THE UNIVERSITY OF MELBOURNE

27 August 2021

Strengthening Australia's cybersecurity regulations and incentives

Response to the Department of Home Affairs Discussion Paper

The University of Melbourne welcomes the opportunity to provide views in response to the Discussion Paper on Australian Government incentives and regulation of cybersecurity, as part of *Australia's Cybersecurity Strategy 2020* (the *Cybersecurity Strategy*).

The development of the regulatory and incentives framework is a key opportunity to align Australian enterprises' cybersecurity practice with latest research, particularly on consumer protections, and emerging cyber threats and security challenges. The Australian Government has an essential role in establishing incentives to encourage best practice and consequences to combat poor practice. It will be increasingly important for government at all levels to act as a role model, by following best practice in the conduct of its public business.

Summary Recommendations

We emphasise that cybersecurity standards/regulations will often be an effective and appropriate model, provided they are co-designed with relevant industries and respect the diverse regulatory environments in different sectors. Codes of Conduct provide another level of governance by clarifying expectation standards. Importantly, it will also be important to encourage a dynamic, proactive, and expert cybersecurity capability within organisations.

In respect to smart devices, along with adopting a mandatory Internet of Things (IoT) Code of Practice and a labelling system to inform consumer choice, the Australian Government should equip regulators, such as the ACCC, with powers to investigate and remedy non-compliance. To be effective, labelling must be employed judiciously and convey specific, concrete, and actionable information. Labelling should be mandatory for devices that deal with biometric and personal data.

We are also supportive of the proposals for strengthened data protections for consumers and enforcement powers for regulators made by the ACCC in the Digital Platforms Report (2019)[1] and under consideration in the current review of the *Privacy Act 1988*[2]. Consumers should be given greater control over their data, including to review, correct and withdraw data (as under the GDPR[3] and envisaged under the Consumer Data Right[4]) — giving consumers a self-help response to firms that fail to properly engage with cyber protections. Additionally, the

[1] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
[2] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988
[3] https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/
[4] https://www.cdr.gov.au/

Australian Government should legislate a *right to repair* and we refer to the inquiry currently being conducted by the Productivity Commission on this issue.

The University of Melbourne is committed to working with government to help identify future cyber threats and associated legal and regulatory frontiers; share expert research and analysis of global approaches; and to educate cyber-trained professionals with much-needed skills in Australia's cyber industries and business sector more broadly. The University endorses this consultation as a positive move towards increasing the regulatory requirements around responsible disclosure of vulnerabilities (for both government agencies and businesses) and setting a shift in focus from cyber awareness to cyber behaviour, both of which were recommended in our submission to the *Cybersecurity Strategy* development in 2019.

For more information, please contact Professor Liz Sonenberg, Pro Vice-Chancellor (Research Infrastructure & Systems) on l.sonenberg@unimelb.edu.au.

Chapter 2: Why should government act?

Question 1: What are the factors preventing the adoption of cybersecurity best practice in Australia?

Cross-disciplinary education and training to overcome adoption barriers

Ensuring Australia's digital economy is more resilient to cybersecurity threats requires stakeholder investment along with coordinated policy design, incentives, and regulation across areas such as data protection, privacy, artificial intelligence and digital technologies and cybersecurity. As part of building cybersecurity best practice, education and training programs will be important. These should not be siloed in one discipline or sub-discipline, and should highlight and convey connections between elements of cybersecurity grounded in the social sciences and those grounded in technology. The Australian Government and regulatory bodies should actively seek out and promote training programs that meet a high standard of interconnectedness and cross-disciplinary strength.[5]

With regards to factors preventing adoption, the Discussion Paper covers salient points, such as negative externalities, information asymmetries and difficulties in building a skilled workforce. In addition, University of Melbourne researchers have identified organisational factors that prevent the adoption of cybersecurity best practice in Australia.

Systemic business-IT disconnect among organisational leadership

Our research has identified deep-rooted misperceptions in many Australian organisations about the nature of the cybersecurity challenge. Cybersecurity is widely seen not as a business problem, but as a technology problem that is best delegated to the IT operations division. This misperception manifests in several ways: in how Australian organisations structure their cybersecurity function; in the way roles and responsibilities are created to manage cybersecurity; and in the methods for measuring cybersecurity 'performance'.

