and organisation.

As its widest point, cyber security risk is a rapidly evolving and dynamic class of risk. There is rarely industry wide agreement on the most appropriate and cost-effective measures or how data security exposures should be managed at an organisational risk level.

This creates ongoing disagreements within the industry as to what constitutes a "mature" organisation. Risk focus areas continue to shift due to changing malicious actor behaviours and the rate of new technology controls constantly being introduced to the market. Examples of the confusion created by this backdrop can be seen in the ongoing debates occurring within the industry regarding the benefits of Security Orchestration Automation and Response (SOAR), and the processes that constitute effective ransomware risk mitigation controls.

Designing and implementing uplift strategies within organisations is made more complex by the wide variance in frameworks and workstream strategies pushed by information security expert providers within Australia. Even amongst the largest information security consulting firms, clients will be presented with different, and at times contradictory advice in relation to asset identification and management, control posture assessment, application security strategies, identity management protection and patching cadence. In many cases, clients are also unaware that certain solutions and tools are pushed by experts because they create additional implementation work streams for the consultant or because a wider reseller and referral relationship exists between the consultant and the technology product provider. Unfortunately, this relationship can regularly result in organisations receiving sub-par advice and undertaking work which does not deliver cost effective security posture uplift.

Finally, the lack of uniformity in the advice clients receive also creates difficulty in information sharing between peer organisations and the wider industry around effective cyber security strategies. This results in organisations with similar profiles and operational activities often having entirely different processes to manage cyber risk assessment, internal governance, quantification, and resilience.

Question 2

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

We agree that negative externalities and information asymmetries create a need for Government action on cyber security. We therefore encourage Government to provide resources and incentives for the development and adoption of cyber security standards, best practices, and education.

Today, cyber security is important in areas such as health and wellbeing products, wearables such as clothing and glasses, sports, kitchen and cooking products, loyalty programs, retail and supermarkets, and many other areas. Even businesses are regularly making investments in cyber security to achieve multi factor authentication, endpoint detection and monitoring, failover capabilities and enhanced incident recovery. As a result, cyber security has become increasingly important in protecting consumer rights. As the world continues to generate more data, the domains in which cyber security matters will grow.

As the Call for Views notes, there is information asymmetry as to cyber security risks. Information asymmetry results from most consumers not knowing how the technology they buy works, particularly from a security perspective. Consumers may not realise a traditionally analogue non-digital product, such as an oven or a pacemaker, can now be hacked, creating real health and safety risks.

Products are often marketed as 'safe and secure.' To protect general consumers from misleading or deceptive conduct under s 18 of the Australian Consumer Law, such terms need to be given a clear meaning, ideally by reference to standards. Generally worded principles, such as APP 11 of the *Australian Privacy Principles*, are too vague to be useful. It is more useful for consumers to be told that a product complies with objective and clear criteria contained in a recognised standard.

Question 3

What are the strengths and limitations of Australia's current regulatory framework for cyber security?

The Australian Prudential Regulation Authority mandatory Prudential Standard CPS 234 on Information Security is one of the more comprehensive cyber security approaches within Australia regulatory landscape and provides key insights on how a wider cyber security regulatory framework can be developed. Globally, a common tension in the cyber security space has been the need to avoid "box ticking" activities and instead instil a wider "risk principles" approach within organisations.

CPS 234 tackles this problem by including pro-active obligations for regulated organisations to assess the sufficiency of their information security capability, across resource adequacy, funding, staff, access to expert skills and the comprehensiveness of the control environment.[1] CPS 234 requires adequacy assessments to incorporate situational awareness and intelligence.[2] While situational awareness may seem like an obvious component for any risk assessment, this is commonly overlooked in many organisational cyber security strategies.

The ideal cyber maturity investments for each organisation should be driven by their own individual circumstances and incorporate factors such as key data asset held, the employee base and behaviours, how malicious actors are engaging with their industry or sector, business and operational requirements, contractual and counterparty obligations and the extent of manual and technology redundancy which exists within the organisation. Distilling these unique circumstances however requires an engagement with stakeholders across the wider organisation, and the need to understand cyber security impacts on an organisational wider business goals and objectives.

Cyber security professionals are often poorly equipped to address these wider issues, as traditional security education and the vast majority of their training and expertise focuses on ground up technology controls and the triaging of individual impacted data assets within the environment. Few if any receive proper risk governance or professional engineering training, and wider issues such as the interplay between regulatory requirements, contractual obligations and cyber are almost never assessed in traditional cyber security uplift engagements. A legislative requirement to drive wider engagements that incorporate business risk and highlight the need for situational awareness will create strong incentives to change this behaviour and align cyber risk management with wider business processes. This will also promote other objectives outlined by the Department of Home Affairs such as director uplift.

CPS 234 also requires clearly defined roles and responsibilities for those who will have accountability within an organisation for information security. This is to be achieved through a combination of role statements, policy statements, reporting lines, charters, decision-making structures, and oversight processes.[3] Requiring a clear accountability structure serves the immediate forcing senior leadership within an organisation to holistically examine their internal processes and requires the affirmative empowerment staff to take ownership of the exposure. An additional benefit of this approach is that it requires organisations to clearly document accountability and risk ownership, addressing the traditional problem of organisations relying on “lived” cyber security processes that are not properly documented or supported with clear risk management procedures.

A third benefit of CPS 234 is that it calls out the need to assess the capability of third parties and related parties. Supply chain cyber risk remains a critical challenge across the Australian landscape as seen in numerous recent data breach incidents such as the Kasaya ransomware attacks. Many outsourced due diligence processes used to manage third party cyber risk are inefficient as they focus on large, automated question and information gathering activities that do not tie to the risk drivers of the individual organisation. CPS 234 demands organisations to identify the scope, depth and independence of any provider certifications, attestations, and assurance and to take steps to address any limitations identified.

Finally, CPS 234 highlights for cyber security risk management to be constantly revised, and that each regulated entity must actively maintain an information security capability with respect to changes in

[1] Australian Prudential Regulation Authority Prudential Standard CPS 234 Information Security June 2019, at para 15

[2] Ibid at para 16.

[3] Ibid at 11.

vulnerabilities and threats.[4] The ties in well with CPS 234's requirements to promote situational awareness, as one of the most effective measures of cyber risk management is the ability to quickly distil changes in the threat environment, and to identify the need to revisit security controls in a way that addresses realistic current exposures. Ensuring cyber security risk management becomes a dynamic process will be critical to achieving the Department's maturity uplift objective.

In examining the current framework, it is also important to address the existing *Privacy Act 1988 (Cth).* APP 11 requires a regulatory entity to (amongst other things) take such steps as are reasonable in the circumstances to protect personal information held by the entity from misuse, interference, and loss, as well as unauthorised access, modification, or disclosure. The Notifiable Data Breach scheme housed within the Privacy Act is also an important mechanism for increasing cyber security accountability and testing an organisation's compliance with the wider APP framework.

The Call for Views correctly calls out a lack of clarity in how existing legal obligations apply to specific cyber security requirements. The *Privacy Act* is unfortunately a significant example of the problems caused by this lack of clarity. A demonstration of this problem is seen in the recent determination made by the Office of the Information Commission of Uber Technologies, Inc (UTI).[5] The basic facts of this matter were that:

1. Malicious actors successfully compromised UTI's system and were able to access client data of some 57 million users stored in Amazon Web Services (AWS) from 3 October 2016 to 15 November 2016, including 1.2 million Australians;
2. The attack chain involved compromising Amazon Web Services (AWS) credentials in one of UTI's GitHub repositories. The Attackers used these credentials to obtain programmatic access and download the contents of 16 files from AWS;
3. In October 2017, after becoming aware of the incident, UTI's external counsel engaged a forensic IT consultant firm, Mandiant, to conduct an analysis of the data downloaded by the Attackers.
4. Following Mandiant's investigations UTI undertook a number of uplift measures including:
    a. resetting the compromised access key credentials;
    b. requiring two-factor authentication for all of its private GitHub repositories;
    c. paying US$100,000 to the Attackers under a 'bug bounty' program in December 2016;
    d. Obtained written assurances in January 2017 from the Attackers that the downloaded data had been destroyed and that they would not disseminate the data.

A number of valid criticisms were made of UTI's approach to compliance with the Privacy Act within the decision. The commissioner's specific findings with respect to APP 11.1 were:

1. Multi-factor authentication should have been implemented for UTI's private repositories in GitHub, particularly given UTI did not have a written policy in place that prevented employees from hardcoding access keys in plain text in code in GitHub.
2. Multi-factor authentication should have been implemented for programmatic access to UTI's AWS S3 repository. This would have ensured that the Attackers would not have been able to access the compromised files unless they had also been able to obtain access to UTI's network.

[4] Ibid at 20.

[5] Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34 (30 June 2021)

3. UTI has been unable to explain why the AWS access credential obtained by the Attackers had not been rotated. Written policies should have been implemented that required UTI employees.
4. UTI should have adopted a policy not to make functional access keys available in plain text in code, in GitHub or elsewhere.
5. UTI should have rotated access keys on a regular basis using UTI's secrets management tool.
6. The backup files that were the subject of the Data Breach were not created as part of UTI's ordinary processes. UTI should have adopted and implemented a policy to encrypt backup files containing personal information that were created in this way for a particular purpose like migrating to a new system.
7. Regular training of relevant UTI employees should have been required to monitor compliance with those policies.

