OCSC
Oceania Cyber Security Centre

Strengthening Australia's Cyber Security Regulations and Incentives

September 2021

Introduction

The Oceania Cyber Security Centre (OCSC) was established in 2016 as a collaboration between eight Victorian Universities and the State Government of Victoria. The Centre's mission is to work with sovereign governments and deploy the Cybersecurity Capacity Maturity Model for Nations (CMM) in partnership with the University of Oxford for the purpose of identifying capacity-building initiatives which can improve a nation's cyber maturity and resilience. To date, the OCSC has successfully led eight CMM review missions with neighbouring nations and international partners in the Oceania region. The OCSC works with international partners such as the International Telecommunication Union (ITU), Asia Pacific Network Information Centre (APNIC), Asia-Pacific Telecommunity (APT), The World Bank and the Global Forum on Cyber Expertise (GFCE). OCSC works at the forefront of research to strengthen cybersecurity capacity and build contextualised resilience, exploring questions of what works, what does not work and why. OCSC's expertise across cybersecurity is all-encompassing, rich and diverse. It includes expertise on: policy and strategy; culture; education and training; law and regulation; governance and structure; and incident response and technical controls to protect information and intellectual property (IP).

Executive Summary

The Oceania Cyber Security Centre (OCSC) welcomes the opportunity to respond to the Australian Government's Call for Views on *Strengthening Australia's cyber security regulations and incentives* ('the Discussion Paper').

In this submission we propose that Australia's regulatory framework for cyber security and associated incentives are currently overly complex, sectoral, and generally not fit for purpose. Therefore, steps should be taken to remedy the current framework to ensure greater coherency. Reform should also be tailored towards providing a clear outline of cyber security best practices, resolving the current regulatory gaps, introduce measures of accountability, and finally, provide remedies. Overall, the workability of the current framework needs to be developed through repackaging, expansion in scope, and education.

Digital technologies are evolving at a pace which is placing the current regulatory framework under pressure. Not only is the technology becoming more advanced, but cyber criminals are also becoming more sophisticated in their targeting and intrusion activities, making the already complex nature of policy and regulatory response even more strained. Cyber criminals and their activities continue to target Australia's critical infrastructure and businesses at an increased rate, such increase is in many ways attributable to the current pandemic, as our dependence on digital technologies grows. Simply stated, as technology evolves, so must the regulatory framework.

The current regulatory framework for cyber security in Australia is a patchwork of legislation and regulations. Added to this dynamic are the governmental and non-governmental organisations which have created several initiatives and sector-based guidelines. The legislative framework governing cyber security not only includes the *Privacy Act 1988* (Cth) (*Privacy Act*), Australian Consumer Law (ACL) and the *Corporations Act 2001* (Cth) (CA), but also, the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), the *Telecommunications (Interception and Access Act) 1979* (Cth), the *Telecommunications Act 1997* (Cth), the *Crimes Act 1914* (Cth), and more recently, the *Privacy Amendment (Notifiable Data Breaches Act) 2017* (Cth) and the *Security and Critical Infrastructure Act 2018* (Cth) (SOCI Act). Each of these statutes have their own focus and whilst not all are relevant to the overall purpose of this submission, they all contribute to the cyber security framework of Australia. Notably, a number of these statutes have established or empowered relevant governmental bodies with oversight roles including but not limited to the Office of the Australian Information Commissioner (OAIC), Australian Competition and Consumer Commission (ACCC). Some of these statutes are currently undergoing significant review and reform, as such, it is important to factor the key discussion points that emerge in the coming months and avoid unnecessary overlap of regulation and its applicability.

In addition to the above, there are numerous examples of other corporate governance and industry-based regulations, the Australian Stock Exchange (ASX) for example, has implemented the *ASX Corporate Governance Principles and Recommendations,* which also creates obligations upon listed entities relating to the management of personal and sensitive data and responding to data breaches. Further, in September 2020, the Australian Cyber Security Centre (ACSC) published *IoT Code of Practice: Guidance for Manufacturers* along with the *Code of Practice: Securing Internet of Things for Consumers.* As such, there are already numerous guidelines and industry-based cyber security regulations that require some level of compliance. Despite the vast amount of regulation, there is limited accountability and costs of non-compliance and poor practice disproportionately impacts consumers who are unable to obtain compensation.

This submission makes the overarching argument that the way forward in strengthening Australia's cyber security framework should through the consolidation of the existing framework and development of current structures (provide clarity and reduce overlap requirements) and where necessary broaden the scope of legislation to address current gaps (reconsider the AU$3million threshold in the *Privacy Act* and provide an avenue for legal redress for consumers/individuals). Thus, the amendments moving forward should be targeted and specific, with the main objective to encourage, promote and improve the workability of the current framework.

It is therefore proposed that three steps should be considered. The first step should be to consolidate the current framework. Secondly, overlaps and gaps in the overall regulatory framework require identifying and redress. Thirdly, there needs to be increased accountability, through for example, potential and proportionate punitive actions and performance reporting.

In amending the current regulatory framework, it is vitally important that Australia remains aligned with international standards and agreements, and takes advantage of the opportunity presented, so that Australia can become a leading digital economy in the Asia-Pacific region, as envisioned within the Federal Budget 2021-22.

In our submission, OCSC will respond to each of the questions proposed in the Discussion Paper individually. Whilst several of our answers are more in-depth due to relevant and available evidence to support our position, OCSC notes that our overall submission outlines that additional regulation of the digital space would not result in more effective cyber security controls or prevention of cybercrime. Our position outlines that there exists currently effective regulation which can be adapted to be more targeted to intended audiences and/or simplified similar to what has occurred in other countries to increases awareness and compliance.

Several proposals outlined in the Discussion Paper have little basis either from a technology basis or from an application of regulation. OCSC has provided examples and comparisons of international regulation and included commentary as to their effectiveness and application as the basis for recommending an adapted policy approach rather than a new set of regulations.

Chapter 2: Why should government take action?

As noted in the Australian Government's *Digital Economy Strategy* (DES 2030) "the *Small Business Digital Taskforce Report 2018* showed many SMEs struggled to understand how digital technology could generate growth and productivity benefits for their business. SME engagement with digital products was low, with only half of businesses having a web presence, 40 per cent using cloud services, and very few citing cyber security as a priority."[1]

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

It is worthwhile to note that there are already several strategies and initiatives available to businesses that promote and assess cyber security best practices including the Australian Cyber Security Centre's (ACSC) 'Cyber Partnership for Small Businesses', the 'Cyber Security Business Connect and Protect Program', the 'IoT Code of Practice: Guidance for Manufacturers' and the 'Cyber Security Assessment Tool'. Importantly, such initiatives have been allocated budgets, and yet there is limited, accessible data relating to performance.