In many organisations, the IT operations division is a cost-centre, rather than a revenue-generator, the mandate, resources, and political authority available to IT operations to

[5] By way of example, we note training and education programs in cybersecurity, AI ethics, and regulation of emerging technologies being developed at the University of Melbourne under the Ninian Stephen Law Program as an initiative of the Faculties of Law and Engineering and Information Systems.

manage cybersecurity are often limited. For example, cybersecurity activity typically occurs at the operational level rather than at the strategic level of the organisation. This activity typically addresses a narrow section of the total attack surface (i.e. availability of digital platforms). IT operations are typically under-resourced, meaning IT teams do not have the time, capability, and tools to conduct root cause investigations and develop sufficient organisational learning to adapt organisational defences to the evolving threat landscape.[6]

Lack of connection between compliance and cybersecurity threat drivers

An underlying compliance culture leads many organisational leaders to believe that compliance with regulation and industry standards is sufficient protection against cyber-attacks. As a result, many organisations are oblivious to the highly dynamic external cyber-threat landscape, and do not actively consider which threat actors might be interested in targeting them, and whether they have the means and motivation to successfully penetrate the firm. Cybersecurity investments are made using the same logic. Therefore, some organisations tend to purchase IT security infrastructure (firewalls, intrusion detection systems, anti-virus software) and implement generic management practices (policy, risk management, training) in order to satisfy generic 'best practice' controls. Much less investment goes towards critical customisation and adaptation of cybersecurity to the firm's threat profile (e.g. threat intelligence and management capability, and incident response capability).

Lack of focus on protecting sensitive information and intellectual property

Related to the above points is the lack of protection afforded to intellectual property and sensitive information. There is a typical misconception that 'cybersecurity' and 'information security' are one and the same. As a result, we have observed that even 'best practice' cyber teams tend to focus on the availability of digital platforms and neglect the business' information confidentiality problem, as it requires an understanding of the business practice which is deemed outside of their capability, mandate, and expertise.

In summary, the University recommends that adoption of cybersecurity best practice would be enhanced through promoting:

- greater understanding amongst Australian organisational leaders that cybersecurity protection is a core business priority;
- greater understanding of, and response to, the specific threat environment facing an Australian organisation; and
- greater emphasis on, and broadened protections for, business intelligence and protection of digital platforms.

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

Yes, negative externalities, information asymmetries and other factors create a need for regulatory intervention. The concrete risk of security exposure from any individual product to an individual entity is small, but across a large suite of products and a broad swathe of the

[6] For a case study on how one of Australia's leading cybersecurity teams identifies opportunities and deficiencies relevant to operating conditions, see Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M., & Baskerville, R.L., (2021). *How can Organisations Develop Situation Awareness for Incident Response? A Case Study of Management Practice.* Computers & Security. Vol 101. (pp. 1-15).

community, the costs are measured in the many billions. This is a collective action problem well beyond the capacity of consumers and many organisations.

Choosing a secure product is a challenge with significant externalities and information asymmetries for consumers, SMEs, and large enterprises. Small businesses and consumers lack the relevant expertise to evaluate the security of the products and services they purchase and use. Even for an expert evaluator, products often lack sufficient documentation and evidence trails to be confident in product security.

For large institutions, the problem is no less severe, despite their greater ability to engage in consultations and negotiation to gain insights into the products they use. Even research conducted by experts in the field, such as studies completed by the University of Melbourne and partners into the security and privacy of educational technologies adopted during the pandemic, required months and significant expertise to produce clear and evidenced insights.[7]

Chapter 3: The current regulatory framework

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

We recognise, as discussed below, that some mandatory requirements for companies to protect individual consumers' interests and information are necessary as a legal bulwark defending the most vulnerable/least powerful party in the transaction. However, we suggest that imposing a mandatory regime of general cyber security governance and standards across industries would impose significant costs. Mandatory regimes risk losing nuance as between industries and specialised regulation. Regulatory regimes must therefore be carefully tailored to retain flexibility and minimize the extent to which firms treat security as 'just another' compliance exercise.

Mandatory cybersecurity governance and standards carry with them a significant risk of becoming a 'tick-the-box' compliance-focused activity that may not necessarily improve an organisation's cyber resilience. A mandatory approach may result in boards and executives treating compliance with the prescribed standards as the 'maximum required' security posture; and consequently, minimising cybersecurity investment in other controls recommended by the organisation's cybersecurity teams who have greater insight into their individual threat environments.

Mandatory governance standards could result in the devaluation of the organisation's cybersecurity resilience as compliance becomes the only measure of good cybersecurity practice. In addition, as acknowledged in the Discussion Paper, mandatory governance standards carry with them a risk of operational overheads that would increase costs in the cybersecurity governance/compliance domain, but potentially reduce organisational investment in operational cybersecurity and proactive, dynamic cybersecurity controls.