While each of these criticisms seem to create reasonable grounds for the underlying APP 11 breach finding, they become less convincing with further analysis:

1. The GitHub credentials which appear to have been instrumental in this attack appeared to be sourced from UTI employees from a different data breach, which was "unrelated to UTI".[6] The determination makes no consideration of whether UTI could reasonably have been aware of this other compromise, or whether GitHub credential security environment was otherwise lax.
2. The commissioner's complaint that access keys were apparently in plain text in code in GitHub misses the point, as to get to this stage the repository asset had already been compromised. Viewed in this light is it unclear whether the conduct of which the OAIC complains would have prevented a compromise of UTI's external perimeter.
3. While multi-factor authentication (MFA) is accepted as a fundamental cyber security investment in the current environment, this matter arises from a 2016 compromise. Any assessment of reasonable steps should be based on analysing the historical cyber security investments that were viewed as appropriate within the industry at the time of the breach. Without this factual analysis any findings risk being significantly tainted by the benefit of hindsight.
4. The level of knowledge within the industry on cyber security maturity strategies was fundamentally different in 2016. For example, the Essential Eight Maturity Model had not yet ever been released by the Australian Cyber Security Centre when the UTI breach occurred.[7]
5. The failure to analyse what was subjectively reasonable as at 2016 is also problematic given the OAIC's decision acknowledges UTI had at least implemented a partial MFA rollout within the organisation prior to the breach.[8] The issue of whether multiple MFA processes within a single environment was a reasonable step for IT environments in 2016 is likely to be open to significant debate.
6. The effectiveness of password rotation strategies was a live issue in 2016 as was seen in an article published by the United Kingdom National Cyber Security Centre in October 2016 highlighting the problems with forcing regular password expiry and password policies more generally.[9]

---

[6] Ibid at para 6.

[7] The Essential Eight Maturity Model was first published in June 2017.

[8] Note 5 at para 89.

[9] "The problems with forcing regular password expiry", National Cyber Security Centre, 5 October 2016, accessed online: https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry

It is also worth highlighting that the specific findings of breach which the OAIC identify strongly mirror the voluntary uplift steps that were taken by UTI following the data breach.[10] This does not provide principles to assess what UTI or other organisations should have realistically known, or the vulnerabilities they should have realistically identified, in the absence of having absolute knowledge of a successful attack chain against their environment. This is one reason why the determination cannot be leveraged to provide organisations with any realistic guidance on how a risk assessment strategy compliant with APP 11 can be undertaken as part of their own compliance processes.

The above criticisms are not intended to undermine the important work which the OAIC performs, or to suggest that UTI conduct was defensible. Clearly there were fundamental cultural and control failures within the organisation, however the OAIC's determination is not conducted on a risk principle basis and fails to identify any test that can be used to assess those measures and cyber security controls that are reasonable within the context of each organisation's circumstances. Australia's regulatory approach to cyber security should reference clear requirements that apply at each point in time against which companies can be fairly held to account at a later date.

Question 4

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

The use of standards (technical, governance, management) has a number of advantages in the highly technical and rapidly evolving context of cyber security. However, there are also limitations, including the lack of free public availability of many standards instruments, the fact that Australia is too small a market to set its own standards, the fact that standards may be based on patented products and processes, the fact that standards come with a compliance cost, and the fact that some standards are only relevant to part of the challenges (or part of the markets) identified in the Call for Views.

We believe the best way forward is (1) for Australia to be involved in standards development for relevant international standards (eg through Standards Australia, the International Organization for Standardization or other professional-based standards bodies) and for this to be appropriately resourced, (2) for requirements, recommendations or labelling to be based on compliance with a suite of standards with alternatives specified where more than one acceptable standard exists, and (3) for the government to subsidise access to standards to ensure their availability to those (such as consumers, consumer bodies and smaller enterprises) that may not be able to pay the required access fees. The government can also be proactive in supporting the development of an evidence base that can be used by those doing standards development work to better understand Australian industry and consumer needs and expectations. Incorporation of industry-driven technical standards into legal requirements may send a co-regulatory message to the industry, creating a risk of regulatory capture (as industry is involved in standards development). This risk needs to be managed, including by supporting diverse actors (including consumer organisations) to participate in standards development.

Ideally standards will be sufficiently clear and well-aligned with Australian expectations so that they can be followed by businesses and understood by consumers. Legal requirements that reference standards should be specific about which standards (which can involve a choice) constitute compliance. Standards can also be cross-referenced to terminology that can be used in advertising so that "safe" or "secure" is given specific meanings (like "free range" in the context of eggs).

[10] Ibid.

Compliance could be managed through certification, but enforcement would need to be resourced, likely through the ACCC. There are two examples of where this works well in practice. The first is in the Australian Consumer Law in relation to defective products. In this example, there is a defence available that the state of scientific and technical knowledge available at the time of supply did not enable the supplier or manufacturer to discover the defect. This is usually demonstrated by the supplier or manufacturer providing evidence that the product met the requirements of a standard used in Australia. The second relates to the burden of proof. In respect of electromagnetic compatibility (EMC) standards enforced by the ACMA, if there is an EMC issue and a product has been tested and shown to comply with an appropriate standard, then the ACMA must demonstrate that the product has caused interference. If the manufacturer asserts that the product meets relevant standards but has not been tested, then the manufacturer must demonstrate that the product has not caused interference.

There is no one-size fits all with cyber security standards. Standards adoption needs to be based on risk profiles, industry segment, budget, organisational maturity and likelihood of implementation. While cyber security professionals are well aware of ISO 27001 and NIST standards, these are largely unknown in industry. There are 2,065,523 small businesses in Australia employing less than 19 people, accounting for 97 per cent of all Australian businesses by employee size.[11] Many of these businesses play critical roles in Australia and are often part of supply chains for larger businesses. On the whole, most have no idea and no interest in cyber security, let alone adopting a recognised international framework. The government needs to give options and implementation guidance to small and medium businesses on fit-for-purpose standards and frameworks.

Question 5

What is the best approach to strengthening corporate governance of cyber security risk? Why?

Of the options set out in Chapter 4 of the Call for Views, we prefer option 2, which requires mandatory governance standards for larger businesses. Specific entities subject to the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* are already subject to security legal obligations to manage the security and resilience of their critical infrastructure asset. In addition, there are already existing standards (such as ISO/IEC 27001 and NIST) available to be adopted by organisations voluntarily. Without making these standards mandatory, compliance will likely remain at current levels.

That does not eliminate the challenges of option 2 identified in the Call for Views, including costs, interaction with other legislation, requirements on international organisations and cumulative burden on businesses to operate. We suggest that these challenges be managed, within the framework of option 2, as follows:

- the timeline given for compliance be achievable, with an ability to apply for an extension where warranted;
- the governance standard should be function-based rather than role-based given organisations may already have complying functions under various work titles;
- the governance standards should be adaptable to different contexts (alternatively, organisations can be given a choice among different standards that target different organisation structures, industries or systems);

[11] Australian Government. Australian Small Business and Family Enterprise Ombudsman. [https://www.asbfeo.gov.au/sites/default/files/Small_Business_Statistical_Report-Final.pdf]

- organisations subject to analogous requirements (such as the APRA's prudential standards, the *Security of Critical Infrastructure Act 2018* or analogous laws or standards in overseas jurisdictions) should not be forced to comply with standards that duplicate existing requirements.

The idea is to capture organisations not currently subject to sufficient cyber security requirements. Costs to implement can be managed through a progressive approach. In addition, organisations subject to the *Privacy Act 1988* (Cth) already have an obligation to report notifiable data breaches. These organisations are likely to maintain existing reporting lines for incident management, incident assessment, operational risk control, risk assessment and provide risk reporting to the head of the organisation. Between January and June 2021, 43% of the reported incidents are cyber security incidents.[12] To accurately assess whether incidents meet the threshold of notifiable data breach, organisations already have internal cyber security resources to identify, assess, report and mitigate security risks in relation to the incidents. These mandatory corporate governance standards can leverage the existing cyber security resources required for the notifiable data breach assessment to provide consistent and regular oversight and review from the corporate leadership level as a preventive method.

Question 6

What cyber security support, if any, should be provided to directors of small and medium companies?

The corporate governance standards for larger organisations will provide a strong reference for small and medium companies. Currently there are some resources for small and medium company directors offered on cyber.gov.au. The Cyber Security Cooperative Research Centre is creating an additional resource for small and medium enterprises in the supply chain for critical infrastructure in partnership with the Department for Home Affairs. Provision of static resources is a helpful start but this needs to complemented by readily available high-quality education and training in order to bring about changes in understanding, mindset and culture. This is particularly important given that there is a significant risk that smaller enterprises in supply chains will merely claim to be compliant without acquiring a genuine security culture in order to obtain relevant work.

The Corporations Act places the same responsibilities on company directors, regardless of the size of their organisation. SME's need to understand risk management of internet-facing assets and subsequent controls need to be implemented.

The vast majority of small to medium enterprises in Australia lack the resources to invest in cyber security resilience that can outpace the rapidly changing threat landscape. In addition to cyber security guidance material, incentives must be developed to support company directors. Cyber security is not free. These incentives should promote self-sufficiency, rather than Government funded resilience. The promotion of a cyber security insurance sector could assist to promulgate self-sufficiency across smaller enterprises. Larger business could also be incentivised to provide "in-kind" support for smaller enterprises in their supply chain. Another example of support might be that the fully recovered labour costs of providing this support receive more favourable tax treatment than merely being an expense, providing a similar incentive to the Research and Development Tax Incentive.

[12] Notifiable Data Breaches Report: January–June 2021, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021/

Question 7

Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Relevant and high-quality education initiatives are required to support business leaders to prioritise investment in cyber security and to bring about the adoption of security culture across organisations from the top, in the same way the adoption of safety culture by leadership has uplifted transport and occupational safety. Extensive passive guidance material exists but it is rarely tailored based on sector specific risks and requirements and active engagement in education and training is required to bring about meaningful culture change.

