27 August 2021

Department of Home Affairs
Submitted via the online form at https://bit.ly/388xm9m

Submission - Strengthening Australia's cyber security regulations and incentives

This submission is in response to the Australian Government's consultation on options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy. Specifically, the *Strengthening Australia's cyber security regulations and incentives* discussion paper of 13 July 2021 (**Discussion Paper**).

We commend the Government for the work done to date and are grateful to participate in this open democratic process.

Our approach to this submission is one of general observation, applied in some detail to questions raised that fall within our area of expertise. Therefore, not all the questions have been answered, although we have retained them in sequence below for reasons of integrity and the connectedness of the subject matter.

General Observations

1. Founded under the executive branch of British government, Australia is unique in understanding rules and the sanctions that follow non-compliance with rules. This means that voluntary incentives will not easily succeed. Australians will do something if they are told to it in order to avoid punishment.

2. Sanctions are insufficient to effectively act as a motivator or deterrent. Consider the Luxembourg National Commission for Data Protection which made the decision on 16 July 2012 to fine Amazon €746 million (AU$ 1.2 billion) for violating the EU's *General Data Protection Regulation* (**GDPR**) rules on how to process personal data by comparison with Uber[1] which the OAIC found had interfered with the privacy of an estimated 1.2 million Australians but issued no fine, merely a determination that Uber improve its practices. It is cheaper not to comply with Australian law than to comply with it.

3. The regulatory landscape in Australia is complex. Like the United States, as a result of federalism, Australia has a 'patchwork' of laws, regulations, and other legislative instruments that apply in

[1] The Australian Information Commissioner and Privacy Commissioner Angelene Falk has determined that Uber Technologies, Inc. and Uber B.V. interfered with the privacy of an estimated 1.2 million Australians. Commissioner Falk has ordered the Uber companies to: (i) prepare, implement and maintain a data retention and destruction policy, information security program, and incident response plan that will ensure the companies comply with the Australian Privacy Principles, and (ii) appoint an independent expert to review and report on these policies and programs and their implementation, submit the reports to the OAIC, and make any necessary changes recommended in the reports. The full determination can be found at oaic.gov.au/privacy-determinations.

various jurisdictions and various industry sectors that have oversight by various responsible regulators. Sometimes, the ambit of responsibility is shared.[2] This complexity leads to inaction. Australians don't know what to do so tend to do nothing. Adopting a uniform approach to cyberlaw (any law dealing with information and information systems) which per definition involves Confidentiality, Integrity and Availability (**CIA**) will go a long way to lessening the level of regulatory complexity making it easier for Australians to know what to do.

4. In the international context, Australia was an early adopter of the model laws and international conventions that recognised and facilitated electronic commerce and communications,[3] yet it failed to adopt into domestic law two important provisions,[4] which has added to the legislative approach of sector, system and issue-specific legislation. This means that the advantages of technological neutrality and the over-arching interpretative ability of law to keep up with changes in how people use technology have been lost. The result is the constant need to make new law specific to new use cases and crimes.[5]

5. The limited scope of the Discussion Paper which focuses on the *Corporations Act 2001* (Cth), *Privacy Act 1988* (Cth) and *Competition and Consumer Act 2010* (Cth) does not do justice to the raft of available law that can be applied to address the issues at hand through a simple re-interpretation and application of these laws to cyberspace. A specific omission in our view is a consideration of the *Criminal Code Act 1995* (Cth). If the Government seeks to strengthen the cyber security of Australia's digital economy, it cannot do so without consideration of offences against the confidentiality, integrity and availability of computer data and systems. Amending fault elements from the definition of crimes, and introducing positive obligations to share information on cyber threats will go a long way to strengthen the cyber security of Australia by empowering Australians to better defend themselves.

6. Information sharing, specifically Cyber Threat Intelligence (**CTI**) sharing is fraught with risk as the acquisition of intelligence and its disclosure can lead to anything from breaching confidentiality, contractual obligations, the *Privacy Act*, *Anti-money Laundering, Counter-Terrorism Financing Act 2006* (Cth), *Telecommunications (Interception and Access) Act 1979* (Cth), and other laws even, causing Australia to breach Mutual Legal Assistance Treaties (**MLATs**) entered into with other countries.

   This complexity and the risk attached to it leads to inaction.