Specific technical controls may become outdated quickly. Law and regulation move more slowly than technology in general, and cybersecurity is one of the fastest moving subsections

[7] See Cohney, S., Teixeira, R., Kohlbrenner, A., Narayanan, A., Kshirsagar, M., Shvartzshnaider, Y., & Sanfilippo, M. (2021). *Virtual Classrooms and Real Harms: Remote Learning at US Universities*. In Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021) (pp. 653-674).

of technology. Rigidly regulating for 'yesterday's problem' is a danger in itself. Trying to keep a standard up to date when it is mandatory therefore carries grave risk if there is non-compliance by boards. It is a suboptimal solution. Indeed, it may in effect push Australia backwards in terms of the currency of its cybersecurity posture. This reinforces the need for any regulation to be adaptive and flexible.

Voluntary and co-designed governance standards can be highly effective where concerns about consumer protection are less salient. In the context of the university sector, the discussions around the *Security Legislation Amendment (Critical Infrastructure) Bill 2020,* as well as the work of the University Foreign Interference Taskforce (UFIT) and the *Guidelines to Counter Foreign Interference in the Australian University Sector* (the UFIT Guidelines) are all steering universities towards enhanced cybersecurity reporting obligations. Enhanced incident reporting and these collaborative processes are assisting in improving the cybersecurity posture for most universities.

It is important to note that universities cannot adopt a one-size-fits-all approach, as every university has its own risk appetite, risk profile, operational requirements, and business requirements that need to be taken into consideration when formulating its cybersecurity strategy and posture. This diversity carries over into organisations across Australian sectors.

For example, the initial UFIT Guidelines, which covered cybersecurity, were co-designed by the sector alongside the Department of Education, Skills and Employment, the Australian Cybersecurity Centre (ACSC), Group of Eight universities, Universities Australia, and others through a collaborative process. Given the diversity of the sector and the progress made to date through the collaborative process of informing and benchmarking within the sector, voluntary and co-designed cybersecurity regulations should continue to be the path forward.

The University recommends that voluntary and co-designed cybersecurity standards/regulations are an effective and appropriate model, reflecting the diversity within sectors and the need to maintain a dynamic, proactive, and expert cybersecurity capability within organisations.

Chapter 4: Governance standards for large businesses

Question 5: What is the best approach to strengthening corporate governance of cybersecurity risk? Why?

Strengthening corporate governance to improve cybersecurity requires a fundamental transformation in the way cybersecurity is managed in Australian organisations. As discussed above, the business-IT disconnect and the delegation of responsibility to an under-resourced and narrowly scoped IT operations divisions is the root cause of many cybersecurity problems.

In terms of the best approach, the University suggests:

- Consideration of the responsibilities of company directors, listed companies and companies subject to licencing regimes should continue. Increasingly, corporate Australia and the regulatory bodies are recognising this imperative, which raises several complex legal questions (for instance, director's duties are arguably already present in some licencing regimes).

- The Australian Government should work actively with firms to develop models of cybersecurity governance, such as through the Australian Cyber Security Centre (ACSC). Where firms are at a high risk of cyber-attack, cybersecurity should move outside of IT operations to a dedicated fusion division combining professionals from IT security, human factors security and physical security that is adequately resourced and has the authority and mandate to protect the enterprise.
- The Australian Government should consider how to improve threat intelligence sharing with critical infrastructure operators and support services to assist with cyber-defence configurations and remediation post-attack (potentially also through the ACSC).

Question 6: What cybersecurity support, if any, should be provided to directors of small and medium companies?

Education, access to training, and sectoral models and guidance would assist directors of small and medium companies. As stated above at Question 1, cross-disciplinary education and training programs delivered by experts in the field should be prioritised as an implantation aspect of rolling-out a regulatory and incentives framework.

Various organisational factors explain why cybersecurity is poorly managed in companies. Although negative externalities play a significant role, the key cause lies in the perception and practice of business leaders. An informal review of information security curricula reveals, unsurprisingly, that most cybersecurity education and awareness is offered by technologists for technologists.

The educational and awareness raising initiatives raised in the response to Question 7 (senior business leaders) apply to directors of small and medium companies.

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

Australian business leaders need to be well versed in cyber-safe behaviours, because cyber-risk is increasingly moving out of the IT realm to become a core business risk. Providing organisational leaders with awareness and education that promotes better decision-making with regards to cyber activities for themselves and their teams will assist in improving the resiliency of the organisation via a top-down approach.