Achieving the required scale, quality, and effectiveness of knowledge and behaviour uplift across businesses and customers requires two pillars which need to be achieved simultaneously. Quality and delivery. The right expertise and information needs to be identified for the individuals being trained and the educational design needs to be effective – it needs to be taught well. Achieving only one of these two leads to wasted effort. It is important to note that education is required not simply communication, so educational experts must be closely involved, and that the advice and expertise needs to be relevant and up to date so industry experts need to be closely involved.

This training should look like a suite of educational programmes for executives and leaders. Those with time and need can consider formal postgraduate qualifications. A range of shorter informal programmes, for example backed by micro-credentials, could be encouraged. Rather than developing these directly themselves the government should play a role in encouraging, facilitating, accrediting and promoting them. It would also be of great value for government to facilitate communities of practice amongst education providers and industry experts to enable a wide range of quality programmes to be developed and delivered to as wide a possible collection of industries and risk types.

In addition to education and awareness raising initiatives the Australian Government should also consider mechanisms to promote the collaboration across industry communities of practice or Information Sharing and Analysis Centres (ISACs) to support increased self-sufficiency and prioritisation of business cyber security investment. As an example of sharing technical information additional funding for the ACSC Cyber Threat Intelligence Sharing (CTIS) initiative and support to the formation of industry ISACs will help provide technology and cultural mechanisms to support senior business leaders to make informed decisions.

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?

Given the intent is to protect personal information and to specify minimum requirements for personal information security protection, it is a viable option to include a cyber security code under the Privacy Act and give concrete criteria for APP 11. Linking security and privacy requirements is a good idea *provided that* the government recognises that we need “privacy and security” (both are co-dependent and equally important) rather than “privacy or security” (with the former giving way to other concerns).

The Privacy Act only applies to Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million, and there are exceptions. If a cyber security code were to be incorporated into the Privacy Act, a few additional considerations should be taken into account:

- The Commonwealth government should encourage states and territories to introduce a similar requirement into their own general and health privacy laws to provide consistent coverage for state agencies, public hospitals and public schools.
- The code should be more specific than APP 11 to ensure requirements for compliance are clear and auditable.
- Small businesses not otherwise subject to the Privacy Act should have an ability and incentive to opt in, including for cyber security compliance (the question of expanding the Privacy Act is a separate one, currently under a separate policy process). This protects against an assumption that smaller businesses are necessarily less secure.
- If authored by the government, the cyber security code should be reviewed regularly to assess the need to update relevant sections and wording based on the latest technology. It may be preferable, however, to use an existing internationally recognised standard or to create options to choose from a list of standards.
- There needs to be a process for conformance testing and certification, with oversight. Certification processes already exist for some internationally recognised standards but would need to be created for a new government-developed standard if that were created. An agency will need to oversee the scheme and list non-compliant companies publicly to raise consumer awareness of security risks.
- A mechanism should be available for individuals to report non-compliant behaviours and products to the ACCC or to the OAIC.

There are however structural issues within the Privacy Act that may prevent it from effectively housing a cyber security code. Many of the legal obligations housed within the Privacy Act's APPs focus on consent and collection behaviour. For example:

1. APP 1 requiring the entity to have a clearly expressed and up-to-date policy about the management of personal information by the entity;
2. APPs 3 and 4 regarding the collection and solicitation of personal and service information;
3. APP 5 deals with notification of the collection of personal information;
4. APP 6 regulates the purposes for which personal information can be used.

While these APP promote important privacy hygiene, they cannot be readily tied to cyber security assessment methods given:

1. Cyber security strategies must address all data security assets, not just those related to personal and sensitive data;
2. Many of the key components that form part of an effective cyber security strategy such as perimeter investments, identity management and security strategies, endpoint detection and response and security operations are not applied at an individual data asset level. They instead are tied to the totality of an environment as opposed to individual data collection points; and
3. Many of the above APPs are complied with through user consent and disclosure methods. The requirements for reasonable cyber security posture must be clearly distinguished from any behaviour tied to risks and data behaviour that an individual subject has consented to.

The APPs focus on consent and compliance behaviour also results in many privacy compliance work programs and expert engagements focusing almost exclusively on these data lifecycle functions. For many organisations APP 11 is often treated as a footnote or small subset of privacy compliance engagements.

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)?

The feasibility of including specific technical controls in a standard depends on whether the government develops its own standards or adopts internationally recognised standards. However, we make some specific suggestions which could be considered for a new standard or included in Australian recommendations in a standards development process.

Best controls change more rapidly than legislation. Referencing standards makes mention of controls more future proof. Otherwise, it is possible that controls mandated in legislation may be found to be inefficient use of resources or even harmful at a later date yet still required.

Standards should capture specific actions rather than ask organisations to take reasonable efforts. They should provide clear instructions to cater for organisations of various maturity levels. Simple but effective security controls such as patching, multi factor-authentication, restrictions on the use of Microsoft Office Macros and user privilege access controls should be included. Additional controls, suggested by the professional experience of one of the authors of this submission, might include:

- **Research:** Restrictions on the use of personal information for research or analytics purposes without a research ethics process, including sunset clause and guaranteed eventual deletion of data. Various levels of de-identification may be required for such uses and would require ongoing independent third-party audit.

- ∉ **Storage and retention:** Personal information can only be stored in an encrypted environment with encryption applied at rest or in transit. More precise encryption requirements may also be specified. Personal information stored in transition platforms for file sharing purposes will be removed within 48 hours following completion of the transition.
- ∉ **Education:** Organisations will provide onboarding training for staff members to understand what personal information means and what simple and effective ways are available to protect personal information, including as first preference not collecting it and securely deleting personal data as soon as practicable. Individuals to be made aware of their legal and ethical obligations.
- ∉ **Statutory privacy officer role:** Organisations which deal with personal information to have an appropriately qualified privacy officer role with reporting duties and a duty to act independently and on behalf of individuals whose data is collected. The role would report to the general counsel (if privacy is a legal function) or governance and compliance (otherwise) but not the data officer.
- **Sharing personal information**: Organisations will make a disclosure in their privacy policy when sharing personal information with organisations not complying with recognised information security standards, including organisations found non-compliant, overseas organisations and small businesses not required to comply. Organisations sharing or storing personal information overseas will list all the destination countries. When sharing with an international service provider, the list of countries should include where the data will be stored and where staff members having access will be located. Organisations selling personal information for a profit will make a clear disclosure in their privacy policy, including as to whether the buyer is required to comply with recognised information security standards.

- **Restrict access privileges**: Unauthorised users cannot access personal information. Requests to privileged access to personal information are reviewed every 6 months by the privacy officer function to validate if the user presents an ongoing need to access personal information.

- **Audit**: Privacy control adequacy and privacy compliance, complaints, and incidents to be included in company audits. Undeleted personal information to be reported and assessed as a company risk.

Questions 11-21

Our recommendations on these issues are the result of significant research into the nature of security vulnerabilities in smart devices, and the specific harms that may arise from these vulnerabilities. A short summary of this research is set out at Appendix A.

Question 11

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

Currently, manufacturers of smart devices and developers of related services lack strong incentives to invest in security features or maintain ongoing security quality after sale. The 'Code of Practice: Securing the Internet of Things for Consumers' ('Australian Code')[13] released by the Federal Government in 2020 does **not** provide the needed incentive, as it is voluntary and therefore the chances of compliance are low. Even industry representatives criticised the Code for 'lack[ing] an implementation and compliance framework'.[14] The recognised failure of the United Kingdom government's voluntary 2018 Code of Practice for consumer IoT security[15] ('UK Code') is significant proof of the lack of incentive provided by voluntary codes. The existence of a voluntary Code in Australia may even *cause* problems, as it may lend weight to erroneous assumptions that products allowed to be sold are secure by default.[16] Mere encouragement, without more, means little in an environment where change is complex and likely to be expensive, and where directors are expected (and even legally required)[17] to make decisions in the financial best interests of their *shareholders*, not their customers.

Additionally, market failure in the context of encouraging good security practices in consumer smart devices is almost inevitable in situations where a smart device's inbuilt security features, or lack thereof, is not readily obvious to an ordinary consumer deciding whether a device is suitable. Most consumers would not appreciate the security attributes that make devices suitable for a home network in the first place. Additionally, one of the major proxy indicators for quality in consumer goods, price, is not currently indicative of the standard of security in a smart device.

---

[13] Commonwealth of Australia, Code of Practice: Securing the Internet of Things for Consumers (2020), available at https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf ('Australian Code').

[14] T Burton, 'Internet of things sets the cat among the pigeons', Australian Financial Review (online, 12 October 2020) <https://www.afr.com/technology/internet-of-things-sets-the-cat-among-the-pigeons-20201001-p5612g> quoting F Zeichner, CEO IoT Alliance Australia and Adam Beck, Smart Cities Council.

[15] United Kingdom Government, Code of Practice for consumer IoT security (14 October 2018), available at https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security ('UK Code').

[16] United Kingdom Government, Proposals for regulating consumer smart product cyber security - call for views (Policy paper, 1 October 2020) ('UK Call for Views')

[17] Corporations Act 2001 (Cth) s 181(1)(a); Mills v Mills (1938) 60 CLR 150; Westpac Banking Corporation v The Bell Group Ltd (in liq) (No 3) (2012) 44 WAR 1; [2012] WASCA 157; Ngurli v McCann (1953) 90 CLR 425, 438; Kinsela v Russell Kinsela Pty Ltd (in liq) (1986) 4 NSWLR 722, 730.

