

STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS & INCENTIVES

DATE: 1 September 2021

Contact:

Andy Kuoch,
Policy Officer

Tel: [REDACTED]

E: [REDACTED]

Web: www.liv.asn.au

© Law Institute of Victoria (LIV)

No part of this submission may be reproduced for any purpose without the prior permission of the LIV. The LIV makes most of its submission available on its website at www.liv.asn.au



TABLE OF CONTENTS

| | |
|--|------------------------------|
| Introduction | 3 |
| Recommendations | 4 |
| Executive Summary | Error! Bookmark not defined. |
| Chapter 2: Why Should Government Take Action? | 6 |
| 1. What are the factors preventing the adoption of cyber security best practice in Australia? | 6 |
| 2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not? | 7 |
| Chapter 3: The Current Regulatory Framework | 8 |
| 3. What are the strengths and limitations of Australia’s current regulatory framework for cyber security? | 8 |
| 4. How could Australia’s current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements? | 10 |
| Chapter 4: Governance Standards for Large Businesses | 12 |
| 5. What is the best approach to strengthening corporate governance of cyber security risk? Why? | 12 |
| 6. What cyber security support, if any, should be provided to directors of small and medium companies?..... | 13 |
| Chapter 5: Minimum Standards for Personal Information | 14 |
| 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? | 14 |
| 9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards? | 15 |
| 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?..... | 15 |
| Chapter 6: Standards for Smart Devices | 16 |
| 11. What is the best approach to strengthening the cyber security of smart devices in Australia? | 16 |
| 12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices?..... | 16 |
| Chapter 6: Labelling for Smart Devices | 17 |
| 16. What is the best approach to encouraging consumers to purchase secure smart devices? Why? | 17 |
| 17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?..... | 17 |
| 18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? | 17 |

| | | |
|---|--|-----------|
| 19. | Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?..... | 18 |
| Chapter 8: Responsible Disclosure Policies | | 19 |
| 22. | Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered? | 19 |
| Chapter 9: Health Checks for Small Businesses | | 19 |
| 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? | 19 |
| Chapter 10: Clear Legal Remedies for Consumers | | 20 |
| 24. | What issues have arisen to demonstrate any gaps in the ACL in terms of its application to digital products and cyber security risk?..... | 20 |
| 25. | Are the reforms already being considered to protect consumers online through the <i>Privacy Act 1988</i> and the ACL sufficient for cyber security? What other actions should the Government consider, if any? | 21 |
| 26. | What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers? | 24 |
| Conclusion | | 24 |

INTRODUCTION

The Law Institute of Victoria (**‘LIV’**) is Victoria’s peak body for lawyers and represents more than 19,000 members working and studying in the legal sector in Victoria, interstate and overseas. The LIV welcomes the opportunity to provide this written submission to the Department of Home Affairs’ (**‘DHA’**) consultation on *Strengthening Australia’s Cyber Security Regulations and Incentives* (**‘the Consultation Paper’**).

The LIV recognises the need for an overarching framework for cyber security regulation in Australia. The proposed regulatory framework must consider the comparatively few regulatory burdens for local businesses seeking to innovate in Australia and for those global businesses looking to expand into the Australian market. The LIV cautions against reform that would discourage businesses and corporations from venturing into or remaining in the Australian market, noting the DHA’s intention to consider a whole of economy approach to cyber regulation.

The LIV supports initiatives which encourage greater involvement from consumers, business owners, and company directors in cyber security risks. Unfortunately, cyber security expertise is often relegated to internal/external information technology (IT) teams, while many consumers rely on an assumption that cyber services and smart devices are sufficiently protected from cyber threats. It is vital to the strength of Australia’s cyber security environment that education is

encouraged at all levels of the market, from consumers to company directors, to reduce the siloed nature of cyber security expertise and encourage a level of responsibility and accountability for threats.

RECOMMENDATIONS

This submission is informed by the LIV Technology and Innovation Section's Privacy, Cybersecurity and Risk Sub-Committee. The LIV recommends:

1. The DHA consider that an approach to non-compliance or poor cyber security practices, such as that taken by the EU under the GDPR, risks too great an emphasis on penalising non-compliance rather than demonstrating the value of compliance.
2. That the overarching framework for cyber security in Australia to respond to the gaps and inconsistencies in the legislative framework consider the issues in relation to the definition of personal information under the Privacy Act; the ambiguity around digital products and its coverage under the ACL's goods and services definitions; the ACLs 'reasonable consumer test'; the scope of misleading and deceptive conduct provisions in this digital context; and the absence of clear guidance for director's duties in the context of cyber security.
3. Consideration of the American Institute for Security and Technology's *Combatting Ransomware Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*.
4. Improvement of coverage of cyber security requirements under the current regulatory environment through implementation at the federal level before being narrowed under state-based requirements, as state-based regulations are currently inconsistent.
5. Amendment to the Privacy Act precluding businesses who are handling financial and sensitive information, including personal information, from the small business exemption.
6. Development of a voluntary Small Business Code, including standards of privacy practices that small businesses must abide by under the Code to promote self-regulation and improve coverage of cyber security requirements.
7. Introducing financial penalties which are proportionate with company revenue to ensure that larger businesses are sufficiently covered by the penalty thresholds and it is not otherwise deemed the cost of doing business.
8. Option 1 for voluntary governance standards, noting the risk of a 'checkbox' response to compliance under the corporate governance framework.
9. The DHA consider making available support for SMEs to ensure that cyber security obligations do not become a barrier to establishing new businesses in Australia, which