However, as observed in the Discussion Paper there are currently several factors that is preventing the adoption of cyber security best practices in Australia. There are also obvious asymmetries between providers of technological products and buyers/consumers,[2] such that the 'buyer' lacks a basic technical literacy surrounding security offerings. As noted in the 2020 ACSC *Cyber Security and Australian Small Businesses Results from the Australian Cyber Security Centre Small Business Survey* four key barriers were reported.

1. Not having dedicated staff with an IT security focus – Cyber security has to compete for time and other resources with multiple demands.
2. Planning and responding – Businesses need to better plan for and respond to cyber incidents.
3. Complexity and self-efficacy – Business owners fail to identify weaknesses in security practices and know they are struggling, but do not know where to begin.
4. Underestimate risk and consequences of a cyber incident – Businesses need to better understand the risk and impact of a cyber incident and to not underestimate their recovery period from a cyber incident.[3]

Furthermore, the current regulatory framework is sectoral and fragmented. Further, small and medium businesses in many situations have no obligation to comply, as there is minimal applicability of the regulatory framework.

The Small Business Digital Taskforce, in their report submitted to government in March 2018, highlighted that 'current ecosystem for providing small businesses with information and advice is disjointed and in need of repair'.[4] Further, stating that small business:

"…tend not to go to government for digital advice, and governments' efforts to engage small businesses online have been mixed; trust peak industry associations, but these bodies have not been able to provide best practice digital advice or effective digital awareness campaigns for their members; and trust their accountants' advice on digital issues, but the profession lacks a central, authoritative reference point to source this advice."[5]

The OCSC therefore recommends that such asymmetries should be addressed by governmental programs that emphasise awareness and education. Such recommendation is aligned with Australia's Cyber Security Strategy 2020 which highlighted the need for broad engagement and awareness directed towards the education industry.

Australia's approach to cyber security can be contrasted to the United Kingdom's (UK) approach. After conducting qualitative comparative research, it has become very evident that finding relevant resources to learn about cyber security best practices are referenced across several UK Government websites and departments. Whilst the ACSC's website *cyber.gov.au* is Australia's primary source of cyber security information, the OCSC proposes that a more streamlined approach should be considered, where all resources are consolidated and located in one dedicated website. OCSC contends that although the *cyber.gov.au* website is useful, its practical reach is limited by the number of other government websites providing similar information. OCSC further notes that the ACSC alert service frequently sends out delayed 'ACT QUICKLY/HIGH ALERT' messages, which are often sent more than a week after a critical vulnerability was identified and first published. It is therefore recommended that the workability of this website should be improved, and that the ACSC should further review its mechanisms to provide more responsive and timely alerts. Accordingly, Australia could look to the UK's National Cyber Security Centre (NCSC) approach. Improving the workability and streamlining online content, may improve the adoption and awareness of cyber security best practices.

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

Australia has a unique opportunity to address the negative externalities and information asymmetries relating to cyber security best practices. As already recommended above, such issues can be addressed through targeted education and awareness programs. It is also vitally important that all businesses are provided the opportunity to gain an understanding of cyber security best practices as we move towards becoming a digital economy as envisioned in the Federal Budget 2021-22 and the DES 2030.

Whilst it is acknowledged that the Discussion Paper was one of the first 'next steps' outlined in the DES 2030, the DES 2030 itself sets out a structured plan on how Government can improve cyber security and address some of the negative externalities with businesses, such as the 'Digital Readiness Assessment Tool', which operates as an educative tool, and the 'Small Business Digital Champions Project', designed to provide free sector-specific digital advisory services.[6] And, as stated in the DES 2030, many of the foundations are already in place to ensure that Australia is on the path to becoming a leading digital economy, with over 150 existing programs and policies designed to support opportunities for a digital future.[7] The key objectives of the DES 2030 are to facilitate and deliver the right foundations to grow our digital economy through; the provision of digital infrastructure; increasing cyber security, safety and trust; skills and inclusion; systems and regulation; and, trade and international engagement.[8] Therefore, it is recommended that further consideration of the DES 2030 should occur, to ensure alignment between goals, and regulatory frameworks.

Further, it has been argued that there is currently little incentive for manufacturers to produce secure products and there are "information asymmetries" between producers and consumers.[9] As will be recommended in Chapter 6 and 7 of this submission, it has been observed that one way to reduce these asymmetries and to enhance consumer trust is through the development of a labelling scheme and implementation of standards, that can inform consumers and retailers regarding the quality of security of a device.[10]

Chapter 3: The current regulatory framework

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

As discussed in the preceding sections, Australia's current regulatory framework is a patchwork combination of Commonwealth and state legislation, and governmental and industry-based guidelines. It has been observed that Australia's Cyber Security Strategy 2020 'brings together cyber security capabilities from across Australian Government'.[11] However, it has been argued that Australia does not have the same level of cyber security regulation as seen elsewhere around the world.[12] In fact, Australia's regulatory framework for cyber security has often been criticised as a 'piecemeal' and 'patchwork'.[13] This is due to the amount of legislation governing Australia's cyber security framework, which in many areas suffers from a lack in clarity and is limited in scope. In relation to privacy, and general concerns relating to the regulatory framework, the Australian Law Reform Commission (ALRC) stated:

> *"In the ALRC's view, the existing law is a patchwork, with some important pieces missing and inconsistencies between others."*[14]

Further, when discussing the legislative framework relating to surveillance devices, the ALRC argued:

> *"… there is significant inconsistency in the laws with respect to the types of devices regulated and with respect to the offences, defences and exceptions. This inconsistency results in uncertainty and complexity, reducing privacy protection for individuals and increasing the compliance burdens for organisations."*[15]

Another criticism of the current framework is that it mainly relates to large private enterprise, and government (public) organisations, and as pointed out in the Discussion Paper, this leaves several types of organisations and businesses outside the scope of current regulation. As of "30 June 2019, small businesses with a turnover of $3 million or less comprised 95.2% of the 2,375,753 businesses actively trading in the Australian economy".[16] As it stands, due to the restricted scope and limited avenues of accountability, the current regulatory framework exposes vulnerabilities and increases risk.