Best practice would require manufacturers and other service providers to integrate effective **technical security measures** both at time of sale and ongoing within a reasonable lifetime of a smart device. These measures should be further supported by clearly communicated and reasonable **device management measures** that are either automatically controlled or easy for consumers to implement. However, these must be designed with real consumers in mind, that is consumers with *bounded rationality* and *limited capability* to support complexity. Special care must also be taken in providing real protection for vulnerable consumers, such as:

- children; and
- those in the aged and disability communities who have issues with accessibility and/or understanding of device management measures; and
- those at risk of technology-facilitated abuse, particularly in a family violence context where the perpetrator may well have set up the system and is the only party in relevant service contracts.

Therefore, **we support the introduction of mandatory regulation** to bring about real change to security practices.

For the avoidance of doubt the mandatory code should also address user privacy, for example clear labelling to indicate the capability of devices to scan the environment such including containing microphones, cameras, blue tooth receivers, location, monitoring communications, network access and so forth.

A mandatory code, whatever its regulatory form takes, needs an inbuilt level of responsiveness to sociotechnical change. Often this responsiveness is pursued by means of regulation that is 'technologically neutral'. However, 'technology neutral' legislation can suffer from uncertainty, particularly in the inevitable lag time between the passing of the legislation and interpretation of new provisions by the courts. Uncertain regulation is problematic for businesses who are looking for guidance on how to structure their operations to comply. Regulation needs to be fit for purpose, or 'technologically appropriate'. This includes providing some form of certainty for business around expected standards for compliance, particularly in complex technical areas such as cyber security.[18]

Current Californian and Oregonian legislation provides that 'reasonable security features' must be implemented in connected devices.[19] The Australian and UK voluntary Code set out thirteen principles for good cyber security. However, the position put forward by industry representatives in the roundtable discussion on smart device security (consumer Internet of Things) hosted on 27 July 2021 by Home Affairs is sensible. They believe that general principles, such as those provided in the voluntary Codes, are **insufficient** to give proper guidance to business. Instead, they supported the use of standards to provide the detail necessary to flesh out requirements for cyber security measures to be implemented into devices. Therefore, a general obligation to implement reasonable security measures should be supplemented by reference to standards that are updated as conditions change. A choice of standards (as long as all standards are adequate), rather than only one standard, can offer businesses who source their products from a variety of different jurisdictions some flexibility.

Enforcement by an appropriately skilled, resourced and activist regulator is crucial. In the Call for Views, the OAIC has been proposed as an appropriate regulator for cyber security issues, because of its current remit in relation to personal information. It is not realistic to assume that consumers, almost all of whom

[18] For an expanded discussion on this concept in the context of regulation of another form of sociotechnical change, see K Manwaring, 'Surfing the third wave of computing: Consumer Contracting with eObjects in Australia' (PhD thesis, University of New South Wales, 2019), http://handle.unsw.edu.au/1959.4/64921, pp 321-325.

[19] See K Manwaring and R Clarke, 'Is your television spying on you? The Internet of Things needs more than self-regulation' (2021) 93 Computers and Law: Journal for the Australian and New Zealand Societies for Computers and the Law 31-36

buy goods at prices well below the cost of litigation, would regularly engage in substantial litigation in relation to smart devices. Therefore, in order to ensure appropriate enforcement, a regulator will need to be empowered to bring actions on their behalf. This regulator will need to be appropriately skilled, resourced and empowered to act. The Hayne Royal Commission's[20] assessment of the failure of ASIC to properly enforce financial services legislation and the resulting misconduct by the financial services industry underlines this need.

A substantial critique and comparison of the regulatory activities, skills and resources of both the OAIC and the ACCC has recently been published.[21] In the light of these criticisms, and also in light of the OAIC's lack of experience in relation to physical safety and physical goods, we would recommend against the use of the OAIC as a regulator in relation to smart devices. We would suggest the ACCC (who has significant experience in safety) or a stand-alone cyber security regulator.

Successful regulation would require additional resourcing and change of culture. As has been evidenced from three and half years of the Notifiable Data Breach Scheme, there has been no demonstrable change in reporting statistics and the AOIC has completed no own-motion investigations, resulting in no available sanctions being delivered.

Question 12

Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices

In relation to standards relating to smart devices, we reiterate some important points from question 4 above, namely:

- Australia should be directly involved in standards development, and diverse actors (such as consumer organisations) should be supported to participate.
- A suite of alternative standards should be offered to meet compliance, where more than one acceptable standard exists.
- The provision of subsidised access to standards for SMEs and consumer bodies.

Rather than regulating the devices directly the Department should also consider the possibility of network-level security monitoring and reporting standards.[22]

It is clear that if it were possible to regulate and assure individual smart devices it would address a large and growing category of cyber security/privacy risks to the citizenry and organisations. It is worth noting however that there are a number of factors that may well make it difficult technically (e.g. form factor), economically (if per unit compliance costs exceed likely sale cost of device) or comprehensively (direct imports) to ensure that all smart devices arriving in Australia comply with particular standards. One possible gap arising from the Government's Call for Views is the omission of any substantive discussion of the role of network-level security solutions and standards relating to smart devices. We recommend that the government investigate the potential of these. For example, UNSW researchers have developed an approach that can:

- augment existing security solutions implemented by smart device manufacturers; and/or

[20] Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry ('RCMBSFS') (Final Report, 2019).

[21] K Manwaring, K Kemp and R Nicholls (mis)Informed Consent in Australia (Report for iappANZ, 31 March 2021) (UNSWorks, http://handle.unsw.edu.au/1959.4/unsworks_75600]), Ch 3 (by Dr K Kemp).

[22] This section is based on research in which Dr Hassan Habibi Gharakheili of UNSW has been involved in since 2015.

- provide security capabilities in circumstances where manufacturers are unable or unwilling to support device-level security.[23]

In 2019 the Internet Engineering Task Force (**IETF**) ratified a relevant new standard (RFC 8520), called the 'Manufacturer Usage Description' (**MUD**).[24] This standard provides the first formal framework for Internet of Things (**IoT**) devices behaviour that can be rigorously enforced. This framework requires manufacturers to publish a behavioural profile of their IoT device, that is, how their device is *expected* to behave when installed in a network.

The MUD standard provides a lightweight model to enforce effective baseline security for IoT devices. Access to a MUD profile allows a network provider (such as an ISP) to lock down and/or verify the network behaviour of a smart device in any operating environment. It allows a network to auto-configure the required network access for the devices so that they can perform their intended functions without having unrestricted network privileges.

The research team at UNSW closely collaborated with the authors of MUD, and developed an opensource tool (**MUDgee**), to assist IoT manufacturers in generating MUD profiles. This tool has been adopted by academia and industry.[25] This research team was also the first group to publicly release (https://iotanalytics.unsw.edu.au/) the MUD profile of 28 consumer IoT devices. The research team has published a significant body of work on network-level security,[26] MUD and the MUDgee tool.[27]

In addition to MUD, there is a new paradigm called "Software Bill of Material" (**S-BOM**), advocated by the US National Telecommunications and Information Administration (**NTIA**). Like the MUD, manufacturers of IoT devices are expected to publish formal descriptions (S-BOM profile) of what pieces of software are included in their devices. S-BOM will be an invaluable tool for managing cyber security and software supply chain risk since vulnerabilities in a software component will probably impact millions of devices. UNSW researchers are currently involved in a research project to contribute to the S-BOM paradigm. The IETF is currently discussing how an extension to the MUD could allow the S-BOM profile to be retrieved as well,[28] allowing network providers (and regulators!) to have access to both sets of information relevant to security.

The role of ISPs is also important. ISPs traditionally have not seen sufficient incentive to examine the behaviour of individual smart devices in home networks, and the set-up of home networks usually means that this type of network activity is not visible to ISPs. Putting consideration of user privacy and home network autonomy to the side it is certainly the case , technically speaking it is possible to give network providers greater visibility into smart devices connected *within* home networks. This greater visibility could provide ISPs with the capability to monitor (continuously and/or on-demand) the behaviour of

---

[23] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli and O. Mehani, 'Network-level security and privacy control for smart-home IoT devices' *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 163-167, doi: 10.1109/WiMOB.2015.7347956.

[24] See IETF Specification at https://datatracker.ietf.org/doc/html/rfc8520. See also National Institute of Standards and Technology (**NIST**), National Cybersecurity Center of Excellence, 'Securing Home Smart devices Using MUD' (Web Page) <https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos/securing-home-iot-devices>.

[25] Including NIST.

[26] Ibid and a magazine-style article at H. H Gharakheili, A. Sivanathan, A. Hamza and V. Sivaraman, 'Network-Level Security for the Internet of Things: Opportunities and Challenges' *Computer*, vol. 52, no. 8, pp. 58-62, Aug. 2019, doi: 10.1109/MC.2019.2917972

[27] See eg; A Hamza, D Ranathunga, H H Gharakheili, M Roughan, and V Sivaraman,'Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles'. In *Proceedings of the 2018 Workshop on IoT Security and Privacy* (IoT S&P '18, Budapest, Hungary 20 August 2018) 8–14 and A Hamza et al, 'Verifying and Monitoring IoTs Network Behavior using MUD Profiles' (2020) *IEEE Transactions on Dependable and Secure Computing*.

[28] See the IETF Internet Draft at (https://datatracker.ietf.org/doc/html/draft-lear-opsawg-mud-sbom-00)

individual devices inside home networks, and report on their cyber health. Importantly, they would then have the technical capability to verify whether or not the observed behaviour of smart devices conforms to what is claimed by manufacturers in a MUD profile.

Increased device-level visibility has some profit potential for ISPs, as it will allow them to provide managed services to consumers, such as security-as-a-service (**SECaaS**), quota management and parental controls.[29] This could perhaps provide benefits not only to the ISPs, but also consumers, manufacturers and content providers. For example, SECaaS could go a long way towards limiting the impact of complexity on the average consumer, as well as vulnerable consumers.