- could include independent technical support, more frequent/practical best-practice advice or subsidies with industry standard services (e.g. common network security providers).
- 10.** Additional education and awareness raising initiatives to reduce the siloed nature of cyber security expertise in large organisations, for example through expanding initiatives such as the Cyber Security Awareness Month and stakeholder engagement with c-suites or mandatory reporting requirements on cyber security practices.
 - 11.** Consideration of internationally accepted Standards or Codes such as the NIST Security Guidelines or SOC 2 and their appropriateness in the Australian context, with a view to providing a level of consistency and ease for Australian businesses seeking to venture into overseas markets.
 - 12.** Broad technical controls which are directed towards key areas of cyber security, including: User Access, incident and event management, cyber breaches, access logging and other key areas that are fundamental to reducing cyber breaches and protecting data generally.
 - 13.** The adoption of ESTI EN 303 645 as an appropriate international standard for smart devices, noting the low priority in strengthening Australia's cyber security regulations and incentives, and the importance of a cautious adoption of standards in view of the impact of this standard in other jurisdictions.
 - 14.** Consideration of a prescribed timeline of security support, acknowledging that a prescribed minimum period under a mandatory labelling scheme will likely be low cost for businesses and will also provide a significant benefit for consumers.
 - 15.** That if forced disclosure were mandated in Australia, the liability of companies must be limited to encourage companies to make disclosures.
 - 16.** As an alternative to the cyber security health check program, implementing a business education survey which outlines a business' obligations under a regulatory framework based on the type of data held, how the information is stored and the actions a business should undertake.
 - 17.** Clarity in the current definitions in the ACL with regards to how digital products fits within goods or services and in identifying the responsible business for consumer recourse.
 - 18.** The introduction of a statutory tort for serious invasions of privacy which should be limited to:
 - i. Intrusion Upon Seclusion; and
 - ii. Public Disclosure of 'Private Facts'
 - 19.** Implementing a notice and remedy period for each breach that gives reasonable opportunities for the controller/processor to take action to mitigate the breach.
 - 20.** The Introduction of a limitation of liability scheme with monetary caps for businesses that report in a timely period and have taken reasonable steps to enable information sharing about the breach.

Chapter 2: Why Should Government Take Action?

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

The Consultation Paper identifies that cyber security threats targeting Australia's national and economic interests are increasing in frequency, scale, and sophistication. The Australian Institute of Criminology has estimated the total economic impact of pure cybercrime in 2019 was approximately \$3.5 billion.¹ The LIV notes that the low level of overall maturity of cyber security legislation in Australia prohibits the introduction and development of broader cyber security best practices. This lack of holistic legislation or defined standards for cyber security best practice in Australia is a significant factor preventing the adoption of appropriate and secure policies, procedures, and technology by businesses.

Further, cyber security expertise is generally siloed in practice. Businesses expect cyber risks to be monitored and prevented by internal or external IT teams, often without engagement from a company's board of directors. As a result, organisations are taking very little ownership of cyber security and have a minimal or casual understanding of the obligations and risks. This increases cyber vulnerabilities where organisations are not aware of the nature of the information held, how the data could be accessed or weaponised, and how the data could be better protected, which should inform how to define the cyber security framework of their business. The LIV notes that while most organisations want to be associated with cyber security best practice, the issues relate to the siloed development of cyber structures and systems within organisations are often without practical application of systems and risk.

¹ Coen Teunissen, Isabella Voce, Russell Smith, 'Estimating the cost of pure cybercrime to Australian individuals' (Australian Institute of Criminology, Statistical Bulletin no 34, 2021).

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

The LIV agrees with the need for further government action on cyber security to address negative externalities and information asymmetries, which are disincentivising organisations from investing in cyber security. Addressing negative externalities by imposing clear liability would encourage organisations to change their practices, by placing greater cyber security measures upon the data they keep and decreasing the amount of unnecessary data that increases their risk and liabilities.

Education and Training Grants

Government action in education and grants for government-supported programs that aim to promote cyber awareness in organisations require a more consistent approach and greater oversight over how these grants are being applied. The LIV notes that Australian government has contributed significant funding to support education and training grants through the Australian Cyber Security Growth Network Nodes (**'AustCyber'**) and cyber investment grants provided to industry and education providers, including for example TasTAFE in Tasmania.

However, this significant funding is without a well-defined approach which targets the application of cyber security and promotes communication between stakeholders. AustCyber are a network across Australia working with different levels of government designed to 'foster and accelerate cyber capability development' and 'develop a strong and confident ecosystem that supports creating mature, market-ready and competitive local businesses' across Australia.² On 15 February 2021, AustCyber announced that it would become a wholly-owned subsidiary of Stone & Chalk,³ and will continue to operate as one of the Australian Government's Industry Growth Centres, until the end of its Funding Agreement on 30 June 2022.⁴

TasTAFE received a \$1.45 million grant through the Australian Government's Security Skills Partnership Innovation Fund to establish a Cyber Innovation Training Hub. This project will provide security training to small business, ICT professionals, and individuals, and provide a Certificate IV in Cyber Security or a nationally accredited Diploma or Advanced Diploma in ICT. While the LIV

² AustCyber, *AustCyber's National Network of Cyber Security Innovation Nodes*. Available at <<https://www.austcyber.com/grow/collaborate/nodes>>.