Despite these criticisms, there have been substantial reforms undertaken, which in many respects, are a positive step forward. The recent amendments to the SOCI Act, for example, have the main objective in expanding the number of industries falling within the scope of the legislation, and as such has a significant impact on those industry sectors which it could apply. The proposed amendments also include a positive security obligation, and mandates cyber incident reporting, the implementation of risk management programs, and enhanced cyber security obligations.

The *Protective Security Policy Framework* (PSPF), established pursuant to the PGPA Act, is another positive initiative that has clear scope, applicability, and reporting requirements. Under the PSPF, there are clearly articulated guidelines for Executives. Such style of approach should be considered moving forward.

Another recent amendment, the *Privacy Amendment (Notification of Data Breaches) Act 2017* (Cth), created the Mandatory Data Breach Notification requirements. Whilst this amendment can be observed as a positive step towards an improved regulatory framework,[17] it has been argued as an "internationally important, yet imperfect, contribution to data breach notification law".[18] It should be noted that such reform is welcomed, however, cyber security legislation is still in need of a more comprehensive update to address privacy and cyber security threats, which this amendment cannot achieve alone.[19] Beyond the legislative frameworks, Australia's approach to cyber security can be contrasted to the UK's approach.

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

It has been predicted that Australia's future will be immersed in a digital world, one that is characterised "by data-driven new business models, platforms, and e-commerce, enabled by global supply chains".[20] As such, Australia requires a robust framework that is equipped with the necessary safeguards, defences, and regulations to ensure businesses, individuals and critical infrastructure can operate online safely. Further, it has previously been recommended that Australia should learn from the legal and regulatory systems of other countries, such as the US, when reviewing the current regulatory framework.[21] The OCSC agrees that the current legislation and guidelines require further clarity regarding cyber security expectations and that coverage of the current regulatory framework should go further in protecting consumers, who, as stated, 'are likely to bear some of the costs of a cyber security incident'.

One of the main criticisms of the current regulatory framework, is that it lacks clarity.[22] To improve clarity, it is recommended that the current framework is simplified and consolidated, with understandable definitions and clearly outlined scope and applicability. Currently, there is considerable overlap between legislation and regulation, and limited consistency.

The current regulatory framework, as outlined above, has limited coverage. Currently, the main organisations falling within the scope of the regulatory framework are security and enforcement agencies, governmental and public organisations, and big business (for example, publicly listed companies and the financial sector). This limited coverage means that a very large percentage of Australian businesses and organisations are not obligated to adhere or adopt privacy protections and cyber security best practices. As such, it is recommended that the current regulatory framework extends beyond big business and the AU$3million threshold in the *Privacy Act* be revised.

Whilst it may be observed that removing the AU$3million threshold would increase the burden on small businesses in relation to regulatory compliance, there are benefits to the consumer if small businesses had obligations relating to privacy and reporting requirements. It has been argued by the OAIC "that the

small business exemption is no longer appropriate in light of the privacy risks posed by entities of all sizes and the regulatory uncertainty created by the application of the exemption."[23] Further, as pointed out by the OAIC:

> *"The small business exemption is also an anomaly amongst international privacy laws. No other comparable international jurisdiction exempts small businesses from the coverage of privacy legislation. The small business exemption has proved to be one of the major issues for Australia in seeking adequacy under the GDPR, due to the lack of privacy requirements in relation to a large section of the economy."*[24]

Compared to other jurisdictions, Australia lacks an enforcement mechanism and limited accountability where cyber security best practices are ignored, and where data breaches result in damage to businesses or individuals. Further, government initiatives after commencement, lack performance measures and performance measures. Therefore, it is recommended that Australia seek guidance from international standards such as the *General Data Protection Regulation* (GDPR) in relation to enforcement powers and penalties.

Australia's recent Mandatory Data Breach Notification scheme applies to entities that have an obligation under APP 11 of the *Privacy Act* to protect the personal information they hold.[25] Further, when an eligible data breach occurs, the Mandatory Data Breach Notification scheme states that an APP entity to which the *Privacy Act* applies should first "contain the breach where possible and take remedial action."[26] Further, "where serious harm cannot be mitigated through remedial it must notify individuals at risk of serious harm and provide a statement to the Commissioner as soon as practicable."[27] There are three notification options open to APP entities where a breach occurs: they can choose to notify all individuals; notify only those individuals at risk of serious harm; or publish a notification which is uploaded on their website and forwarded to the Commissioner. The GDPR, similarly to Australia contains provisions stating the data breach notification requirements. In comparison to Australia's approach however, the GDPR's data breach notification scheme applies to "the data processing activities of businesses, regardless of size, that are data processors or controllers with an establishment in the EU."[28] As such, the GDPR has broader application, greater recognition of individual rights and enforcement mechanisms.

As consumers are likely to bear some of the costs when a cyber security incident occurs, it is advised that personal and public enforcement mechanisms are adopted within the legislative framework beyond the Mandatory Data Breach Notification scheme. Such mechanism could consist of a dedicated compensation mechanism which falls within the scope of existing legislation, whether that be the *Privacy Act* or ACL. It is suggested that where personal information is misused, the *Privacy Act* would seem appropriate. However, for consumer products that fail to meet baseline security requirements and damage ensues, the ACL, and more specifically the ACCC would have greater authority.

Finally, this submission would argue that Australia should seek guidance from international standards to address the current concerns relating to clarity, coverage and enforcement.

Chapter 4: Governance standards for large businesses

As already mentioned in the preceding sections many large businesses already have extensive reporting requirements and corporate duties, and those falling within the scope of the SOCI Act are also subject to mandatory risk management plans, positive security obligations and mandatory notification scheme. Whilst these are positive developments, there is however, a need to review the framework closely to enhance workability. Consolidation of the current reporting requirements should be also considered.