Network-level security measures can augment device-level security. They can also act as a replacement where device-level security implementation cannot be achieved. In both cases, however, implementation would require smart device manufacturers to publish the 'expected behaviour' of devices in the form of MUD profiles (preferably including the S-BOM information). While much cheaper for manufacturers than actual changes to their devices, to ensure compliance this should be mandated.

Network-level security requirements could also provide an additional or replacement point of regulation, that of ISP behaviour. This could take several forms, such as requirements to provide SECaaS to consumers and/or report risk patterns or unusual device behaviour to regulators.[30] However, because this does require increased visibility into individual devices connected into a home network, the impact on consumer privacy would need to be considered, and strict protections put in place around identification of individual consumers.

Question 14

What would be the costs of a mandatory standard for smart devices for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?

The cost has two dimensions: the complexity of designing and building devices so that they comply; and of monitoring and enforcing compliance. Hence the total cost is closely tied to how strict the standards adopted are.

The first type of cost – that of designing and building in compliance is likely not a real cost - in that devices which do not comply with sensible requirements are not devices we would want Australian consumers to have. Much like cars without seatbelts, or electrical devices with unsafe earthing, or unhygienic food products.

The second category of costs depend upon the level of strictness of the regulation. One possible approach if cost turns out to be a blocking factor would be to introduce a broad but low level of regulation initially and then adjust this over time to respond to the emerging threats and attacks experienced. This would reduce the likelihood of inadvertent initial overregulation stifling innovation and functionality while creating a framework for delivering evidence-based improvements to regulation in an ongoing way as the cyber risk landscape continues to evolve.

When considering the question of regulation cost, it is important that regulation costs should viewed as balanced against the benefits. This involves the prospect and scale of future harms prevented, particularly

---

[29] H H Gharakheili and V Sivaraman. 2017. 'Cloud assisted home networks'. In Proceedings of the 2nd Workshop on Cloud-Assisted Networking (CAN '17). Association for Computing Machinery 31–36.

[30] The ACCC currently monitors (through ISPs) and publishes broadband performance data https://www.accc.gov.au/consumers/internet-landline-services/broadband-performance-data.

seeing the growth in smart devices, brought about by new technologies (such as 5G). By 2025 it is expected there will be approximately 40 billion devices and over 80% on 5G networks.[31] with innovations in 'edge computing' and recent contracts between ISPs and Amazon Web Services (AWS). These innovations are also open to their own vulnerabilities, such as power outages that create permanent hardware operation damage that restricts retrieval of data.[32] For example, the opportunity for targeted DDoS attacks will increase with the growing number of attack surfaces, like the advent of 'island hopping' attacks vulnerable via the outsourcing to RS (remote storage) or trusted third parties. This means there is a need for supply chain risk assessments: ranked as a high priority for APAC and European respondents.[33]

Question 16

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

Labelling may be *helpful* in encouraging consumers to become aware of cyber security in relation to smart devices, and consequently improving their purchasing choices in this area. The components of smart devices that make devices secure/insecure cannot be readily discerned by an ordinary consumer inspecting the goods and unsecure smart devices are visually indistinguishable from safe equivalents. It could also assist in raising awareness of appropriate device management measures.

However, labelling alone without education cannot be considered as anything other than a small part of the solution, considering the large range of price points (from budget to premium) for, and the large variety of, smart devices. Consumer devices range from the sensible (eg smart thermostats) to the frivolous (eg a soap dispenser that connects to a smart home hub so that it can sing and tell jokes).[34] Motivations other than security are likely, in many cases, to dominate a purchasing decision.

Labelling may be most helpful in encouraging *premium* brands to improve their cyber security practices. Without labels, consumers aware of the importance of cyber security are more likely to mistakenly assume that products from lesser-known manufacturers are unsafe, whereas reputable branded products are safe(r). However, labelling is problematic unless consumers are educated on what the labels are proposed to achieve. For example, food labelling research has shown many shoppers find food labels confusing which leads to many people not really understanding what they are eating.[35]

A significant research study has just been completed on the value of *privacy* icons applied to smart devices. This study included interviews with 844 consumers and 32 experts. While there was some 'notional support for an icon system to enhance consumer awareness of the privacy implications of CIoTs', it was 'recommended that an icon… system be incorporated into a broader process of reform to current privacy and consumer protection laws, which includes enhanced enforcement and placing

[31] https://www.itnews.com.au/feature/optimising-businesses-on-the-edge-567054

[32] On August 31, 2019, an Amazon AWS US-EAST-1 data center in North Virginia experienced a power failure. After the power was restored, some EC2 instances and EBS volumes incurred hardware damage and the data stored on them were no longer recoverable. L. Abrams, 'Amazon AWS Outage Shows Data in the Cloud Is Not Always Safe', Sep. 2019, Online. Available: https://www.bleepingcomputer.com/news/technology/amazon-aws-outage-shows-data-in-the-cloud-is-not-always-safe.

[33]https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/TELE0394_Security_2019_WhitePaper_Digital_V14_compressed.pdf

[34] By Amazon. https://www.theverge.com/2021/8/3/22607219/alexa-smart-soap-dispenser-price-specs.

[35] Dawn Liu, Marie Juanchich, Miroslav Sirota, Sheina Orbell, 'People overestimate verbal quantities of nutrients on nutrition labels', Food Quality and Preference, Volume 78, 2019

increased obligations on the [smart devices] industry to participate in these processes.'[36] Considering the considerable intersections between privacy and security in relation to smart devices, much of the learning in this study could be applied to this consultation process.

We agree that security labelling is unlikely to work unless there is a mandatory and enforced punitive regime for manufacturers who do not place labels on devices. Accuracy of labels is also essential but may not need additional regulation as it is already covered under provisions of the ACL prohibiting misleading or deceptive conduct, and false or misleading representations.

One interesting possibility introduced by the universal provision of labels is the capability to carry additional consumer security functionality not currently possible. For example, QR codes which link to resources for maintaining and upgrading the device, privacy policies, latest security audits and so forth. The ability to access such information in an authoritative way would make more effective requirements for companies to provide it.

For further example, currently, if consumers of companies wish to evaluate the security of legacy devices on their network or home or to access information about them, there is no universal way to enable this. A mandatory QR code linking to such resources, perhaps on a government repository, would be of considerable benefit for those educated to look for them. Many additional features could piggyback on such an enabling infrastructure – for example code, update, and manual repositories for those wishing to maintain and repair their own devices. This would be attractive for "right to repair" style capabilities.

It is likely that mandatory security labels, like electrical compliance and clothing and mattress tags, would facilitate many future security enhancements such as the examples outlines above but not yet envisioned, by empowering the consumer and owner of the good with more information about the nature of what they have purchased, which would normally not be disclosed by the manufacturer and which most consumers are not capable, or legally permitted under patent restrictions, to discover for themselves.

Question 17

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

The device management issue noted above (and the nature of vulnerabilities being exposed over time) means that, while labelling and standards will be effective in *increasing* cyber security, they are not panaceas. Labelling and standards, in theory, could reduce time and complexity for a regulator or consumer seeking to enforce consumer rights. Clearer expectations for device security would support and assist regulators' and ordinary consumers' understanding of if and how consumer rights are breached when a device has failed (or is at risk of failure). However, the labels and standards are unlikely to be sufficient in themselves without some form of **mandatory** implementation.

[36] I Warren, M Mann, D Harkin, *Enhancing Consumer Awareness of Privacy and the Internet of Things*, (ACCAN report, August 2021) https://accan.org.au/files/Grants/2021%20Deakin%20IoT/Deakin%20grants%20report_v5_web.pdf, 6.

Question 20

Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

Smartphones and the applications installed on them form an integral part of many systems in which other smart devices participate, primarily as a remote controller and also often the device to which data is transmitted and delivered to humans in an intelligible form. Vulnerable endpoints, including smartphone devices, will inevitably compromise the security of network ecosystems containing smart devices. Fortunately, mobile phones have not suffered from the same level of security issues as smart devices. However, depressed economic conditions during and post-COVID may lead to a lowering of quality standards. Additionally, as tasks once accomplished in the office are now handled "in the field," like in cafés or homes and with mobile devices in challenging environments that should be weighed against the need to protect sensitive data, address privacy concerns, financial costs and personal flexibility. Therefore, there should be some form of regulated minimum cyber security standard for smartphones so that existing security practices are not abandoned, and labelling could form part of this scheme. NIST provides guidance here, for example developing use cases specific to any business or organizational needs for mobile devices to identify and clearly describe requirements and assessments proportional to risk like understanding who users are, their need for mobile devices, what apps or device features will be necessary to meet their needs against a set of aims necessary to meet organisational objectives.[37]

Question 21

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

Any label must be placed in front of the consumer contemplating a purchase at the earliest possible opportunity with minimal consumer intervention. An effective labelling scheme should not and cannot rely on a consumer having to expend much time locating device labelling for themselves. The form of any label must consider the consumer's purchasing context. For the foreseeable future, at least some purchases will continue to be made in physical stores. A label scheme must be supported in physical stores, which may require physical labelling. However, labelling should also be cost effective and able to be altered as required (a label might need to be amended as new security information becomes known to a manufacturer). Physical labels could consist of a QR code or some other unique digital tag, leading to a product or service provider's website. However, this requires that regulation be in place preventing manufacturers amending security labelling information at will, without appropriate recall, refund options and notification processes.

Question 26

What issues have arisen to demonstrate any gaps in the ACL in terms of its application to digital products and cyber security risk?