³ Stone & Chalk and AustCyber merge to accelerate growth for Australian emerging technology companies, Media Release (15 February 2021), <<https://www.austcyber.com/sites/default/files/2021-02/Stone-%26-Chalk-and-AustCyber-merge-to-accelerate-growth-for-Australian-emerging-technology-companies.pdf>>.

⁴ *Two Powerful Networks Connected by Commitment, Inspired by Impact* <<https://austcyber.com/shapingthefuturetogether>>.

applauds these significant investments, the provision of point-in-time funding is not always effective to advance such cyber capability development.

Chapter 3: The Current Regulatory Framework

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

Strengths

The flexibility within the current Australian cyber security environment provides opportunities to align with and utilise aspects of existing regulatory frameworks in other jurisdictions. LIV members report a broader appetite to adhere to and seek some level of conformity with the patchwork of legislation within the regulatory framework, which the consultation paper rightly identifies is limited in incentivising uptake of uniform cyber security standards.

As many Australian businesses operate globally, these organisations have developed systems and policies which meet existing frameworks and standards internationally. The flexibility in the Australian environment means there is opportunity for alignment with existing regulatory frameworks elsewhere. This would be valuable for creating a streamlined process for businesses expanding globally, as international companies must navigate many hurdles to set up in different countries, due to lack of uniformity and guidance. LIV members note the many benefits to establishing a business in Australia, due to the openness to innovation and ease for small businesses in relation to privacy. Benefits are drawn from a stable government, an established common law system, and a level of regulatory flexibility for new businesses seeking to expand overseas. LIV members recognise that Australia is well-placed to be an innovation hub for technology businesses in the Asia Pacific region, positively contributing to Australia's economic growth.

While supportive of holistic reform contemplated by the DHA to Australia's regulatory framework for cyber security, the LIV cautions against reform which has the effect of limiting technological innovation growth in the country, small business innovation and entrepreneurship in Australia. The LIV notes that the GDPR, for example, may be restrictive in this regard, due in part to its burdensome nature, it leading to confusion due to its onerous provisions and it being unsettled and

in a massive state of flux.⁵ Investment in European start-ups have reportedly dropped by 36 per cent compared to American or other global start-ups since the rollout of the GDPR.⁶

Moreover, compliance obligations under the GDPR are quite high, with data privacy compliance more difficult due to data subject access requests ('**DSAR**') in locating personal data in an unstructured format, monitoring data protection practices of third parties and data minimization.⁷ Strong identical personal data in various formats spread among different systems makes responding to DSARs more time consumer and costly.⁸ The LIV notes that the Californian Consumer Privacy Act also has a DSAR component, so these issues are not confined just to the GDPR. Moreover, with GDPR fines rising by nearly 40% in the period between 26 January 2020 and 27 January 2021, with penalties amounting to \$191.5 million, the LIV considers this approach to non-compliance or poor cyber security practices risks too great an emphasis on penalising non-compliance rather than demonstrating the value of compliance.

Limitations

The LIV recognises that Australia's current regulatory framework consists of different and overlapping pieces of legislation, resulting in a lack of consistently defined terms and obligations. The Consultation Paper identifies three key pieces of legislation which are intended to cover the whole economy approach, including the Privacy Act, the Corporations Act and the Australian Consumer Law. In comparison, the European Union's ('**EU**') General Data Protection Regulation ('**GDPR**') is more heavily developed and comprehensive in scope.

The LIV recommends that an overarching framework for cyber security in Australia to respond to the gaps and inconsistencies in the current legislative framework, ought to consider the issues in relation to the definition of personal information under the Privacy Act; the ambiguity around digital products and its coverage under the ACL's goods and services definitions; the ACL's 'reasonable consumer' test; the scope of misleading and deceptive conduct provisions in this digital context; and the absence of clear guidance for director's duties in the context of cyber security.⁹ Clarifying

⁵ Nicholas Martin et al, 'How Data Protection Regulation Affects Startup Innovation' (2019) 21 *Information Systems Frontiers* 1321; Norton Rose Fulbright, 'Schrems II Landmark Ruling: A Detailed Analysis' (July 2020) <<https://www.nortonrosefulbright.com/en-au/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis>>.

⁶ James Hercher, 'Academic Study Shows European Startup Investments Diminished in the Wake of the GDPR', *Adexchanger* (6 August 2021) < <https://www.adexchanger.com/data-exchanges/academic-study-shows-european-startup-investments-diminished-in-the-wake-of-gdpr/>>.

⁷ IAPP-EY Annual Privacy Governance Report 2019," IAPP-EY, www.iapp.org, 2019.

⁸ Meribeth Banaschik, 'How to comply with data subject access requests' (15 December 2020) < https://www.ey.com/en_au/forensic-integrity-services/how-to-comply-with-data-subject-access-requests>.

⁹ *Corporations Act 2001* (Cth), s 180(1), 181.

these existing gaps and providing further guidance through an overarching framework for cyber security would greatly assist in strengthening Australia's regulatory framework.