7. Far from adding further requirements, we are of the opinion that the Australian Government should undertake a full evaluation of existing requirements - and there are thousands - in State and

[2] For example, in making the CDR Rules, the ACCC consulted with the OAIC (Attorney General's Department / privacy), Treasury (& DSB / security and standards), and with the primary regulators in the banking sector, namely, ASIC and APRA.
[3] The UNCITRAL Model law on Electronic Commerce adopted in June 1996, was the first legislative text to adopt the fundamental principles of non-discrimination, technological neutrality and functional equivalence which are the founding elements of modern electronic law. The second UNCITRAL Model Law on Electronic Signatures adopted in July 2001 clarified use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures, facilitating the use of Public Key Infrastructure.
[4] Article *bis 5* which provides for the incorporation of information by reference, which was added to the Model Law in 1998, and the UNCITRAL Model Law on Electronic Signatures adopted in July 2001.
[5] For example the *Treasury Laws Amendment (2021 Measures No. 1) Bill 2021* - Schedule 1 amends the *Corporations Act 2001* to create new rules which will allow meetings to be held virtually, to allow documents relating to meetings to be provided and signed electronically and for minutes to be kept electronically.

Federal law, standards, codes of conduct etc., and rationalise these for application to cyberspace.[6] Australia needs to simplify and clarify existing laws, not to add new laws, principles, and codes. We should seek to empower Australian businesses by helping them understand what they can and must do.

8. We encourage a higher degree of international co-operation. See the response to question 3 and 4 below. This requires the participation of the Department of Foreign Affairs and Trade (**DFAT**).

9. Australia is a safe and wonderful country. Its people are good natured, supportive and community minded. Australia is unique in its culture of community and willingness to support all manner of causes. So, while the historic lack of any 'real and present danger' has let us to believe that we are safe has perhaps made us complacent, it also means that this cultural uniqueness will inevitably lead to people doing the right thing and agreeing to abide by codes of conduct.

Responses to Questions in the Discussion Paper

Chapter 2: Why should Government take action?

1. What are the factors preventing the adoption of cyber security best practice in Australia?
    a. Answered under General Observations: regulatory complexity, low level of sanctions and Australian culture.

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

    In both cases, Government action is required to ensure both companies and consumers can make informed decisions.

    a. Negative externalities
    Negative externalities create a need for government action on cybersecurity as not all Australian businesses understand how their decisions on cyber security affect their own companies let alone the companies within the supply chain. At the same time, under corporations' law, they are required to manage risk with due care, skill and diligence. Understanding that these duties encompass seeking out knowledge and understanding of cyber security issues within the company and its supply chain and how to respond to them should be made clearer to companies through education and clarification on these laws. See further comments in 5 below.

    b. Information asymmetries
    With regards to information asymmetries, Government action is required to assist consumers to make informed decisions on cyber security risks, and to assist companies to provide clear and verified information on the security of products and services provided to consumers. Clarifying (rather that amending) existing laws such as the *Competition and Consumer Act* will provide increase certainty in relation to legal consequences.

[6] For example, what does "to remove …" from computers and networks a person who is committing criminal trespass mean? See - https://www.ictlegalconsulting.com/2021/07/23/does-self-defence-apply-in-cyberspace/?lang=en.

Chapter 3: The current regulatory framework

3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?
    a. Answered under General Observations.

4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?
    a. Answered under General Observations no. 7. Specifically, (i) undertake a body of research to establish what current Australian law applies to cyberspace, (ii) work with UNCITRAL and other international organisations to develop a new model law on the commonalities in national legal systems to establish what constitutes acceptable behaviour in cyberspace, (iii) negotiate and enter into a new, updated Cybercrime Convention, subsequent to the Convention on Cybercrime Budapest, 23.XI.2001. European Treaty Series - No. 185 (**Cybercrime Convention**). Retain technological neutrality.[7]
    b. Australia has adopted the requirements of the Cybercrime Convention into law. (*Crimes Act 2001* and the *Criminal Code Act*, specifically Part 10.7 - Computer offences). See also Chapter 6 on drafting:[8]

> *"The Committee was told that computer offences need to be drafted in technology neutral language to minimise repeated amendment of the Criminal Code. According to AGD, the Part 10.7 offences are drafted so as to apply as technology evolves: For example, the term "computer" was not defined to ensure the computer offences will encompass new developments in technology, for example, mobile phones that allow access to the Internet."*

In our view there is sufficient detail to prosecute – even for something like 'ransomware' already.[9] Australia however needs clarity on how the law will apply. This is an issue of interpretation of existing law, not a requirement to draft a new law on ransomware. This point supports using what we have rather than adding further layers of complexity.

Note 1: International conventions like the Cybercrime Convention are a source of national law. So, a new treaty is the most efficient way for countries to agree on new norms of behaviour. This is how to raise the bar and block threats at scale to protect Australia's digital economy.

---

[7] Ransomware already contravenes provisions in the *Criminal Code Act 1995* (Cth).