There is little instructive case law clarifying how the Australian Consumer Law (**ACL**) may apply to unique harms resulting from the use of smart devices. This is concerning as the ACL's effectiveness is likely to be reduced when the application of its provisions to a factual scenario is uncertain or ambiguous. Under the ACL, consumer goods are sold subject to a guarantee of 'acceptable quality' under s 54 of the *Australian*

37 Refer to 5.1.1 Explore Mobile Use Cases p28 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2-draft.pdf

Consumer Law (ACL) (and 'due care and skill' for services under s 60). The effectiveness of a consumer guarantee scheme in promoting cyber hygiene depends on:

(1) consumers having a clear understanding as to how and when relief under the ACL may be available; and
(2) on business understanding their obligations under the scheme.

However, consider this scenario and others like it. A lamp that does not turn on is obviously not of acceptable quality. However, can the same be said of an Internet-connected lamp that **does** turn on, **does** connect to the Internet and perform all of its advertised functions, but also contains a security vulnerability? What if this security vulnerability allows a rogue to hack into your smart house system, turn off the sprinklers and the fire alarm, and turn on the stovetop, causing a fire in the kitchen? The rogue is often not discoverable, but will the supplier be liable in this circumstance? The uncertainty of the answer to this type of question was reflected in the 2017 ACL Review Final Report which concluded 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*.[38]

Practical issues also arise. The nature of cyber security attacks, particularly those involving misuse of data, is that in some cases a consumer may remain completely unaware that any such harm has or could occur. Provisions such as the consumer guarantees, requires awareness of a harm or fault (or that a risk of harm or fault exists). If, for example, a consumer's personal data is exfiltrated due to poor security, a consumer may never become aware of this, or only become aware much later but remain unaware of the source of the harm or be able to attribute it to a single device (especially if multiple smart devices are connected to the same network, which is common).

Certain more common smart device security issues, such as the use of default or universal passwords, ***may*** be covered by consumer guarantees on acceptable quality for exposing a consumer to an unacceptable risk of harm.[39] However, until a judge answers the specific question as to on which side of the 'acceptable quality' line particular kinds of security vulnerabilities lie, consumers, suppliers and insurance companies will not know how the law applies in this situation. And, as factual situations shift, this uncertainty will continue. The consequences of this uncertainty outside of judicial decisions may not favour the consumer, nor promote good security practices by suppliers. For example, while consumer guarantees of acceptable quality cannot be excluded by contract, the ACL allows specific disclosures by a supplier to remove the protection of this guarantee.[40] Consequently, suppliers may include in their terms and conditions (rarely read by consumers) a clause that disclaims that any cyber security protections are included with the device. This will be cheaper and easier for suppliers than implementing security measures, but more detrimental to consumers.

Other uncertainties also arise in relation to the consumer guarantees. For example, it is also uncertain how goods that become insecure *over time* due to the inadequate provision of software updates or patches will be dealt with under the consumer guarantees, as acceptable quality is determined at the

---

[38] Consumer Affairs Australian and New Zealand, *Australian Consumer Law Review Final Report* (March 2017), 96.

[39] UNSW researchers are currently undertaking a doctrinal analysis of this question. No cases on smart devices exist in Australia, but principles in relation to other consumer goods discussed in *Capic v Ford Motor Company of Australia Pty Ltd* [608]-[613]; *Protec Pacific Pty Ltd v Steuler Services GmbH & Co* KG [2014] VSCA 338 [516]-[531]; *Medtel v Courtney* (2003) 130 FCR 182 may be of assistance.

[40] *Competition and Consumer Act 2010* (Cth), Australian Consumer Law, Schedule 2, ss54(2)– (4).

time of supply. There are also potential difficulties with applying remedial provisions in the context of smart devices and related services that have some form of autonomous decision-making. For example, s 259(5) of the ACL precludes damages for harm for 'a cause independent of human control that occurred after the goods left the control of the supplier'. It is unclear how this provision will be interpreted if, for example, a remedy was sought for damage caused by AI-driven botnets hijacking smart devices.[41] The data collected by smart devices and transferred to manufacturers can further create a secondary power imbalance between a consumer and manufacturer if a consumer seeks to access an ACL remedy. Data collected by smart devices (including usage and wear data) empowers a manufacturer to monitor a smart device's ongoing functionality. Consumers do not ordinarily have the advantage of this information. In theory, this information could be unfairly relied on by a manufacturer to avoid liability if used to mount arguments against a consumer's claim.

The same points about uncertainty can be made about the sections of the ACL dealing with the liability of manufacturers of goods with safety defects (Ch 3 Pt 5) and product safety (Ch 3 Pt 3-3). The question remains: in what circumstances does poor security practice make a 'unsafe' product?

This analysis is by no means comprehensive. The ACL Review Final Report concluded that there was a need to provide more investigation and specific guidance relating to digital products under the ACL, but this guidance has not been provided by the relevant regulatory agencies.

Question 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?

Reforms being considered to the *Privacy Act* will not adequately cover the field in relation to smart devices. For example, not all data collected by smart devices will fall under the definition of 'personal information'. A cyber attacker hijacking a large amount of smart devices to use in a botnet to carry out a DDOS attack may **never** use personal information in that attack. Additionally, not all manufacturers of smart devices, and those providing additional services relating to smart devices, fall within the scope of the Act in the first place. Therefore, personal enforcement rights for data breaches, if this is introduced, will have limited effectiveness as it relates to smart devices.

Reforms being considered for the ACL include the introduction of a civil prohibition against failing to provide a consumer guarantee remedy. This would assist consumers who have been wrongly denied a remedy because of third-party repair at some earlier occasion. For issues unique to smart devices mentioned above, for example the circumstances creating the conditions for unauthorised access or data exfiltration, it is difficult to appreciate how a civil prohibition against failing to provide a remedy would adequately address these harms.

The current proposed measures on strengthening protections against unfair contract terms,[41] may have an effect, albeit a limited one. The licence for use of devices is usually a standard form agreement. Unfair terms in such agreements in relation to a product or a class of products would also apply. Terms unreasonably excluding liability for harm related to cyber-attacks may be considered unfair, although it would be better again for business certainty that this be made explicit rather than waiting for a court decision.

---

[41] D Chema, 'The next generation of cyber-AI defense and the emerging AI-driven IOT botnet crisis' *Cyber Defense Magazine* (13 April 2019) https://www.cyberdefensemagazine.com/the-next-generation-of-cyber-ai-defense-and-the-emerging-ai-driven-iot-botnet-crisis/

However, other types of amendments to the ACL hold more promise, as the fair trading agencies are experienced and often effective as enforcers in relation to goods or services which cause physical or economic harm (when given power to do so). Clarifying or extending the reach of the ACL (in relation to the consumer guarantees, liability of manufacturers of goods with safety defects, and product safety) is a more promising approach. Amendments would need to make it clear that these provisions of the ACL do extend to poor cyber security practices, and the declaration of a cyber security product safety standard under Ch 3 Pt 3-3 should be considered. If this approach is taken, care should be taken to ensure that **services** related to smart devices (for example, cloud data processing services) are also covered. The decision in *Valve*[42] still leaves much uncertainty as to in what circumstances 'software as a service' and data analytics services (common in smart devices) will be considered a good or a service.

Question 28 – Strict Liability

The Call for Views describes the externality problem of cyber security - that most of the harm of a security flaw is outsourced to consumers and data subjects, so the incentive for good practice is less than it should be. If the average outsourced cost of a cyber incident could be quantified (as say $x - although this may vary by category of incident), then one could take a direct approach to removing the externality.

Suppose personal information "held" (for the purposes of the *Privacy Act*) by an entity is accessed by a malicious actor. Alternatively, suppose that an IoT device is compromised by a malicious actor, leading to privacy or other harm (although for simplicity, we focus here on the data breach example). The proposal that the relevant entity (for example the entity responsible under the Privacy Act) pay to a fund $x multiplied by the number of Australians affected. Such a legal change would have several effects:

- Entities holding data would delete personal information that has no known value - thus decreasing the risk of data breach for all Australians.
- Insurance would be easy to calculate (eg $x times number of people whose data is stored times estimate of security risk).
- Insurance would likely be priced so as to correspond to risk (which relates to security measures taken) and volume of data held.
- Entities seeking to reduce insurance costs would thus both delete unneeded personal data (as per above) and improve their security settings. But this would be done only to the extent that it (approximately) internalises the risk - there would be no incentive to over-invest in security.
- The government would no longer need to set standards as this would be done *de facto* by the insurance industry.

In terms of how the fund would be used, one can allow for compensation for those who can provide evidence of harm as well as possibly (depending on the modelling) a small payment for those affected who cannot prove harm (but may nevertheless be stressed or inconvenienced). This is both more useful for consumers who are harmed than the expense and vagaries of litigation (even assuming some of the suggestions proposed in the Call for Views are adopted). Consumers also need only prove that there has been a breach and that they were affected (and harmed), not prove that systems they cannot see are not compliant. It might also be preferable for those made liable under it due to its quantifiable nature (again, compared to the vagaries of litigation). But the primary focus is on consumers and ensuring that they are compensated for harm suffered irrespective of their ability or willingness to identify the correct defendant, obtain access to information necessary to make out a claim, hire expertise to understand why the breach occurred, and then pursue a remedy in court.

In addition to efficiency and reducing the costs associated with litigation, the primary advantage of this approach compared to liability for negligence or breach of the privacy principles is that the consumer does not have to prove something that may be beyond their knowledge and expertise.

If this (or a variation of it) were adopted, it would need to be managed by a government agency. The data breach scheme runs through the OAIC, so that is one possibility. However, it is only likely to work if the agency is properly resourced and its mandate expanded beyond information and privacy (which tends to be a political orphan) to "cyber security". Alternatively, if a separate cyber security regulator were established, then that might be the better home.

There is obviously more work to do to develop this proposal, and we are happy to engage with the Department in undertaking the necessary research should the proposal prove of interest.