Promoting cyber resilience for the organisation via the universal language of risk awareness will benefit a better understanding of the cyber-risk landscape for executives. Ideally, cyber awareness should be tailored to different cohorts, such as developers, IT staff, non-IT staff, executives and so on, to increase engagement and provide a more contextualised view of cyber threats. However, this is a mature implementation goal, and it should be acknowledged that enabling this will take time and effort on behalf of organisations and government. As discussed above, voluntary guidelines should be used to encourage this approach to education.

Senior business leaders learn best when they leverage their own experiences and engage in problem-based learning, action-learning and reflective learning in a community of practice.

These educational formats are best delivered by experienced cybersecurity experts with sufficient business knowledge and experience that they can present cybersecurity using a business or management practice lens, rather than the traditional technology lens. There may also be a valuable cross-disciplinary lens, given lawyers, IT experts, and cyber professionals are all critical to organisational adoption of cyber safe behaviours. Given most executives are time-poor, we recommend this education and awareness-raising should take the form of short immersive programs on cyber leadership that utilize case-based learning approaches, workshops, and panel discussions with peers.

Chapter 5: Minimum standards for personal information

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

The response to Question 4 above about ensuring that compliance does not become a 'tick-the-box' exercise also applies for the privacy updates covered in Section 5. Given the rapidly changing cyber threat and risk environment, the University recommends principle-based regulation in addition to any necessary baseline requirements addressed herein.

Chapter 6: Standards for smart devices

Question 11: What is the best approach to strengthening the cybersecurity of smart devices in Australia? Why?

As recognised in the Discussion Paper, information asymmetries place consumers in a weak position to monitor the security of devices and even to adopt cybersecurity measures. This insight justifies placing significant primary responsibility for cybersecurity in smart devices on manufacturers and retailers. It is also prudent to ensure Australia' regulatory response is consistent and compatible with those adopted overseas. As such, the Government's adoption of a cybersecurity code for smart devices that is similar to the United Kingdom's *Code of Practice for Consumer IoT Security (2018)* will beneficially promote complementary compliance between domestic regimes.

However, stronger measures are also required. As recognised in other regimes, including in the United Kingdom,[8] there are good reasons for making the IoT Code of Practice mandatory. Only a mandatory code ensures a strong baseline level of protection for consumers. Additionally, only a mandatory code ensures that these baseline protections are available across all smart products and to all consumers, including those affected by security flaws in devices they did not themselves purchase.

To support this move, there should be a regulator responsible for compliance with the code, such as the ACCC. This regulator should be equipped with powers to investigate non-compliance and have a full suite of sanctions, redress, and remedies to deter non-compliance, including the power to seek injunctive relief and award civil pecuniary penalties. Consideration should also be given to a private right of action for individuals who suffer or

[8]https://www.gov.United Kingdom /government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation.

are likely to suffer loss or damage as a result of breaches of the standards or an overall expectation of reasonable cyber security in smart devices.

Question 12: Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices? a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? b. If not, what standard should be considered?

ESTI EN 303 645 would be an appropriate standard for smart devices and the 13 requirements listed in the standard broadly cover different security properties. However, while some requirements are straightforward to be applied and checked (e.g., 'no universal default passwords'), other requirements come with limited guidelines for application (e.g. 'validate input data'). Due to this, manufacturers face difficulties testing their products to meet requirements. Vague standards without clearly defined compliance criteria are less likely to effectively improve security.

We agree that having a minimum standard by mandating the top N requirements (e.g., N=3) would have a positive impact on raising the awareness of manufacturers and customers. These should be the minimum requirements for products to be sold and deployed in Australia.

Question 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?

Standards, and compliance with standards, provide a potentially useful protection for consumers and an incentive to industry to improve overall cyber security in smart devices. However, for the reasons we have already discussed, mandatory standards should not be wholly relied upon to improve or assure product security.

However, the government should not assume that products that adhere to a standard are, in fact, secure. While it is nonetheless useful to require or request adherence to effective standards (such as NIST's suite of IoT standards and SP 800-53), this alone should not set a safe harbor or otherwise supplant principle-based regulation premised on reasonableness or reasonable expectations as a baseline.

In some circumstances, security standards can counter-intuitively reduce product security.[9] This can occur:

- when the context in which the standard was written does not match the context in which a product is developed;
- When a standard contains technical flaws or outdated information;
- When a standard focuses on process to the exclusion of outcome, or on high-level details to the exclusion of technical controls
- When the drafters of a standard have incentives that conflict with the technical goals of the standard; or
- When a standard is not freely available, and thus may be foregone despite its usefulness or necessity.

[9] See discussion of NIST cryptography standards in Cohney, Shaanan Natanel. *Too Important to Leave to Chance: Pseudorandom Number Generator Standardization & Security*. Diss. University of Pennsylvania, 2019.