In 2019, the NCSC launched an online tool called 'Exercise in a Box', which enables businesses to test how resilient they are to cyber-attacks. The toolkit in its current form offers a range of realistic scenarios businesses and organisations could potentially face, and it allows businesses to prepare themselves.[29] And, with a shift of employees working from home during the pandemic, a subsequent initiative 'Home and Remote Working'. This second online tool allowed staff members to become informed on how they can access networks, what services might be required to secure employee collaboration, and what processes are in place to manage a cyber incident whilst working remotely.[30] By the end of August 2020, 'Exercise in a Box' had more than 7,500 registered users around the world.[31] And, as of 2 May 2021 there were 10,000 users.[32]

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

There are already several programs underway in Australia with the main objective of strengthening corporate governance of cyber security. Such programs are primarily aimed at increasing the cyber resilience of companies whilst providing education and awareness of cyber best practices. As stated in the sections above, when looking at corporate governance and the current tools already available to businesses, initiatives include, but are not limited to the ACSC's 'Cyber Partnership for Small Businesses', the 'Cyber Security Business Connect and Protect Program', the 'IoT Code of Practice: Guidance for Manufacturers' and the 'Cyber Security Assessment Tool'.

One initiative worth mentioning, recently created by the UK was the launch of Financial Sector Cyber Collaboration Centre (FSCCC) in 2020, whilst this is sector-based and limited to the financial sector, the *"FSCCC is a partnership which identifies, investigates and coordinates the response to incidents that have potential consequences for the finance sector, by combining, analysing and distributing information from across the sector to produce timely outputs for the financial industry."*[33] It is one such initiative that can assist large businesses to adopt better cyber security practices without over-burdening directors and senior employees of large businesses.

However, it should be noted that Australia has a very robust regulatory framework for companies. Corporate governance in Australia is a combination of legislation and self-regulation. The *Corporations Act 2001* (Cth) (CA) contains extensive duties owed by directors and officers of a corporation, and the OCSC would propose that there is some level of implied cyber diligence within these duties. The duties of directors, imposes minimum corporate governance requirements and set out the consequences of a breach. Whilst they are often referred to 'directors' duties', ss 180 – 184 are imposed on both directors as well as other 'officers of a corporation'. The self-regulatory aspect of corporate governance refers to the *ASX Corporate Governance Principles and Recommendations.*

The OCSC is of the perspective that the fiduciary duty contained in s 181(1) which requires a director to act in good faith and in the best interests of the company and for a proper purpose, does in fact, imply a requirement to uphold cyber security best practices. A failure or inaction here would likely be found as contrary to this duty, and possibly result in harm being done to the company if a cyber security breach was to occur. Further, the *ASX Corporate Governance Principles and Recommendations* in recommendation 7.2 outline that an effective risk management includes a framework that "deals adequately with contemporary and emerging risks such as digital disruption, cyber-security, privacy and data breaches.[34] The Australian Securities and Investment Commission (ASIC) has also prescribed a number of good governance principles relating to cyber security, stating that board engagement towards cyber security lies at the heart of good governance.[35]

Comparatively, in the US it is already 'expected' that boards of directors take necessary steps to ensure cybersecurity.[36] In 2013, following a very substantial data breach of Target Corp., where personal information of more than 60 million customers was stolen, a US court found that the directors and officers had fallen short in their fiduciary duties by failing to maintain adequate safeguards to ensure the security of data and personal information.[37]

The OCSC recommends that cyber security within companies should be seen as more than just an IT issue, as navigating cyber risks relies on leadership commitment, risk management and good cyber security decision-making.[38] Further, it is recommended that cyber security expertise is incorporated within the board.[39] Such recommendations are aligned with World Economic Forum's *Principles for Board Governance of Cyber Risk.*

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

Continued cyber security support should be made available to small and medium-sized businesses, and not just their directors. Businesses should be able to access robust cyber security products and services. However, greater awareness is required to ensure such support mechanisms have a good level of uptake. Whilst some support is available for small and medium businesses, these initiatives are difficult to find if you are unsure where to look.

It is worthy to note that the ACSC recently launched their 'Cyber Partnership for Small Businesses' program, which has the main objective of promoting and supporting businesses to become cyber resilient and incorporate further cyber best practices. Whilst this program is recent, future performance reports and data should be made available to understand its efficacy and uptake.

Unfortunately, the ACSC Annual Review 2019-2020 does not present data as to the uptake of associated programs designed at strengthening cyber security best practices. Whilst it outlines the threats and prevalence of cybercrime, there is limited guidance and reasoning as to *why* cyber security should

be prioritised, and the benefits of adopting cyber security best practices. There are simply website links to reporting sites where a cybercrime has occurred, and the current initiatives that small and medium businesses can utilise. This is a stark contrast to the NCSC *Annual Review 2020*, where the UK government has provided detailed analysis as to the performance of initiatives, what is being done in certain industries, whilst highlighting *why* adopting cyber security best practices is beneficial.

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

Whilst it is clearly advantageous to provide education opportunities and promote awareness for senior business leaders, there are already several documents and guidelines that assist in this area. And, as stated in our submission responding to *Australia's 2020 Cyber Security Strategy – A call for views*, further awareness and education needs to occur beyond current offerings, and such initiatives should not just be limited to senior business leaders.[40] Therefore, cyber security education initiatives should be delivered specifically across sectors such as, agriculture, health, mining, transport, critical infrastructures, communication, architecture, retail, and hospitality as examples of industry verticles where education could have significant impact.[41] Further, *cyber security literacy* should become a core competency for all sectors and for all positions, rather than a specialised topic.[42] This would also empower all individuals, businesses, and their senior leaders, and reduce the information asymmetries and potential fallout of negative externalities as discussed in Chapter 2.

Chapter 5: Minimum standards for personal information

One recommendation that we would put forward for greater discussion and consideration is that there is a need for greater coordination between the *Privacy Act* and Australia's Cyber Security Strategy 2020. Further, there is a need to provide greater consultation with business to help develop and create awareness surrounding a Code of Practice.

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?
9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?
10. What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

OCSC submits that a proposed Code of Practice is not a necessary method to promote the uptake of cyber security standards and best practices in Australia. The main rationale behind this view, is that the current regulatory framework, upon improvement and refinement, already accomplishes what a Code of Practice would ideally seek to achieve.

It is put forward here that the current Australian Privacy Principles (APPs) are relatively effective. The OCSC therefore questions whether a Code of Practice is necessary, and what benefit it may have, and what would it add to the current framework, that the APPs do not already achieve? The Discussion Paper outlined that one of the benefits of a Code of Practice, "would provide a strong incentive to improve security across the digital economy by entities covered under the Privacy Act". The OCSC would propose that there are already incentives for businesses to improve security measures contained within the regulatory framework. Further, a Code of Practice created to "harmonise international standards and offer opportunities to Australian businesses to market their security credentials internationally", is also achieved by the current legislative requirements, and would also be accommodated under a well devised cyber security standards regime in relation to smart devices. Further, the CA and ACL also prescribe certain obligations and minimum requirements on directors of companies, and in the provision of goods and services. Additionally, it is already established that certain GDPR requirements extend to Australian businesses where operations occur in the EU. Finally, as stated in the Discussion Paper, the limitation of a Code of Practice would be on 'personal information' and *Privacy Act* entities, again, the current APPs already cover this.