Question 28 – Prospects of international harmonisation

We believe that businesses, consumers and regulators may benefit from international legal harmonisation and standardisation of supervisory expectations.[42] This can be helpful for a number of reasons. First, only a coordinated international response is able to address adequately the cross-border nature of cyber threats, which 'requires a high degree of alignment of national regulatory and supervisory requirements and expectations'.[43] Second, harmonisation can help to deal with existing (and potential) overlaps in cyber security regulation, such as conflicting cyber incident reporting requirements that may apply to Australian businesses operating in multiple jurisdictions. Furthermore, harmonisation can provide useful guidance for overseas legislatures and regulators lacking cyber security expertise – thereby helping to increase the overall level of cyber security on a regional (APAC) and global scale. This is particularly important given that, in our experience, there is a considerable dearth in cyber security expertise across developing and least developed economies.

We anticipate that demand for international harmonisation will be different across various sectors of the economy. For example, the financial services sector is more likely to benefit from such harmonisation in the short to medium term, considering the emergence of innovative payment instruments that call for a coordinated international response – in particular, global stablecoins (GSCs) such as Libra/Diem and so-called central bank digital currencies (CBDCs) such as e-CNY developed by the People's Bank of China (not to mention new digital forms of the Australian dollar that could be issued in the future as a response to e-CNY and similar initiatives from other major economies).

Cyber security risks associated with GSCs and CBDCs are more significant due to the increased data concentration that characterises these initiatives. Global stablecoins are, by definition, offered on a wide basis, potentially with systemic implications. CBDCs can be designed to cover a large customer user base (which could be economy-wide or even international). This can make GSC and CBDC platforms attractive targets for cyber attackers, with possible major systemic consequences resulting from successful breaches.

The design of GSCs and CBDCs will determine the magnitude of associated cyber security risks. For example, one important factor is the number and types of end-users with access to new currency types: 'Defending against cyber attacks will be made more difficult as the number of endpoints in a

[42] For a detailed analysis of the benefits and challenges of legal harmonisation in the area of cyber security, see Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond', Uniform Law Review (2020) Vol 25, Issue 1, 125-167 <https://doi.org/10.1093/ulr/unaa006>.

[43] European Commission, 'FinTech Action Plan: For a More Competitive and Innovative European Financial Sector' (2018) 15 <https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC_1&format=PDF>.

general purpose CBDC system will be significantly larger than those of current wholesale central bank systems.'[44]

We expect interlinkages between domestic CBDC platforms to be established in the future, as interoperability is increasingly becoming an essential component of CBDC designs. The recent joint acknowledgement of its importance by a group of central banks (Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England and the Board of Governors of the Federal Reserve System) is an important first step in this direction:

> 'The potential for *cross-border interoperability* should be considered by central banks from the outset of research on CBDC (focusing on broad harmonisation and compatibility between currencies to encourage safe and efficient transfers). The central banks in this group are therefore *committed to coordinating* as we move forward with our own domestic choices, exploring practical issues and challenges.'[45]

Regulatory harmonisation of cyber security regulation in finance is further facilitated by numerous international bodies (including the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the Financial Stability Board (FSB), the Group of Seven (G7), the International Association of Insurance Supervisors (IAIS), the International Monetary Fund (IMF), the International Organization of Securities Commissions (IOSCO), the Organisation for Economic Co-operation and Development (OECD), and the World Bank Group) issuing relevant (albeit high-level and often exploratory) guidelines.

While the financial sector may benefit the most from international harmonisation of cyber security regulations in the immediate future, it is worth identifying other sectors of the economy that may equally benefit from harmonisation or initiatives that could help improve cyber security on an economy-wide basis. One area to consider is harmonisation of any licensing regimes (if established) for cyber security service providers.

This important work should be led by the Cyber Affairs and Critical Technologies Ambassador. This position has been in place for nearly five years and has made no demonstrable difference to any harmonisation efforts.

Question 28 – Cross-jurisdictional learning

In recent years, the cyber security regulatory landscape overseas has undergone significant change. Bespoke cyber security laws and regulations have replaced pre-existing general risk management and business continuity rules in a number of jurisdictions, including the European Union, Hong Kong, Russia, the USA, and Singapore.[46] A characteristic feature of the new cyber security frameworks is their consideration of cyber risks and cyber security from more general issues. They also designate different 'tiers' of cyber security regulation (with corresponding levels of expectation and obligations for entities in those tiers). In the light of the emergence of these new legal frameworks, we encourage extensive comparative research to identify whether aspects that are proven to be effective overseas may be adaptable to an Australian context. In particular, it is worth exploring, through comparative research, the benefits and disadvantages of specific (as opposed to general) regulation in this area.

---

[44] Bank for International Settlements, 'Central Bank Digital Currencies: Foundational Principles and Core Features' (Report No 1, 2020) 5 <https://www.bis.org/publ/othp33.pdf>.

[45] Ibid 17 (emphasis added).

[46] For more detail, see Anton Didenko, 'Cyber security Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond', Uniform Law Review (2020) Vol 25, Issue 1, 125-167 <https://doi.org/10.1093/ulr/unaa006>.

A recurring challenge in designing cyber security frameworks is the need to keep regulations up to date in the light of emerging technologies and increasing sophistication of attackers. In response to this challenge, some of the rules overseas incorporate references to best practices and the latest technological developments in the context of designing cyber security frameworks. Some contain provisions considering the *current level of technology*. For example, under the GDPR in the European Union, technical and organisational measures to ensure security of data processing must be implemented 'taking into account the *state of the art*'.[47] Others implement provisions focused on *current best practices*. For example, the Cyber Resilience Oversight Expectations for Financial Market Infrastructures of the European Central Bank expect financial market infrastructures to 'employ *best practices* when implementing changes' at the basic ('evolving') level of cyber resilience expectation[48] and to set up change management process based on 'well-established and industry-recognised standards and *best practices*' at the 'advancing' level.[49]

Both groups aim to facilitate the highest possible (at the time) level of preparedness and deliberately use discreet language, generally encouraging the use of up-to-date techniques, but not always making them mandatory. Yet, the scope of the two approaches is slightly different. The first group is concerned with the level of technology—that is, *what is physically possible* at the time. The second group is more reactive, as it is based on the *current level of industry practices*, which may or may not adequately tackle cyber security issues at the current level of technology. As a result, the former group likely aimed at more sophisticated firms with sufficient resources to analyse the level of technological advancement in the entire sector.[50]

Yours sincerely,

Lyria Bennett Moses, on behalf of the UNSW Allens Hub

Marina Yastreboff, on behalf of AUSCL

Monica Whitty, on behalf of IFCYBER

With thanks to the authors (listed alphabetically):

Lyria Bennett Moses, Richard Buckland, Benjamin James Di Marco, Anton N Didenko,[551] Hassan Habibi Gharakheili, Kayleen Manwaring, Jessemyn Modini, Rob Nicholls, Nigel Phair, Simon M Taylor, Shengshi Zhao.

[47] Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) (OJ L 119/1), Article 32(1).

[48] European Central Bank, Cyber Resilience Oversight Expectations for Financial Market Infrastructures' (2018) <https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf>, s 2.3.2.1(44).

[49] Ibid, s 2.3.2.1(52).

[50] For further analysis of this issue see Anton Didenko, 'Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond', Uniform Law Review (2020) Vol 25, Issue 1, 158-160 <https://doi.org/10.1093/ulr/unaa006>.

[51] The research conducted by Anton N Didenko was funded by the Australian Government through the Australian Research Council (project FL200100007 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks'). The views expressed are those of the author and are not necessarily those of the Australian Government or Australian Research Council.

Appendix A – Background research on smart devices

The nature of security vulnerabilities in smart devices

Security flaws in Internet of Things ('IoT') devices are acknowledged to be common, more common than those found in conventional computing. Security vulnerabilities have been found in Internet-connected toys, televisions, security cameras, door locks, medical devices, fitness trackers, baby monitors, cars and even guns.[52] This increased risk of remote attack is substantially due to the existence of particular security vulnerabilities in the smart devices themselves and the systems in which they participate, such as:

- insecure network services, interfaces, software and/or firmware;
- missing or unstable interoperability between market platforms[53];
- lack of encryption;
- insufficient authentication and authorisation and/or security configurability;
- the way personal data is stored; and
- the lack of physical safeguards.[54]

These vulnerabilities can leave the devices open to remote attacks. Consequences of these types of attacks include:

- disclosure or modification of sensitive **data**;
- attacks against **other** smart devices or conventional computers; and/or
- **physical harm** to or destruction of the smart devices, surrounding objects and/or people.[55]

Factors leading to poor security outcomes for smart devices include:

- low profit margins and subsequent low-cost design choices;[56]
- the inexperience of (and possible lack of interest by) consumer goods manufacturers in security issues (as compared to specialist IT manufacturers);[57]

---

[52] K Manwaring, 'Emerging information technologies: challenges for consumers' (2017) 17(2) Oxford University Commonwealth Law Journal 265, 267.

[53] With more than more than 300 IoT platforms in the current market, and more to come: 'each promoting its own IoT infrastructure, proprietary protocols and interfaces, incompatible standards, formats etc. in closed systems (sometimes called stove pipes or silos). Nevertheless, with a necessity for these different solutions to seamlessly work together'. M Noura, M Atiquzzaman & M Gaedke, Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Network Applications 24, 796–809 (2019). https://doi.org/10.1007/s11036-018-1089-9

[54] This is a consolidated list adapted from Open Web Application Security Project (OWASP), 'OWASP Internet of Things Project' (2014) <www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29> accessed 12 January 2017.

[55] This is a consolidated list adapted from Cloud Security Alliance, 'Security Guidance for Early Adopters of the Internet of Things (IoT)' (Mobile Working Group, Peer Reviewed Document, April 2015) <https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf> accessed 8 July 2017.