To the extent that mandatory standards for cyber security in IoT or smart consumer products are introduced, we suggest that clearly defined standards with precise methods to assess whether devices comply with those standards are most likely to be successful. Government should also ensure automated compliance testing is part of any mandated or voluntary standards. NIST's experiences and challenges with the Cryptographic Module Validation Program suggest that automated testing is necessary for standards to be effective.

Moreover, even if a mandatory standard is adopted, smart devices should be subject to an overriding general obligation — to have a reasonable level of cybersecurity — having regard to the nature of the product, the circumstances in which it is sold, and the reasonable expectations of consumers. This might for example be included as a unique, new consumer guarantee in the Australian Consumer Law and/or a general obligation.

Chapter 7: Labelling for smart devices

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

Encouraging consumers to purchase secure smart devices will require consumer education to understand how to assess, find and use cyber secure smart devices. Importantly, all products should come with a baseline expectation of reasonable cybersecurity (see response to question 17) with enforcement by regulators.

A labelling system, properly design, should make it easier for customers to choose products with strong cybersecurity standards, provided that the price is reasonable. A labelling system will also incentivise manufacturers to improve the security of their products, in order to compete with other vendors. As recognised in the Discussion Paper, the labelling/ratings approach had success in informing consumers and incentivising manufacturers to improve the quality of other products in Australia (e.g., nutritional information and energy, water, and fuel efficiency).

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

A hybrid approach of minimum required standards and a ratings system can benefit consumers while also not being so rigid as to hold back technology-based innovation. The following considerations are important to effectively protect consumers through this approach:

- Any labelling system must be accessible and simple for consumers to understand. A star-based system or a tiered system, as used in Singapore, is preferable to detailed disclosures. Information overload and other cognitive biases mean that consumers often do not read detailed disclosures or cannot make use of the information contained in such material.
- Required standards such the IoT Code support labelling as additional implementable protection, provided they are sufficiently broadly designed to have relevance across different kinds of project and to adapt to technological and social change.

- As discussed above in questions 11 and 15, there should also be a baseline standard of cybersecurity for all smart devices, backed by regulatory oversight and sanctions for non-compliance. Cyber breaches have consequences for people beyond those who have purchased the product, and those affected should not bear the burden of poor choices by the immediate purchaser of an insecure product. Moreover, it is important not to introduce a two-tier system whereby savvy, well-informed, and well-off consumers can buy secure products while others miss out. Consumers who cannot afford more expensive products should not be left with a greater risk of insecure products and subsequently, greater exposure to cyber or privacy breaches.

One requirement that would benefit consumers and their cybersecurity is to require that manufacturers do not use technical measures to restrict users from their devices themselves. This would allow consumers to replace existing software if a vendor refuses to provide security patches. Further manufactures should be obliged to release any repair manuals used for servicing devices. This issue is under consideration under the Productivity Commission's *Right to Repair inquiry*.[10]

Government has a role to play here in not only setting up and guiding this process, but also supporting smaller organisations who might not otherwise be able to pay for the added cost. It would be detrimental to society if only very large companies could comply, and this led to monopolies in the market.

Question 18: Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? If so, which existing labelling scheme should Australia seek to follow?

(i) Should labelling be mandatory

There will not likely be sufficient voluntary industry uptake. As such, there must be non-voluntary requirements, and these should clearly and adamantly defend consumer privacy rights as part of their security requirements.

IoT device manufacturers have not typically adopted cybersecurity nor privacy security to a sufficient degree. Sometimes this is because it adds expense and does this in a marketing quadrant the manufacturer does not think will enhance sales. In other cases, this is because the self-interest of the manufacturer supersedes consumer protection (e.g. baby monitors or talking/listening toys which transmitted voice conversations from children's bedrooms to company headquarters overseas; using those 'stolen' communications made the privacy of a home for other purposes, such as machine learning training).

This problem will become more exaggerated as devices are able to receive and transmit ever more personal data. This is particularly emerging as a problem for biometric data, such as heart rate, temperature, breathing, speaking, gait, and inferred state of mind from facial expression. This burgeoning industry has shown no evidence of moving towards voluntary labelling.

Given that consumers are often unaware this is happening, there is a clear role for government to step in. Breaches of privacy in this space are not only a human rights issue: they are a cybersecurity problem. This was illustrated in 2018, when a large-scale cyberattack

[10] https://www.pc.gov.au/inquiries/current/repair#report

on Sing Health occurred, which included the theft of personal particulars of more than one million patients, and the medications data of 160,000 patients. Australian Government policy should look beyond consumers' biometric data as more than a consumer privacy issue, to view it as a national security issue.