Perhaps the more suitable solution is to consider redrafting the current APPs to ensure clarity and applicability to small and medium businesses. Ideally, the APPs should be made easier to be interpreted and applied.

OCSC further submits that any mandated or voluntary technical controls which may be included in a code would simply result in additional costs to consumers. Business would have little option but to pass on the cost of such controls which render any suggestion of cost-effectiveness moot. It could be argued that some consumers will pay a premium for a most-secure device or software however it is not the role of the OCSC to provide businesses with any marketing or other advice in this regard. Other industries where increased regulation has impacted upon product development, such as food labelling, has seen such costs embedded into the product's development, resulting in higher prices. A cost-benefit analysis in this regard is a separate piece of research.

Chapter 6: Standards for smart devices

It was noted in 2018 by Telstra, that connected devices and smart consumer products are being installed across society and in consumer homes with many of these devices featuring inadequate security measures. It has been observed that these devices often include unsecured factory default settings and passwords, which can leave consumers vulnerable to attack.[43]

11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why? Mandatory Standards (Option 2)

It was pointed out in the Discussion Paper that voluntary, principle-based guidance had a limited impact on business decision-making. As such it is recommended that Australia follow other jurisdictions such as the UK, and Singapore, and introduce legislation that makes it mandatory for manufacturers of smart devices to ensure that their smart devices contain a baseline of cyber security features. Further, implementing mandatory standards which are consistent with the international standards will also be an incentive for manufacturers to operate in Australia.

The OCSC would like to reaffirm the opportunity that Australia has before itself in being one of the leaders on a global scale when it comes to the development of a digital economy. Therefore, Australia's approach should build on, and align with international standards.

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

The European Union (EU) has been a driving force across the cyber industry where privacy and data regulation is concerned. And, the EU has remained at the forefront for legal reform in recent years. The European Standard EN 303 645 'Cyber Security for Consumer Internet of Things' (ESTI EN 303 645), one of their recent reforms, makes a valuable contribution to the regulation, and promotion of a safer digital future. Pleasingly, there has already been some uptake of the ESTI EN 303 645. As observed by Juhani Eronen, chief specialist at Traficom:

> *"To date we have awarded the labels to several products including fitness watches, home automation devices and smart hubs. Being involved in the development of the ETSI standard from the start helped us a lot in building up our certification scheme. Feedback from companies and hackers has been very positive so far."*[44]

As already stated in previous sections, CSIRO has stated that Australia's future will be immersed in a digital world, one that is characterised "by data-driven new business models, platforms, and e-commerce, enabled by global supply chains".[45] Therefore, it is critical that Australia remains at the forefront of emerging regulatory trends. Whilst the UK approach is commendable, it would be prudent for Australia to lead the way in the Asia-Pacific region and consider adopting the whole of the ESTI EN 303 645. This would, as outlined in the Discussion Paper, ensure consistency with international standards.

It is further recommended that mobile phones are also included within this standard for smart devices. The UK has decided to include smartphones in the scope of their new reforms. As mobile phones are now entrenched within everyday lives and include applications which allow consumers to pay for items, conduct online banking and participate in online trading, it is crucial that these smart devices also contained embedded security features.

However, the OCSC would question the practicality of implementing such standards. Whilst the benefits of aligning Australia's standards with those currently adopted internationally are very clear. The OCSC would recommend that attention would also need to be given to education for consumers, especially in relation to update firmware and software to ensure continued security.

13. [For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

Removing smart products that do not comply with a baseline security standard from online marketplaces would ultimately benefit the consumer. It would ensure the consumer is able to purchase smart devices that have a minimum baseline security protection. Online marketplaces adopting such voluntary approach would also have the potential to in-still greater consumer trust. It would also incentivise manufacturers to adhere to baseline security requirements to ensure competitiveness and maintain market-share.

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

It has been observed in the UK that there is a willingness to pay more for certain classes of devices such as those which are linked to physical security and online security measures to protect their home computers.[46]

15. Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

OCSC is not able to provide any further response to this question beyond our answers above.

Chapter 7: Labelling for smart devices

Finland in November 2019 become the first European state to commence certifying safe smart devices. Their cyber security label has assisted consumers in buying safer products. The label created by the Finnish Transport and Communications Agency, Traficom guarantees to consumers that the labelled device has basic information security features and is based on the ESTI EN 303 645.[47]

A consumer survey commissioned by Traficom in early 2021, indicated that almost 80% of Finns are aware of the risks related to smart devices, which is a steady increased since 2019, when awareness was below 70%. Further, almost 45% of the consumer surveyed indicated that an information security label on smart devices would play a part in their purchase decisions.[48]

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

The UK National Cyber Security Centre has adopted an educative focus in their approach when conveying advice to consumers and businesses. Pleasingly, they currently offer a great deal of information which is audience specific, to assist all sorts of organisations and individuals when securing devices and selecting such devices.[49]

Therefore, it is recommended that greater public awareness initiatives are required to guide consumers and empower them to make informed decisions. Greater public awareness is also likely to create market demand for more secure devices.

Furthermore, in addition to being educated and aware, consumers would need the ability to distinguish secure smart devices from less secure options. Thus, regulated mandatory information on security, such as provided by labels based on ESTI EN 303 645 is an essential prerequisite.

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

There are already several jurisdictions implementing labelling and standards for smart devices. Currently, labelling schemes for smart devices are already being implemented in the EU, the UK and Singapore. Further, it has been argued that labelling schemes are a positive way that allow consumers to make an informed decision.[50] The OCSC agrees that a combination of labelling and standards for smart devices would be practical and effective, as it would assist in reducing the "information asymmetries" and promote trust between the manufacturer and consumer. Importantly, it should be noted than an effective label will be one where consumers are able to distinguish between a secure and less secure product, and where consumers from various demographics will find it easy to understand.[51] However, it is worthy to mention that labels are arguably only effective where the consumer are educated.