LIV members report a lack of a structured governmental programs for knowledge-sharing across incident response, including ransomware, limit a considerable volume of learning and prevents stronger engagement with cyber security at the highest levels of organisations, including Chief Information Officers and Chief Technology Officers. Additionally, there is a lack of policy and clarity around laws relating to ransomware attacks. In America, the Institute for Security and Technology have developed the '*Combating Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*' (**'the Ransomware Framework'**) to provide guidance for American organisations wishing to prevent or respond to ransomware attacks.¹⁰ The Ransomware Framework provides a summary of recommendations, based on three goals for responding to the prevalence of ransomware attacks,¹¹ which the DHA should consider with respect to Australia's regulatory framework. The Ransomware Framework also outlines the practical challenges in preventing ransomware attacks through a prohibition on ransom payments while recognising the lack of organisational cyber security maturity across sectors, different sizes of organisation and locations.¹² The Ransomware Framework recommends three factors to consider before prohibiting ransomware payments, including:

- Allowing governments and organisations time to adapt to the abrupt change in law. This requires time-based milestones to allow for the implementation of victim support programs and appropriate insurance policies for private insurers.
- Phasing in prohibitions in specific sectors over time. Prohibitions on ransomware payments could be enacted on public entities before being extended to the private sector.

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

The LIV highlights the importance of clear definitions and a cohesive approach to terminology for improving clarity in Australia's cyber security environment, either within Federal/State and Territory legislation or within regulator Standards. The LIV notes that state-based regulations are

¹⁰ Institute for Security and Technology, *Combating Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force* (Report). Available at <<https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf>>.

¹¹ Ibid p 52-53.

¹² Ibid p 49-50.

inconsistent and recommends that to improve coverage, and in contrast to the absence of a clear federal approach to cyber security in the United States of America, it ought to begin at the federal level before being narrowed under state-based requirements. The current regulatory framework does not have sufficient scope or scale to deal with anonymous data breach disclosure schemes. Enforcement could be improved by assessing frameworks to identify scope and scale of issues and target that towards evidence-based regulation.

The LIV notes a significant lack of enforcement in cyber security regulation, to the detriment of its development in Australia. The Australian Consumer Law (**'ACL'**) is currently being used to deal with damage resulting from cyber incidents, but this is insufficient where a consumer seeks to enforce their rights without the support of the Australian Competition and Consumer Commission (**'ACCC'**), where a consumer is not aware of the negative externalities resulting in the incident, which can present challenges in identification of the responsible business.

Coverage under the *Privacy Act 1988* (Cth) could be improved through the implementation of a statutory tort for serious invasions of privacy, as well as clarifying the scope of organisations bound by the Act. The LIV supports the recommendation of the Office of the Australian Information Commissioner (**'OAIC'**) that exemptions under the *Privacy Act 1988* (Cth) should be minimised in order to achieve uniformity and consistency.¹³ In its current form, the Act provides for an exemption for agencies and organisations with an annual turnover of less than \$3 million,¹⁴ although they are bound by the Australian Privacy Principles (**'APP'**) in certain circumstances.¹⁵ Acknowledging the need to strike a delicate balance between privacy concerns and the burden placed on small businesses, the LIV recommends the retention of precluding businesses from the small business exemption, who are handling financial and sensitive information, including personal information.¹⁶

However, given the onerous obligations for small businesses, the LIV supports the inclusion of a carveout for those businesses holding significantly less data. As suggested by the Australian Law Reform Commission (**'ALRC'**), this may be achieved through the introduction of an 'accreditation scheme to encourage small businesses to opt in' under s6EA of the Act.¹⁷

Additionally, the LIV recommends the development of a Small Business Code (**'the Code'**), including standards of privacy practices that small businesses must abide by under the Code. A

¹³ Office of the Australian Privacy Commissioner, Submission *PR 215* to the Australian Law Reform Commission, 'The Number and Scope of Exemptions' (16 August 2010) [33.41].

¹⁴ *Privacy Act 1988* (Cth) ss 6C, 6D.

¹⁵ *ibid* s 6D (4).

¹⁶ Australian Law Reform Commission, Review of the Small Business Exemption (15 July 2014) [16.56] <<https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/16-new-regulatory-mechanisms/review-of-the-small-business-exemption/>>.

¹⁷ *ibid*.

non-prescribed voluntary code may be useful in promoting self-regulation and improve coverage of cyber security requirements.

Chapter 4: Governance Standards for Large Businesses

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

Members consider that the lack of standardised terms, coherent regulatory standards or mechanisms for enforcement means there is little appetite to strengthen corporate governance of cyber security risk. Even amongst APRA-regulated entities, there is minimal desire to improve corporate governance of cyber security risk prevention due to the siloed construction of cyber expertise within organisations.

The best approach to improving corporate governance requires incentives to motivate corporations to decrease their cyber security risk and promote a secure by design approach. Company directors must be incentivised to take a certain level of responsibility for cyber security risk to decrease the siloed nature of cyber expertise within organisations. Following the enactment of the GDPR, European businesses became compliant under the regulations to avoid the risk of substantial fines and reputational damage. The LIV is of the view corporations could be motivated to strengthen their corporate governance of cyber security risk through a deterrent approach in the short-term, with a reasonable amnesty period to allow corporations to adapt their systems and policies.