(ii) What labelling approach should be adopted

Singapore's labelling scheme, as noted in the Discussion Paper, would also be a good reference. However, the requirement to use third party independent laboratory testing services to get Tier 3 and Tier 4 labels might be problematic. It could be a barrier for SME manufacturers to enter the market and create an unfair competitive advantage for dominant players if the third-party testing services are too costly.

International exemplar: Singapore's labelling scheme

The Cyber Security Agency of Singapore introduced a voluntary labelling scheme for smart devices in October 2020. The scheme consists of four cyber security levels, with each indicating a higher level of security and/or additional security testing.[79]

Tier 1 and 2 require a manufacturer to undertake a self-assessment of their products and make a declaration of how the device conforms to the requirements. Manufacturers seeking to achieve Tier 3 or Tier 4 are required to undergo third party laboratory testing. The requirements of the scheme align with the international standard ETSI EN 303 645.

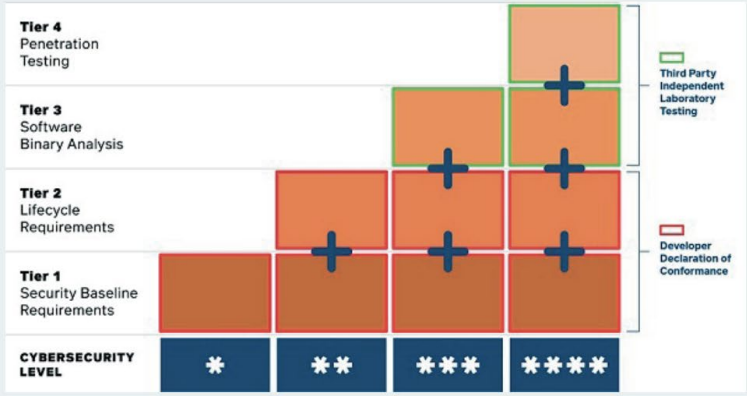

Figure 1. CSA Singapore 4 Level Cyber Security Labelling Scheme[80]

There following points are recommendations to address the above-mentioned problems in the current international standards (e.g. ESTI EN 303 645) and existing labelling schemes (e.g. the Singaporean scheme):

- A solution could be to develop a common (open source, or partially open source) tool set that can be used by both manufacturers and third-party testing services/authorities, so that manufacturers can do as much in-house testing as they can before sending the devices to third-party services for compliance testing. This would support more fair competition between manufacturers.

  Further to this, the Australian Government could initiate a funding program to support companies and research institutions to build a set of automated security testing techniques and tools for smart devices. The tools can be used by both manufacturers while developing their products and by authorities to decide the security labels/ratings. Researchers at Australian universities and government agencies (e.g. Data61, DST) have the expertise to work on building these techniques and tools.

Alternately automated testing could be provided as a government service through existing agencies such as DST.

- Having the same tool set, used by both manufacturers and authorities, would also help to control the correctness and consistency of the labels being attached to smart devices.
- Manufacturers should provide technical documents (including information to identify the debugging interface, the main input/output interfaces, and the memory layout but not including schematic of the circuit board) for the smart devices to be sold in Australia. Access to this information allows authorities to attach equipment and tools for independent security testing with little to no reverse-engineering effort.

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

It is appropriate to mandate a label that specifies *when security updates will no longer be provided*. An expiry date specifying the date beyond which a firm will not offer security updates would be a positive step forward. An analogy to other product expiry dates applies, given the risks to consumers of not patching software.

A security expiry date scoped too broadly would be inappropriate. There is no consensus (academic or industrial) as to what specific features represent a 'secure' product. This is partially because security is contextual and represents weighing the risks specific to that context against the protections present.

Failure to comply with any expiry date label may be misleading conduct under Australian consumer law. The University recommends consideration be given to establishing a penalty regime specifically attached to the labelling regime and the regime should specify that misleading consumers or fail to comply with stated expiry date labelling representations contravenes the regime. The penalty regime will make it more likely that manufacturers actively maintain the security of the device *until the expiry date*. Otherwise, there is a risk that such a labelling scheme could instil a false sense of security in the consumer/end user that their device is genuinely secure up to the expiry date.

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

The mandatory labelling scheme should cover mobile phones. As one of the most common smart devices used by consumers and a key source of significant security failures, it is crucial that a mandatory labelling scheme covers mobile phones. This is particularly so as work increasingly moves to remote arrangements and blurs the line between personal and professional technologies, meaning vulnerabilities in a personal phone quickly threaten Australian enterprises.