With the vast increase of smart devices available to consumers, Singapore observed, that devices were being sold with poor cyber security safeguards, and there was little, if any, security features built in.[52] Singapore's 'Cybersecurity Labelling Scheme' (CLS) was originally introduced for home routers and smart home hubs in October 2020, but has recently been extended to include all consumer smart devices such as smart lights and smart printers.[53] It has since been extended to include all categories of consumer IoT devices, such as IP cameras, smart door locks, smart lights, and smart printers. Such reforms were "aimed to motivate manufacturers to develop more secure products, moving beyond designing such devices to optimise functionality and cost".[54] It is also notable, that this scheme is the first of its kind in the Asia-Pacific region. Whilst Singapore's CLS is aligned with the international standard ETSI EN 303 645, uptake remains voluntary. Such approach can be contrasted to the UK, where legislative reform has recently mandated three security requirements for consumer smart devices.

It is therefore recommended that Australia adopts Option 2 as outlined in the Discussion Paper, which would be similar to the approach taken by the EU and the UK. If Australia were to implement a labelling scheme that is aligned with the international standards, it may reduce burden on manufacturers operating in differing jurisdictions.

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

A label for smart devices is one method to increase consumer trust in smart devices and provides the opportunity for consumers to make a more informed decision when making a purchase. The OCSC agrees that a label for smart devices is a productive reform, however, would recommend that a similar approach to that of Finland, Singapore, the US, and the UK be adopted. Notably the UK and US have moved towards a mandatory scheme in recent months.

a) If so, which existing labelling scheme should Australia seek to follow?

There have been a few recent studies discussing the type of labelling for IoT and smart devices. One study published by University College London assessed types and designs of labels for smart devices. Their study looked that 'graded labels', which would operate similarly to energy ratings, 'seal of approval labels' and 'informational labels' which have icons which represent the type of security provisions and privacy guarantees included within the specific device. Overall, the participating consumers in this study preferred the informational label with 46.5% preferring this type of label and 40.8% preferred the graded label. Another study conducted by Carnegie Mellon University highlighted that privacy and security labels could increase accountability and transparency. Their study assessed the 'star rating system' and 'multiple certification level' label system which adopt a gold, silver and bronze approach. Overall, it did not appear that a 'star rating system' was an effective labelling style. It was also recommended that where labels only provide a small amount of information and consumer wish to have a better understanding of the security features of that device, a QR code could be included on the label to assist the consumer in making a more informed decision. The researchers from Carnegie Mellon University are now in the process of designing usable privacy and security labels for consumer devices. Their label design (Figure 1) has two layers, which include *"includes a simple, understandable primary layer for consumers and a more detailed secondary layer that includes information important to experts. The primary layer is designed to be affixed to device packaging or shown on an online shopping website, while the secondary layer can be accessed online via a URL or QR code."* This label design has already been featured on a number of reports and publications.

Overall, it is recommended that consideration is given to the 'informational labels' and 'multiple certification level' label system, instead of an expiry date label or a star system alternative.

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

It has been noted that currently, there is no other country in the world which has mandated this type of label. Whilst there is a clear benefit of not requiring an independent provider to undergo security testing, which would lead to lower compliance costs for manufacturers than the start-rating label, a security expiry date label may carry unintended consequences. Consumers may see the label and assume that the technology or smart device will be inferior upon that expiry date. Therefore, such style of label may create a misunderstanding as to what the 'expiry' means.

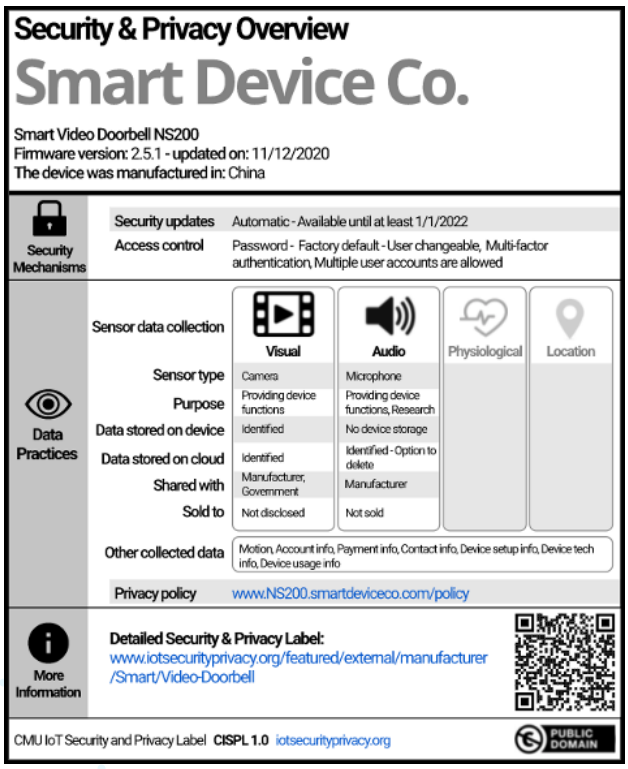

Figure 1: Carnegie Mellon University *IoT Security and Privacy Label* <https://iotsecurityprivacy.org/>.

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

Smart devices including mobile phones and tablets should also be included in any mandatory scheme that is adopted within Australia. As mentioned in the preceding sections, the UK has also included smartphone in the scope of recent reforms. As such, Australia should adopt a similar approach. Due to the interconnectivity of smart devices contained within the home, with many such devices linking to smart phones and tablets through relevant applications, it is crucial that these smart devices also fall within a labelling scheme which outlines the embedded security features.

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

The display of the security rating for each product should not only be displayed on the front of packaging, but also on the retailers' and/or manufacturers' website.[55] This would assist in reducing the "information asymmetries" between manufacturers and consumers. However, digital labels should be implemented with sufficient security to provide authenticity and non-repudiation for the claims.

Chapter 8: Responsible disclosure policies

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

Similar to the response in Chapter 5, the OCSC questions what additional advantage 'voluntary guidance' would achieve beyond what is already prescribed across the regulatory framework. Whilst the OCSC acknowledges the position and commentary contained in the Discussion Paper, the implementation of a standard for smart devices, labelling of smart devices, and the potential expansion of the *Privacy Act's* scope to include small and medium businesses, would eliminate the requirement for 'voluntary guidance'. Further, the *ASX Corporate Governance Principles and Recommendations*, and CA already require disclosure and reporting. If it is proposed that the regulatory framework just mentioned fails to achieve 'responsible disclosure', it recommended that further discussion occurs as to how the existing framework can more readily incorporate such practices/requirements.