[56] K Boeckl and others, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (National Institute of Standards and Technology Internal Report 8228 (Draft), September 2018) 7–8.

[57] S R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85, 94.

- the small size of some devices rendering them unable to support the processing power and energy demands required for strong security measures such as encryption;[58]
- many devices having been designed (for reasons of cost and fitness for purpose) in such a way that hardware and software access, management, and/or monitoring are difficult or impossible.[59] For example, some devices are not designed to accommodate software updates, making security patches unworkable;[60]
- the sheer number of attack surfaces available to an attacker when many smart devices are connected to one organisation's network;[61] and
- the fact that common post-market cyber security controls used for conventional IT (such as firewalls, anti-malware servers or network-based intrusion prevention systems) may be ineffective for smart devices, as smart devices may use alternative protocols or communicate point-to-point rather than through a monitored infrastructure network;[62] and
- many consumers do not understand, or have access to, the different security practices needed to protect themselves across a range of devices used for health, safety, food, information, entertainment and transport.[63]

Security problems with consumer smart devices may also be exacerbated when security features are furnished by a service provider that disappears from the provider network and is not replaced, resulting in the absence of both expertise and security updates. This might happen when a service provider becomes subject to external administration, or management makes a business decision to stop supporting the

---

[58] Ibid. Some smart devices, such as mobile phones, have access to large amounts of processing power, memory and storage. Others, such as low-power sensors, draw from alternative energy sources to access what is effectively unlimited power for their lifetime. However, for many smart devices, resource constraints will drive a design that will not be optimal on all fronts. Some security methods commonly used in conventional computing, such as crypto-processing, are notably detrimentally affected by resource constraints, such as the need to minimise power consumption, which can detrimentally affect processing power and speed. Current alternatives developed to overcome these constraints, such as lightweight cryptography methods, are known to trade off performance against resource drain, with the result that security may be compromised. See W J Buchanan, S Li and R Asif, Lightweight Cryptography Methods (Taylor & Francis 2017) 187, F Ayotunde Alaba and others, 'Internet of Things Security: A Survey' (2017) 88 Journal of Network and Computer Applications 10 and K Manwaring, 'Surfing the third wave of computing: Consumer Contracting with eObjects in Australia' (PhD Thesis, University of New South Wales, 2019) http://handle.unsw.edu.au/1959.4/64921, 183.

[59] K Boeckl and others, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (National Institute of Standards and Technology Internal Report 8228 (Draft), September 2018) 7–8. Problems can arise from '[l]ack of management features … [l]ack of interfaces … [d]ifficulties with management at scale … [a w]ide variety of software to manage … [d]iffering lifespan expectations … [u]nserviceable hardware … [l]ack of inventory capabilities … [and h]eterogenous ownership'.

[60] S R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85, 135–36. Also see Bruce Schneier, 'The Internet of Things is Wildly Insecure – And Often Unpatchable' (Wired, 1 June 2014) <www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/> accessed 17 December 2015.

[61] K Rose, S Eldridge and L Chapin, The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World (Internet Society, October 2015), 21; American Bar Association Section of Science & Technology Law, Submission to the National Telecommunications and Information Administration, US Dept of Commerce, in response to Docket No. 160331306-6306-01: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things (2016) 11.

[62] K Boeckl and others, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (National Institute of Standards and Technology Internal Report 8228 (Draft), September 2018) 9.

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

relevant product (which may be motivated by attempts to minimise the threat of liability for existing defects that cannot be remedied without substantial investment).

Additionally, perpetrators do not even need to be themselves particularly skilled in cyber security exploits. Malware kits and development expertise can now be readily and anonymously purchased online in the form of 'hacking as a service'.[64]

The nature of the harms caused by poor security in smart devices

These security issues in smart devices can give rise to significant consumer and community harm. People can be subject to unwanted surveillance and harassment[65] in the home, not only by malicious strangers but also by intimate current and ex-partners.[66] Personal information can be exposed to the world[67] at large. Physical harm can arise from device failure or malfunction[68] caused by hackers, and malicious remote control of inherently dangerous connected objects.[69]

Consumers do not need to own, possess or be in proximity to devices to be harmed by them, such as when smart devices are hijacked and used in a 'distributed denial of service' (**DDOS**) attack.[70] During these attacks, the person that owns the device is usually unaware that their compromised devices are participating in the attack. Importantly, harms can be caused to parties other than those who own or operate the exploited device. For example, the increase in people working from home during the COVID-19 pandemic may enable hackers to start inside poorly-secured home networks, and apply the employee's privileges to get inside their employer's networks, further expanding the threats.[71] Convergence of consumer and enterprise IoT such as medical devices and smart energy meters has also been identified as an additional risk.[72]

One of the key consequences of technological developments related to smart devices is the re-emergence of physical spaces and places as an important concept in information technology.[73] One of the most obvious implications of the physicality of devices and systems in smart devices is their vulnerability to the

---

[64] L Ablon, Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data (Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, 15 March 2018) 9.

[65] D Lu, 'How Abusers Are Exploiting Smart Home Devices' Vice (online, 17 October 2019) <https://www.vice.com/en_au/article/d3akpk/smart-home-technology-stalking-harassment>

[66] N Bowles, 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' The New York Times (online, 23 June 2018) <www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>

[67] D Sun, 'Singapore home cams hacked and stolen footage sold on pornographic sites' The New Paper (online, 12 October 2020) <https://www.tnp.sg/news/singapore/hackers-hawk-explicit-videos-taken-spore-home-cams>

[68] Phys.org, 'Security flaw could have let hackers turn on smart ovens' (26 October 2017) <https://phys.org/news/2017-10-flaw-hackers-smart-ovens.html>

[69] A Greenberg, 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' Wired (online, 21 July 2015) <www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

[70] T Stevens, 'Internet of Things: when objects threaten national security' The Conversation (online, 29 May 2018) <https://theconversation.com/internet-of-things-when-objects-threaten-national-security-96962>

[71] B Buntz, 'Cybersecurity Crisis Management During the Coronavirus Pandemic' IoT World Today (online, 24 March 2020) <https://www.iotworldtoday.com/2020/03/24/cybersecurity-crisis-management-during-the-coronavirus-pandemic/>

[72] T Burton, 'Internet of Things Sets the Cat Among the Pigeons', Australian Financial Review (12 October 2020) <https://www.afr.com/technology/internet-of-things-sets-the-cat-among-the-pigeons-20201001-p5612g> quoting Lani Refiti, IoTSec Australia.

[73] Paul Dourish and Genevieve Bell, Divining a Digital Future: Mess and Mythology in Ubiquitous Computing (MIT Press 2011) ch 5; Anne Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (PhD thesis, University of Ottawa 2013) chs 1, 4.

security concerns outlined above, particularly in the example of security exploits of motor vehicles.[74] Attempts to cause physical damage may not even be **deliberate:** happenstance, error and unintended consequences (e.g. from attempts at surveillance and tracking[75]) can result in harmful security incidents, even without an intention to cause a specific type of harm.

Security researchers have developed proofs of concept to use botnets[76] of smart devices such as air conditioners and heaters to 'launch large-scale coordinated attacks on the power grid'.[77] Such measures are ripe for exploitation by criminal networks and terrorists, with potential to cause both physical and economic loss. Exploits could also be undertaken in order to benefit individual suppliers within an energy market, for example by forcing increased demand for power which in turn would raise prices for reserve power generators.[78]

The adult sex toy market appears to be subject to similar risks, with the potential for disturbing consequences. The first smart devices vibrator was released commercially in 2015, and since then security vulnerabilities have been identified in at least two connected vibrators on the market.[79] The risk of non-consensual access to these devices due to poor security raises the possibility of remote sexual assault.

The foundations of security must be established by the manufacturer of the device, but device management by end users during the life of the device is also important. For example, in late 2019, remote hackers were accused of yelling racial slurs at a child and at adults in separate incidents, via the speakers in Amazon-owned Ring security cameras. Amazon blamed the security breach on consumers reusing the same passwords on multiple services. Once hackers cracked the password for one of those services, they had access to all the others as well.[80]

---

[74] A Greenberg, 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' (Wired, 21 July 2015) <www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> accessed 1 September 2015; S Checkoway and others, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' (Proceedings of USENIX Security 2011, August 2011); N Bilton, 'Disruptions: As New Targets for Hackers, Your Car and Your House' The New York Times (New York, 11 August 2013) <http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?_r=0> accessed 2 February 2017.

[75] Such as biometrics and sensory algorithms to verify the physiology of bodies in vehicle interiors. Such processes secure cyber-physical space, but also register user capabilities for cognitive capacities and control that yield data as insured risk and automate decisions. S M Taylor, and M De Leeuw. "Guidance systems: from autonomous directives to legal sensor-bilities." AI & Society (2020): 1-14

[76] A botnet can be defined as 'a collection of remotely controlled and compromised computers known as bots … that installs software (typically malicious) on the bots' computer and performs acts, nearly always criminal, using the innocent bot computer': A Maurushat, 'Zombie Botnets' (2010) 7 Scripted 2.

[77] S Soltan, P Mittal and H V Poor, 'BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid' (Proceedings of the 27th USENIX Security Symposium, 15–17 August 2018, Baltimore) 15.

[78] Ibid 16.

[79] K Lawrence, 'Should the Internet of Vibrating Things Be Worried?' (Readwrite, 13 October 2016) <http://readwrite.com/2016/10/13/should-the-internet-of-vibrating-things-be-worried-dl1/ > accessed 6 December 2016.

[80] N Vigdor, 'Somebody's Watching: Hackers Breach Ring Home Security Cameras', The New York Times (online, 15 December 2019) <https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html