Phones sold in Australia must already meet minimum standards in other areas; it is reasonable to extend the minimum requirements to cover key elements of cybersecurity. Some phone providers are notorious for unnecessarily delaying updates and sunsetting updates within short timeframes. As consumers start to give increased attention to cybersecurity, it follows that increased transparency will be significantly beneficial to users of the most-used smart device, that is, mobile phones. We note our comments in the

introduction about the need for labelling to be specifically targeted to the product and the concerns raised.

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

It is taken that the Discussion Paper refers to labelling smart devices physically and then providing the label information about that category of device in an online database that is searchable by the public.

Implementing a meaningful labelling scheme for smart devices would be beneficial for manufacturers, especially for those who make efforts to improve the security of their products. Labels should be both in digital and physical form to prevent/mitigate counterfeiting.

This approach would be in keeping with communicating useful evaluation information to consumers via as many channels as possible. For both consumers and manufacturers, it would have the benefit of also allowing for updates in information via the digital channel, should new security holes be found after shipping. A QR code could be one way to do this that would allow updating of information about known security flaws discovered over time, and how to fix them or otherwise

Chapter 9: Health checks for small businesses

Question 25: Is there anything else we should consider in the design of a health check program?

By a health check program, it is understood that the Discussion Paper refers to an online information sheet with a tick list of improvements to complete for the average small business. If so, this would be beneficial for the small business community. However, while necessary and beneficial, this is not sufficient to improve cybersecurity.

To improve small business cybersecurity, the technology adopter typically needs someone to walk it through for them, addressing their customised issues, and trouble-shooting those issues on the spot. In Europe and the US, one approach used to address this is for government to provide grants to not-for-profit organisations, education institutions, or professional associations to provide free cybersecurity tune-ups to important projects.

This approach would be worth adapting to the Australian context. The technical tune-up program represents value for public money as it fortifies software across private and public sectors and in so doing, raises the overall security of a diversity of supply chains and industries.

Chapter 10: Clear legal remedies for consumers

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

We agree with the Inquiry that the Australian Consumer Law (ACL) has a complementary role to play in both promoting cyber secure practices and providing a remedy to consumers harmed by cyber breaches. It also provides a basis for robust and effective enforcement of

cybersecurity standards and cyber best practice by the regulator, along with the potential to impose penalties for breaches.

The consumer guarantees in the ACL are expressed as 'open-textured' standards,[11] which means they can adapt to changes in consumer markets and new risks of harm such as through increased reliance on emerging technologies. For example, the guarantee of acceptable quality (ACL s54) refers to safety as a consideration. In modern contexts considerations of safety arguable extend to cybersecurity and privacy/ data protection.

The Discussion Paper notes several functional challenges in applying the consumer guarantees. Our comments are listed below:

Determining the transaction is for a good or service

As the Discussion Paper notes, although the definition goods in s3 of the ACL includes software, there are concerns that some aspects of digital products may not fall within the definition of either goods or services.[12] As such it would be desirable in Australia to consider new rules in relation to digital content and consumer remedies such as found in the United Kingdom, in Chapter 3 of the *Consumer Rights Act 2015 (United Kingdom)* which applies traditional statutory rights of satisfactory quality, fitness for purpose and compliance with description to digital content, as well as remedies for breach.

Identifying the responsible business

As the Discussion Paper notes, many digital goods and services are made by multiple businesses, and it can be difficult to tell which business is responsible for a cybersecurity failure. However, in terms of responsibility for the failure and obtaining a remedy, in many cases the business who supplied the product, or identified as manufacturing the product will be liable to the consumer. This means the consumer is not responsible for identifying who made the parts with a cyber weakness. It will then be that manufacturing or importing firm's responsibility to seek contribution from those who made components for the product and which may have been responsible for the cyber breach. A more difficult issue arises with networked devices where it may be problematic to determine which device was responsible as a matter of fact for the weakness.[13] More generally the greatest hurdle for the consumer in bring an action to recover compensation for harms caused by weak cybersecurity in a smart device will be having the technical expertise to prove the claim, particularly the causal link between the harm complained of and the device. This underlies the important role of the expert regulator and for a specialist tribunal or ombudsman service, as discussed below.

Determining what went wrong

The Discussion Paper notes that significant technical expertise might be required for determining whether a cyber breach also amounts to a breach of the consumer guarantees. A comparable issue exists with motor vehicles, where it is often difficult for consumers to establish a failure in the performance of a car is a breach of the guarantees or just age related.