Chapter 9: Health checks for small businesses

23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

25. If there anything else we should consider in the design of a health check program?

In the 2016 Cyber Security Strategy, AU$136 million was set aside by the Federal Government for numerous activities, including a Small Business Health Check. It was forecasted that 5,400 small businesses would undertake the health checks, however after three years as reported in Australia's technology media, it appears that the amount of health checks undertaken on small businesses was significantly below the forecast. Overall, only 35 health checks were reported as being conducted.[56]

Health checks for businesses are undeniably beneficial, and Option 1 would mean that businesses can improve their cyber security. However, as noted above in previous years there has been poor uptake of such initiatives. As discussed in Question 1, the reason behind poor uptake, is because many small and medium businesses dealing with personal information may lack the technical literacy required to understand cyber security, purely due to the fact it is not their direct business focus.

Again, the OCSC would like to draw comparison to the Exercise in a Box initiative rolled out by the NCSC in the UK. Exercise in a Box has clearly had a very good uptake, domestically and internationally with over 10,000 users.[57] One of the main benefits of this initiative are the different tailored simulations that can be conducted by each user. These scenarios are also, explained clearly and in plain English. Such initiative may be a productive alternative to health checks.

The OCSC would further recommend that role of the Joint Cyber Security Centres should reassess their adaptability of their outreach programs to ensure that awareness programs are hitting their target.

Chapter 10: Clear legal remedies for consumers

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

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?

It has become evident that despite the current regulatory framework, legislation protecting consumer privacy and data security has struggled to remain up to date with the considerable transformations occurring across the online domain.[58] As such there is a unique opportunity at present to make a substantial and meaningful change in Australia's attitude towards privacy protection and legal remedies available to those who have suffered material or non-material loss resulting from a data breach or breach in privacy. The Review of the *Privacy Act* already underway is considering the matter relating to the implementation of a statutory tort for serious invasions of privacy and whether individuals should have direct rights of action to enforce privacy obligations. It is recommended that any implementation of such rights and potential causes of action should not be limited to the *Privacy Act,* but also be extended to consumers under the Australian Consumer Law.

In continuation to the discussion above, despite the *Privacy Act* setting out specific legal obligations for businesses with respect to data protection and privacy, there remains no private enforcement mechanism, a stark contrast to the ACL, which does permit public and private enforcement action. Although, there has yet to be a case where the ACL has been used as a mechanism of enforcement for a privacy or data breach. Comparatively, in the United States, a regulator empowered under the *Federal Trade Commission Act,*[59] has the ability to deal with the issue of consumer privacy and companies' data security. Such piece of legislation has been observed as parallel to our Australian Consumer Law, and as such, highlights how our existing domestic consumer regulation framework could be revised to provide consumer reparation where breaches of privacy and data security occur.[60]

Whilst a private enforcement mechanism, namely a statutory tort for serious invasion of privacy under the *Privacy Act* would be a positive step forward allowing individuals seek compensation or damages where a breach has occurred, there should also be consideration of a public enforcement mechanism, which would ultimately operate in the broader public interest. Such public enforcement mechanism could therefore be implemented within the ACL. This would also operate alongside the private enforcement actions contained within the ACL.

Beyond the *Privacy Act* and the Australian Consumer Law, it is also important to consider the role of the *Australian Securities and Investments Commission Act 2001* (Cth) (*ASIC Act)* as a useful instrument in the regulation and enforcement of online privacy and data security for the financial sector.[61]

Chapter 11: Other issues

28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

As outlined in our submission, the OCSC proposes that more effective analysis and application of the myriad of current cybersecurity-related regulations should be conducted as a first step, before proposing additional regulations.

An effective starting point for the Australian government would be to conduct a cyber security maturity review. The 5 dimensions of the cybersecurity maturity review provide an extensive analysis of a country's relative maturity and include examining a nation's: policy and strategy, culture and society, knowledge and capabilities, legal and regulatory frameworks and standards and technologies.

As this review has been deployed to over 85 nations globally, including the United Kingdom, Switzerland and Brazil in additional to many developing nations, a recipient nation can benchmark their cybersecurity maturity across the above 5 dimensions and against other nations.

This assessment assist nations document and benchmark their current cybersecurity capacity, to both identity gaps for consideration of investment and enable the measurement of the impact of any subsequent policy, regulatory or capacity building activities through a second assessment in the future. This can more effectively focus the nation's priorities and ensure that there is a cohesive, coordinate and systematic basis to cyber policy development.

In this regard, Australia would be well placed to conduct a review. Whilst this discussion paper proposes several potential regulatory reforms, it does not provide the basis, or a starting point as to why such reforms as necessary, or what their expected impact maybe.

A cyber maturity review would do exactly this and provide the Australian government with a thoroughly researched, referenced and comparative roadmap of policy and regulatory reform which would result in better policy outcomes. A limitation of Australia's current policy development process is the dis-jointed and often duplicated relationship between government departments which adds to the confusion of policy ownership.

OCSC stands ready to assist the Australian government in this regard and looks forward to conducting a cybersecurity maturity review of the country in 2022.

Endnotes

1 ***Digital Strategy 2030,* 57**; Small Business Digital Taskforce, Report to Government (March 2018) <https://www.industry.gov.au/data-and-publications/small-business-digital-taskforce-report-to-government>.

2 It is also important to note that the 'buyer' in this situation is not limited to the individual consumer, but also small and medium businesses.

3 **2020 ACSC *Cyber Security and Australian Small Businesses Results from the Australian Cyber Security Centre Small Business Survey* 6.**

4 Small Business Digital Taskforce, Report to Government (March 2018) <https://www.industry.gov.au/data-and-publications/small-business-digital-taskforce-report-to-government> 1.

5 Ibid.

6 ***Digital Economy Strategy 2030,* 59.**

7 Ibid 25.

8 Ibid 2.

9 Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T.W. Wong, 'The impact of IoT security labelling on consumer product choice and willingness to pay' (2020) (15)1 *PLOS ONE* <https://doi.org/10.1371/journal.pone.0227800> 2.

10 Ibid.

11 Karen Koegh, Chelsea Gordon and Paticia Marinovic, 'Global development in cyber security law: is Australia keeping pace?' (2018) 42 *LSJ* 82, 82.