The LIV supports financial penalties which are proportionate with company revenue to ensure that larger businesses are sufficiently covered by the penalty thresholds and it is not otherwise deemed the cost of doing business. Under the GDPR, fines for cyber incidents or breaches are tied to the organisation's revenue.¹⁸ If the regulatory framework outlines financial penalties for cyber incidents, the fine should be capped at a percentage of the organisation's revenue. This would incentivise regulatory compliance in industries, while ensuring that SMEs are not disproportionately affected by overwhelming penalties under the regulations.

However, the LIV agrees with the DHA's proposition that the introduction of mandatory governance standards for larger businesses under Option 2 may interact poorly with other jurisdiction's

¹⁸ *General Data Protection Regulation* (European Union), article 83.

regulation of cyber security, which would be prohibitive for multinational corporations seeking to invest in providing goods and services to the Australian market. While proffering Option 1 for voluntary governance standards, the LIV cautions that this corporate governance framework might risk compliance being a 'checkbox' response, with corporations engaging a software provider with a check-box solution. This will increase the risk if corporations are offloading responsibility onto third parties or software which is not appropriately adapted to the corporation.

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

The LIV agrees with the need for extensive cyber security support to be provided to directors of small and medium companies ('SME'). The LIV reiterates that any proposed regulatory framework must include clearly defined terms to enable directors to understand their obligations in relation to the context of information held within their companies. Directors of Australian SMEs may already be under a significant burden from navigating their directors' duties and workplace health and safety obligations. LIV members caution against imposing additional regulatory burdens on directors which would enable the courts to pierce the corporate veil and impose liability for a cyber security breach onto directors or shareholders. LIV members are not aware of any class action lawsuits that have been instigated as the result of a cyber incident. This may be, in part, because there is no current financial punishment associated with a cyber breach, so losses are instead quantified by damage to reputational harm, which is difficult to quantify.

The low level of confidence and maturity within the cyber security industry is proportionate to the level of disclosure, amnesty and support provided to data processors and other impacted services in the industrial relations sector. LIV members report that there are currently little support services to refer SME directors for specific cyber security guidance in Australia. The LIV recommends making available support for SMEs to ensure that cyber security obligations do not become a barrier to establishing new businesses in Australia. This could include independent technical support, more frequent/practical best-practice advice or subsidies with industry standard services (e.g. common network security providers). Grants could be made for proactive engagement and support could be provided to enhancing competition of cyber security testing, self-reporting/public reporting of maturity. Legal protection could also be afforded through demonstrable efforts to improve or maintain cyber security posture within business.

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

The LIV submits that additional education and awareness raising initiatives could reduce the siloed nature of cyber security expertise in large organisations and strengthen corporate governance of cyber security risk. This could include an expansion of Cyber Security Awareness Month into corporate environments, key stakeholder engagements with c-suites or mandatory board reporting requirements on cyber security practices. Moreover, to encourage engagement, this could involve initiatives such as centralised marketing campaigns to business and community groups involved in this space, education grants, and education around cyber risk and tracking metrics.

Chapter 5: Minimum Standards for Personal Information

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?

The LIV is of the view that a cyber security code under any federally mandated piece of legislation would support greater clarity and regulation within the cyber security space. The New South Wales Government, in collaboration with Standards Australia and AustCyber, recently considered the development of harmonised cyber security standards.¹⁹ The NSW Cyber Security Standards Harmonisation Taskforce Recommendations Report (**'the Recommendations Report'**) identified seven priority areas for development, implementation and application of the standards to build a resilient cyber infrastructure across sectors. The Recommendations report supported the adoption of recognised International Organisation for Standardisation (**'ISO'**) or International Electrotechnical Commission (**'IEC'**) standards to outline baseline requirements for information security, protective security, and supply chain and risk management. The report cautioned against creating duplicative requirements at a cost to the business and broader community, and

¹⁹ Standards Australia, "NSW Cyber Security Standards Harmonisation Taskforce" (Report, January 2021) p 9, available at < <https://www.standards.org.au/getmedia/c634a11d-3336-401f-8742-f4b9671fa195/NSW-Cyber-Security-Standards-Harmonisation-Taskforce-Recommendations-Report.pdf.aspx>>.

recommended any approach to cyber security standards should enable businesses to “leverage their existing compliance or identify a maturity lift required from the baseline [requirements]”.²⁰

Despite the potential difficulty in assessing the appropriateness of already recognised Standards in the Australian context, the LIV agrees that an approach could be to adopt international accepted Standards or Codes as a guide, such as NIST Security Guidelines or SOC 2,²¹ to provide a level of consistency and ease for Australian businesses seeking to venture into overseas markets.

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

The LIV reiterates that any consideration of a cyber security code under the Privacy Act must avoid unnecessary duplication resulting from the current review and avoid being too specific or effectively introducing another set of standards that conflicts with established standards used commonly within industries, particularly the proprietary standards. The LIV acknowledges that technical controls included as part of a code under the Privacy Act would be appropriate for areas not already covered by Australian Regulations/Frameworks and would have broader flow-on effects for cyber security as a whole.

The LIV recommends that broad technical controls should be directed towards key areas of cyber security, including: User Access, incident and event management, cyber breaches, access logging and other key areas which are fundamental to reducing cyber breaches and protecting data generally.