---

[11] Bant, E, and Paterson, J. "Statutory Interpretation and the Critical Role of Soft Law Guidelines in Developing a Coherent Law of Remedies in Australia". *New Directions for Law in Australia: Essays in Contemporary Law Reform*, edited by Levy, R, and O'Brien, M, et al., 1 ed., ANU Press, 2017, pp. 301-309.

[12] See further J M Paterson, *Corones' Australian Consumer Law* (2020) ch 8.

[13] Noto La Diega, Guido and Walden, Ian, *Contracting for the 'Internet of Things': Looking into the Nest* (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016, Available at https://ssrn.com/abstract=2725913.

Once suggestion is for specialist dispute resolution tribunals.[14] A similar approach might be adopted for cyber breaches or breaches affecting privacy. However, it may be preferable to adopt an ombudsman service which is responsible for investigating complaints. An ombudsman service has the attraction of lifting the burden from individuals in proving and pursuing redress for cyber breach harms. An ombudsman service can also identify systemic concerns which can be reported to the regulator.[15]

Access to justice

Regulators should be given greater powers to enforce compliance with the consumer guarantees beyond relying on misleading representations about the scope of guarantees rights, which does not always produce consumer welfare promoting outcomes.[16]

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

We note that an effective incentive to firms in providing strong cybersecurity protection is provided by privacy and data protection law. As such we agree with the proposals for strengthened data protections for consumers and enforcement powers for regulators made by the ACCC in the Digital Platforms Report (2019)[17] and under consideration in the current review of the Privacy Act 1988.[18]

We recommend that giving consumers greater control over their data, including to review, correct and withdraw data (as under the GDPR[19] and envisaged under the Consumer Data Right[20]) also gives consumers a self-help response to firms that fail properly to engage with cyber protections. To put is another way, if you want to have a voluntary-based scheme for most cybersecurity protections, then you must make it easy, costless and information-searchable for consumers, and their data, to exit from a company and their product should that product not meet reasonable consumer expectations

Chapter 11: Other issues

Question 28: What other policies should we consider to set clear minimum cybersecurity expectations, increase transparency and disclosure, and protect the rights of consumers?

The Australian Government should legislate a right to repair. We refer to the inquiry currently being conducted by the Productivity Commission on this issue.

As covered in the inquiry, a right to repair allows owners to update devices when firms cannot or will not repair security flaws. It also allows consumers to protect themselves after support periods have ended, without incurring substantial expenses from the purchase of

[14] S Corones, '*Why Australia needs a motor vehicle 'Lemon' Law'* (2016) 39(2) *University of New South Wales Law Journal*, pp. 625-657.
[15] See also ACCC, *Digital Platforms Inquiry Report* (2019) recommending an ombudsman for resolving complaints and disputes between individuals or small business and online platforms.
[16] See *ACCC v LG Electronics* [2018] FCAFC 96.
[17] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
[18] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988
[19] https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/
[20] https://www.cdr.gov.au/

unnecessary new devices, leading to economic efficiencies. Similar laws passed in the USA has included the following:

- Invalidation of license clauses that restrict the rights of consumers and independent operators to repair, update, and patch common devices.
- Explicit exemptions from copyright law that prevent circumvention of DRM and similar technologies
- Requires OEMs to provide access to parts, documentation, firmware, and other necessary components on a fair and equal basis

Opponents of a right to repair have argued that such laws may harm security by requiring them to disclose information that could be used to exploit products. However, experts both (academic and within industry) uniformly agree that security which depends on obscuring functional characteristics offers very poor guarantees. Thus, right to repair will only identify products that had insufficient protection to begin with.

Contributors from the University of Melbourne

Amit Achrekar, Director, Cybersecurity, Business Services

A/Professor Atif Ahmad, Deputy Director for the Academic Centre of Cybersecurity Excellence

Professor Shanton Chang, School of Computing and Information Systems and Associate Dean (International) at the Faculty of Engineering and Information Technology.

Dr Shaanan Cohney, Senior Lecturer, School of Computing and Information Systems, Affiliate, Princeton University Center for Information Technology Policy

Dr Suelette Dreyfus, Lecturer, School of Computing and Information Systems

Professor Chris Leckie, School of Computing and Information Systems

A/Prof Toby Murray, Senior Lecturer, School of Computing and Information Systems

Professor Jeannie Paterson, Melbourne Law School, Co-Director of the Centre for AI and Digital Ethics, and Co-Leader, Digital Access and Equity Research Program in the Melbourne Social Equity Institute, with input from student interns Carmelina Contarino, Liam Harding, and Lucy Wiseman.

Dr Thuan Pham, Lecturer, School of Computing and Information Systems

Professor Liz Sonenberg, Pro Vice-Chancellor (Research Infrastructure & Systems), Chancellery