12 Ibid.

13 Ibid; Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era,* Discussion Paper No 80 (2014) 37-50; Simon Bronitt and James Stellios, 'Telecommunications interception in Australia: Recent trends and regulatory prospects' (2005) 29 *Telecommunications Policy* 875, 876.

14 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era,* Discussion Paper No 80 (2014) 41.

15 Ibid 275.

16 Office of the Australian Information Commissioner, *Submission – Review of the Privacy Act 1988 issues paper* (December 2020) 60.

17 Manoun Alazab, Seung-Hun Hong and Jenny Ng, 'Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia' (2021) 116 *Future Generation Computer Systems* 22, 23.

18 Angela Daly, 'The introduction of data breach notification legislation in Australia: A comparative view' (2018) 34 *Computer Law & Security Review* 477,477.

19 Ibid 478.

20 Joshua P. Meltzer, 'Digital Australia: An economic and trade agenda' (Working Paper No 118, Global Economy and Development at Brookings, May 2018) iii.

21 Ibid iv.

22 Karen Koegh, Chelsea Gordon and Paticia Marinovic, 'Global development in cyber security law: is Australia keeping pace?' (2018) 42 *LSJ* 82, 82; Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era,* Discussion Paper No 80 (2014) 37-50; Simon Bronitt and James Stellios, 'Telecommunications interception in Australia: Recent trends and regulatory prospects' (2005) 29 *Telecommunications Policy* 875, 876.

23 Office of the Australian Information Commissioner, *Submission – Review of the Privacy Act 1988 issues paper* (December 2020) 59.

24 Ibid 60.

25 *Privacy Act 1988* (Cth) s 26WE(1)(a).

26 Office of the Australian Information Commissioner, *Australian Entities and the General Data Protection Regulation (GDPR)* (Web Page) < https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/#ftnref4>.

27 Ibid.

28 Ibid.

29 National Cyber Security Centre, *Annual Review 2020 – Making the UK the safest place to live and work online,* (Report, 2020) 57.

30 Ibid.

31 Ibid 58.

32 @NCSC (National Cyber Security Centre) (Twitter, 2 May 2021, 8:13PM AEST) <https://twitter.com/ncsc/status/1388798675112038402?lang=en>.

33 National Cyber Security Centre, *Annual Review 2020 – Making the UK the safest place to live and work online,* (Report, 2020) 55.

34 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations* (4th ed, 2019) 27.

35 Australian Securities and Investments Commission, *Cyber resilience good practices* (Web Page) <https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/>.

36 Ray A. Rothrock, James Kaplan and Friso van der Oord, 'The Board's Role in Managing Cybersecurity Risks' (2018) *MIT Sloan Management Review* 12, 12.

37 Ibid.

38 World Economic Forum, *Principles for Board Governance of Cyber Risk* (Report, 2021) 7.

39 Ibid 11.

40 Oceania Cyber Security Centre, Submission No 176 to Department of Home Affairs, *Discussion paper – 2020 Cyber Security Strategy* (November 2019) 3.

41 Ibid.

42 Ibid 4.

43 Telstra Corporation Limited, 'Telstra Security Report 2018' (Media Release, April 2018) 45; Thanaphol Pattanasri, 'Mandatory data breach notification and hacking the smart home: A legal response to cybersecurity?' (2019) 18(2) *QUT Law Review* 268, 268-9.

44 James Coker, 'New Cybersecurity Standard for IoT Devices Established By ETSI' *Infosecurity Magazine* (Web Page) <https://www.infosecurity-magazine.com/news/cybersecurity-standard-iot-etsi/>.

45 Joshua P. Meltzer, 'Digital Australia: An economic and trade agenda' (Working Paper No 118, Global Economy and Development at Brookings, May 2018) iii.

46 Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T.W. Wong, 'The impact of IoT security labelling on consumer product choice and willingness to pay' (2020) (15)1 *PLOS ONE* <https://doi.org/10.1371/journal.pone.0227800> 3.

47 Traficom, 'Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products', *Finnish Transport and Communications Agency* (Blog Post) <https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label>.

48 Traficom, 'The National Cyber Security Centre Finland under Traficom opens their Cybersecurity Label certification process to commercial operators', *Finnish Transport and Communications Agency* (Press Release) <https://www.traficom.fi/en/news/national-cyber-security-centre-finland-under-traficom-opens-their-cybersecurity-label>.

49 <https://www.ncsc.gov.uk/collection/device-security-guidance>; <https://www.ncsc.gov.uk/cyberaware/home>; <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>.

50 Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T.W. Wong, 'The impact of IoT security labelling on consumer product choice and willingness to pay' (2020) (15)1 *PLOS ONE* <https://doi.org/10.1371/journal.pone.0227800> 3.

51 Ibid.

52 Cyber Security Agency of Singapore, *Cybersecurity Labelling Scheme (CLS)* (Web Page) <https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls>

53 Ibid.

54 Ibid.

55 Shane D. Johnson, John M. Blythe, Matthew Manning and Gabriel T.W. Wong, 'The impact of IoT security labelling on consumer product choice and willingness to pay' (2020) (15)1 *PLOS ONE* <https://doi.org/10.1371/journal.pone.0227800> 2.

56 Chris Duckett, 'Canberra forecast 5,400 small business cyber health checks, but only 35 happened' *ZDNet* (Blog Post) <https://www.zdnet.com/article/canberra-forecast-5400-small-business-cyber-health-checks-but-only-35-happened/>

57 @NCSC (National Cyber Security Centre) (Twitter, 2 May 2021, 8:13PM AEST) <https://twitter.com/ncsc/status/1388798675112038402?lang=en>.

58 Rachel Falk, 'The case for a new tort of cyber harm' (2020) 71 *LSJ* 70, 71; Stephen Corones and Juliet Davis, 'Protecting consumer privacy and data security: Regulatory challenges and potential future directions' (2017) 45 *Federal Law Review* 65, 66.

59 15 USC §§ 41-58.

60 Stephen Corones and Juliet Davis, 'Protecting consumer privacy and data security: Regulatory challenges and potential future directions' (2017) 45 *Federal Law Review* 65, 67.

61 Ibid, 69.

OCSC
Oceania Cyber Security Centre

Door 34, Goods Shed,
Village Street, Docklands
Victoria, Australia 3008

Email: info@ocsc.com.au

ocsc.com.au