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?

²⁰ Ibid.

²¹ Databrackets, 'Comparing NIST, ISO 27001, SOC 2, and Other Security Standards and Frameworks (Online, 9 September 2020) < <https://databrackets.com/comparing-nist-iso-27001-soc-2-and-other-security-standards-and-frameworks/>>.

The types of data which should be covered by a cyber security code are recognised in Australian legislation and international regulatory frameworks. The LIV supports the maintenance of well-established and defined terms to ensure consistency across Australian and overseas jurisdictions. Under the Privacy Act for example, it is critical to clarify personal information in this context and the distinction between information about an individual and relating to an individual. 'Personal Information' is currently defined to include: a name, signature, address, phone number, date of birth, IP address, geolocation information, voice print and facial recognition biometrics, credit information, health information and sensitive information.²² The GDPR outlines 'Personal Data' as "any data that can be used to identify a specific individual, including names, phone numbers, email addresses, IP addresses, login details, geolocation information, or physical, genetic, economic, cultural or social identifiers."²³

Chapter 6: Standards for Smart Devices

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

The LIV acknowledges that very few smart devices are produced in Australia and queries whether there is a benefit to enforcing standards in this area, when cyber security standards are being enforced in those countries that are developing these smart devices already. The LIV reiterates the importance of avoiding the imposition of barriers for businesses and corporations in or entering Australia. Instead, government and industries should direct efforts towards consumer education to support consumers to make informed consumer choices around smart devices.

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

The LIV supports the adoption of ESTI EN 303 645 ('**ESTI**') as an appropriate international standard for smart devices. The adoption of international standards for smart devices in the UK, Singapore, California, and Oregon provides Australia with an opportunity to observe and analyse

²² *Privacy Act 1988* (Vic) s 6(1), s 6FA.

²³ *General Data Protection Regulation* (European Union), art 4.1.

the comparative effectiveness or consequences of these standards.²⁴ The LIV supports a cautious approach to the adoption of standards, which takes advantage of the opportunity to track and measure the impact of the ETSI standards in other jurisdictions. LIV members reiterate the importance of maintaining Australia's regulatory openness before imposing a standard which may create barriers for industry. The prevalence of different international standards indicates the need for standards tailored to a country's priorities and industry. Additionally, the LIV is concerned that the adoption of a baseline standard will foster a 'checkbox' response to compliance from corporations.

The LIV considers the adoption of an appropriate standard to be a low priority for strengthening Australia's cyber security regulations and incentives. In the interim, it may be beneficial to encourage the use of end-user licensing agreements for smart devices to provide consumers recourse through the courts. However, the LIV notes the barriers to accessing this recourse where it is often difficult to quantify losses and the losses being so low may have the consequence that legal action (unless it is collective) is not commercially viable.

Chapter 6: Labelling for Smart Devices

- 16. What is the best approach to encouraging consumers to purchase secure smart devices? Why?**
- 17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?**
- 18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?**

The LIV recognises that similar approaches to product labelling have been implemented in other jurisdictions, including Singapore, Finland, the UK and the US and these examples could provide a comparative basis for the implementation of a voluntary labelling scheme in Australia.

²⁴ UK Department for Digital, Culture, Media and Sport 2021, *New cyber security laws to protect smart devices amid pandemic sales surge*, <available at <https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge>>; Cyber Security Agency of Singapore 2021, *Cybersecurity Labelling Scheme (CLS)*, available at ><https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls>>; SB-327 *Information privacy: connected devices*. Available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327>; *House Bill 2395*. Available at <<https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled>>.

However, the LIV queries how a voluntary star rating label outlined under Option 1 in the Consultation Paper would be meaningful and effective across the many different industries and areas and if any organisations would be in a position to provide accreditation effectively. Unlike energy star ratings for goods and appliances, there does not appear to be an appropriate metric for calculating the cyber security of smart devices, given this standard would likely be universally applied, for example, to a WiFi-enabled light globe or baby monitor. Additionally, given the wide range of software, applications and tools that may be eligible for accreditation and the practical barriers in keeping up to pace with rapidly developing cyber security threats, this may hamper the coordination of accreditation that is effective, flexible and adaptable.

Given the practical difficulties of adopting a labelling or standard for smart devices, it is likely that a consumer may still suffer a loss as the result of a cyber incident, despite purchasing the product in reliance of the label or standards. The LIV is concerned that this approach will create more mistrust in government or regulatory bodies and increase confusion for consumers, where the regulations do not keep ahead of evolving cyber security risks. Many companies across various industries are advertising cyber security as a point of difference in the market already. The LIV is concerned that a voluntary label will not have a significant impact on consumer decisions or broader scale producers, including Microsoft or Apple, but may create a marker barrier for smaller businesses.

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

The LIV supports the development of a mandatory security expiry date label for smart devices under a mandatory labelling scheme outlined under Option 2 in the Consultation Paper, while noting various practical concerns around the implementation of such a scheme, such as in requiring online retailer operating entirely overseas to use a label and that it would only display the security of a device at one point in time.

The Consultation Paper does not consider a prescribed timeline of security support for smart devices. The introduction of a mandatory security expiry date would require some level of security support during this period to meet the warranty. The LIV recommends consideration of a prescribed timeline of security support, acknowledging that a prescribed minimum period under a mandatory labelling scheme will likely be low cost for businesses and will also provide a significant benefit for consumers.

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?

LIV members report that Australian companies are hesitant to disclose data breaches where it may result in negative media attention. Under the EU's GDPR, mandatory reporting is required where companies have experienced a cyber incident and are subsequently fined significantly. In America, there is scope within the framework for anonymously reporting ransomware incidents to encourage voluntary disclosure.²⁵

The LIV submits that if forced disclosure were mandated in Australia, the liability of companies must be limited to encourage companies to make disclosures. However, this is a concern for consumers, who may subsequently be unable to recover loss caused as the result of the cyber incident. The LIV further recommends the DHA consider separating enforcement options from regulators, as while reporting would overcome regulatory fines, it does not preclude companies from class actions or private actions.

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?

The LIV encourages increased engagement from government in the regulatory space but queries the effectiveness of a health check program. LIV members report difficulty in creating a cyber support partnership that is financially feasible in the private sector. The LIV queries whether the results would be fed to authorised third party companies to help businesses to improve cyber risk.

²⁵ CNBC, *Senate Intel Chairman calls for mandatory reporting of hacks after Colonial Pipeline attack*, (Media Report, 12 May 2021). Available at <<https://www.cnbc.com/2021/05/12/mark-warner-colonial-pipeline-mandatory-reporting.html>>.

It would be beneficial to make grants available to SMEs where necessary, to implement any improvements to cyber security where the health check is not favourable.

As an alternative to the cyber security health check program, the LIV recommends a business education survey which outlines a business' obligations under a regulatory framework based on the type of data held. Businesses could answer questions related to their industry, the type of data collected and how information is stored, generating a guide highlighting what businesses should be wary of and any actions the business should undertake.

Chapter 10: Clear Legal Remedies for Consumers

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

The LIV acknowledges a need for a layered regulatory system with general safety nets and more specific provisions. Currently, the ACL's misleading and deceptive conduct provisions are currently untested for cyber security breaches and consumer rights. Without the support of the ACCC, there is a significant barrier to enforcement for individuals. To bring a claim, individuals must quantify losses, including financial loss, damage to reputation and losses for inability to access services, often without a clear understanding of the factors relevant to the cyber incident. The LIV is unaware of a situation where this has arisen in an Australian jurisdiction and notes that without a significant cyber breach which impacts a high number of businesses or individuals, there is unlikely to be high interest in strengthening regulation.

The LIV notes that the ACL does not cover the overarching considerations regarding cyber security, beyond an individual's right to a remedy. While there are provisions in the ACL which give certainty around consumer guarantees for digital products, cyber security risk is a broader issue beyond just consumer rights. The LIV maintains that cyber risk should be dealt with holistically through an overarching framework before it can be narrowed down to specific consumer protections or individual rights. LIV members have identified further ambiguity in the ACL, including in determining whether digital products are a good or a service or if new category is needed, and the issues with identifying the responsible business for recourse under the ACL. Clarity is needed in the current definitions in the ACL and how they apply to this category of product.

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

The LIV notes that proposed reforms contemplated under the Attorney-General Department's Privacy Act Review have not been made publicly available at the date of submission. The LIV anticipates that any reform to the Privacy Act should cover the gap between the ACL and consider negligence torts to ensure consumers are adequately protected online. Recent cyber security incidents highlight that a breach may cause loss without impacting people's personal information,²⁶ but it is very difficult to quantify subsequent losses. While the Privacy act covers personal data and consumer data and privacy itself, cyber security encompasses a whole range of circumstances, including personal financial loss, business loss, business continuity and disruption. The LIV suggests that alternative avenues to entice businesses could also be considered, including:

- Negligence claims;
- Breach of contract;
- Breach of warranties, including whether there should be a minimum warranty for software and devices for cyber updates
- misleading and deceptive conduct provisions;
- shareholder derivative lawsuits;
- breach of director duties;
- APRA rules; and
- ASIC rules, including producing notice of things that may affect the company value such as lawsuits.

The LIV notes that the ACL is intended to deal with specific breaches of consumer rights or business obligations, and generally requires a positive or affirmative action to establish a breach. The LIV considers that legal remedies for an individual may be better explored through a tort of invasion of privacy, within the context of a notifiable data breach relating to personal information. The current expectation under Australian Privacy Principle 11 is that an APP entity who holds

²⁶ Kari Paul, *Who's behind the Kaseya Ransomware attack – and why is it so dangerous?* (The Guardian, 7 July 2021). Available at < <https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers>>; William Turton and Jordan Robertson, *Microsoft Attack Blamed on China Morphs into Global Crisis* (Bloomberg, 7 March 2021) <<https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world>>; Reuters Staff, *SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft President* (Reuters, 15 February 2021) < <https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R>>.

personal information must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss; and from unauthorised access, modification or disclosure. This would entail implementing practices, procedures and systems to mitigate or prevent cyber risks and breaches.²⁷

The LIV recommends the introduction a statutory tort for serious invasions of privacy. Any privacy tort should not be based upon strict liability as that would be too onerous and broad, and 'inconsistent with [...] trends in tort law' that have favoured fault-based liability,²⁸ to impose absolute liability. Instead, the LIV recommends implementing a notice and remedy period for each breach that gives reasonable opportunities for the controller/processor to take action to mitigate the breach. Moreover, the LIV recommends that any tort should be limited to:

(i) Intrusion Upon Seclusion

Intrusion upon seclusion laws protect your right to privacy while you are in solitude or seclusion. This right extends to you or your private affairs. For example, it is an invasion of privacy for a neighbour to peek through your windows or take pictures of you in your home. Likewise, it is also an invasion of privacy to use electronic equipment to eavesdrop on a private conversation. The general elements of this tort are as follows:

- a) The defendant intruded into the plaintiff's private affairs, seclusion or solitude; and
- b) The intrusion would be objectionable to a reasonable person.

The defendant does not need to communicate the details of the intrusion to a third party; once the defendant has committed the intruding act (and the plaintiff proves the necessary elements), the defendant is liable for invasion of privacy.

(ii) Public Disclosure of 'Private Facts'

Public disclosure of private facts laws protects the right to keep the details of private life from becoming public information. For example, publicising facts about a person's health, sexual conduct, or financial troubles is likely an invasion of privacy. Generally, elements follow:

- a) The defendant publicised a matter regarding the private life of the plaintiff;
- b) The publicised matter would be highly offensive to a reasonable person; and

²⁷ Australian Government, Office of The Australian Information Commissioner, *The Australian Privacy Principles* (Canberra: Commonwealth of Australia, 2014). Available at <<https://www.oaic.gov.au/assets/privacy/australian-privacy-principles/the-australian-privacy-principles.pdf>>.

²⁸ Australian Law Reform Commission, 'Strict Liability' (15 July 2014) [7.72], [7.77] <<https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/7-fault/strict-liability/>>.

- c) It is not of legitimate concern to the public.

NB: To publicise a private matter, laws generally require that private information is disseminated in such a way that it is substantially certain to become public knowledge.

Cyber Insurance

The LIV is concerned that in circumstances where a product is put to market with certification that is compliant with the laws and a breach occurs, these losses would be passed on to the certification body. The LIV queries whether this outcome would result in the industry becoming uninsurable in practice due to the considerable risk. Losses resulting from a cyber security incident can be extensive and difficult to ascertain in advance. In effect, insurance companies may elect to avoid the cyber security industry entirely, including by refusing to cover directors' indemnity insurance or insurance for the organisation itself. Members report that insurance companies are taking a look at cyber policies and amount of liability and are pulling back their liability and in turn companies are discouraged because they cannot get any insurance to cover the liability. Additionally, insurance claims are insufficient where the damage is to the economy generally or where the organisation makes the loss and passes on the subsequent insurance rebate through increased costs to the consumer.

Moreover, insurance does not suffice where the damage is to the economy generally or where the organisation makes the loss. The LIV queries whether an insurance payout might entail a rebate being passed on to the customer. In the UK, the risk has been shifted to insurers and based on recent developments, the expectation is that an organisation would take reasonable steps to prevent issues, attacks and breaches.

The LIV recommends a limitation of liability scheme with monetary caps for businesses that report in a timely period. This would help companies access insurance with a known quantity for insurance companies to insure, despite inherent and unavoidable cyber insecurities within organisations. This scheme would be beneficial in addition to consumer protections and good faith obligations within the *Corporations Act*. It could be dependent on legislative disclosure obligations for directors when a company is the victim of a cyber-attack. To this end, the framework could be similar to the Notifiable Data Breach Framework, which would put forward a requirement to take reasonable steps to mitigate loss and enable information sharing about the breach to access the limited liability scheme.

A framework similar to the NDB framework, which places a requirement to take steps to mitigate, would enable consumer to reflect on that in terms of enforcement by the regulator or a private course of action. In these circumstances, where something has been hacked and has nothing to

do with personal information, accessing the benefit of the limitation liability scheme up to a certain amount would require the business to have been compliant.

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

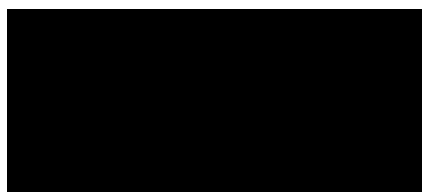
LIV members note that the legislation does not sufficiently cover the situations of the largest breaches that have occurred this year, including the SolarWinds, Colonial Pipeline and Microsoft hacks. These platforms and services are third party management systems for IT and due to the ransomware attack, people lost access to their computers and their systems, resulting in significant damage to the economy more broadly. These breaches did not necessarily impact upon personal information, although they have had wide ranging consequences for the economy. In the context of insurance, it is difficult to see who the insurer will payout in these circumstances.

Improved reporting from regulators for cyber risk and tracking metrics would encourage engagement in this area. Notifiable data breach statistics are released every quarter, but more reporting is necessary to determine if responses to these breaches by organisations are appropriate. The LIV also encourages a continued and greater focus on cyber education and security in professional education systems, particularly in relation to how companies are being targeted.

CONCLUSION

The LIV is grateful for the opportunity to provide feedback to the DHA's Consultation. Should you wish to discuss any of the above matters further, please contact Policy Officer, Andy Kuoch, or Paralegal, Sarah Cooney, at [REDACTED].

Yours sincerely,



Tania Wolff
President
Law Institute of Victoria