[8] https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms/cybercrime/report.htm

[9] There are currently 66 parties to the Budapest Convention. This means that 66 countries agreed to adopt (the same) cybercrimes into their national legal systems. Chapter II. Sec. 1. Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems. Art. 4 provides:
"Each party (66 countries) shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right."
Similarly, Art 6 – Misuse of devices, provides:
"… the production, sale, procurement for use, import, distribution or otherwise making available of: … a device, including a software program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Art. 2 through 5;" (illegal access, illegal interception, data interference, system interference).
Surely, this renders ransomware a criminal offence. We do not need a new law that says, "ransomware is an offence"
Clarification on the application of electronic law will solve problems at scale.

Note 2: The suggestions made under question 4 are different from what Australia is doing at the United Nations with the UN Cyber GGE. This work relates to relationships between sovereign entities and has reference to the work done at Tallinn 1.0 and 2.0.[10] Notably, expert input has been invited for Tallinn 3.0, and Australia has long been a participant. What we recommend is that Tallinn 3.0 considers also the applicability of national law to cyberspace. The earlier Tallinn work determined that international (public) law applies to cyberspace.

Chapter 4: Governance standards for large businesses

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?
   a. Hold the directors and officers of an organisations accountable. Sections 180 - 183 of the *Corporations Act* largely codify the common law on directors' duties. This Act does not need amendment to include 'cyber' provisions.

      Standards (of behaviour, not technology) play an important part here, because they assist in establishing what reasonable behaviour is. Australian and international standards (on technology and its use) also demonstrate compliance with law through the production of artefacts etc.

      Directors must exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise if he or she were a director in the company's circumstances and had the same responsibilities of that director.

      Current company director liabilities: When company directors breach the law, they can be personally liable. Apart from personal liability arising from criminal and other offences, directors can also become personally liable as a result of breaching director duties that caused the company to suffer loss.

      So, failure to identify a risk such as ransomware (due diligence), and failure to address the risk of ransomware (due care) can already render a company director liable under the *Corporations Act.*

      A director who fails to perform their duties, may:[11]

      - Have contravened a civil penalty provision such as the care and diligence requirements under section 181(1) of the *Corporations Act* (see section 1317E). The court may order the director to pay to the Commonwealth up to $200,000).
      - Be personally liable to compensate the company or others for any loss or damage they suffer.
      - Be prohibited from managing a company in future.

      There is sufficient protection for directors and officers under the business judgment rule under Section 180(2) of the *Corporations Act* in relation to an alleged breach of the duty to act with care and diligence.

[10] Michael Schmitt et al, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017, 2nd ed, Cambridge University Press).
[11] Be guilty of a criminal offence with a penalty of up to a maximum of $200,000, or imprisonment for up to five years, or both.

6. What cyber security support, if any, should be provided to directors of small and medium companies?
    a. Not answered.

7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?
    a. Yes, education and awareness are key for informed decision-making. Managing risk is an important element of corporate governance. There is little difference between managing risk of insolvency and managing cyber risk other than being required to understand or employ a different set of skills. Therefore, education and awareness should be made easily accessible for both SMEs and sole traders as well as for executives of larger entities. The Government can assist with this by implementing mandated minimum requirements for example, providing basic training and awareness as a compulsory aspect of applying for business registrations/renewals for SMEs and sole traders.

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?
    a. No. Firstly, this is an example of overlapping responsibility between the Attorney General's Portfolio (privacy compliance and Australian Privacy Principle 11 (**APP 11**) on security of personal information), and the Department of Treasury (privacy safeguards for CDR Data). Does the question imply yet another code of conduct under the *Competition and Consumer Act*? Secondly, this adds to complexity. Thirdly, codes are ineffectual 'tick-box' mechanisms that tend to lack auditability. See General Observations no. 1.
        - There are already excellent international standards providing for privacy. For example:
            - ISO/IEC 29100:2011 – Information technology — Security techniques — Privacy framework;[12] and
            - ISO/IEC 27018:2019 Information Technology — Security Techniques — Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors.

        Standards such as these effectively implement law. Australian organisations are largely unaware of these or similar standards. We do not support adding to existing complexity, rather we support the use of what already exists. These kinds of standards are in any event based on 'Statements of Applicability' (**SOA**) or 'Targets of Evaluation' (**TOE**), so are equivalent to the APRA CPS 234 approach that security is treated as commensurate to the business (not a one size fits all approach).

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

[12] ISO/IEC 29100:2011 provides a privacy framework which: specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology. ISO/IEC 29100:2011 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

a. We do not support a code of conduct. We do support that adoption of, and alignment with, standards like ISO, NIST etc. The promotion of a maturity model and Plan-Do-Check-Act approach would assist businesses grow in cyber security maturity.

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?
    a. We do not support a code. The *Privacy Act* provides for the protection of personal information (**PI**). Any entity that is subject to the *Privacy Act* must comply with the Act. APP 11 addresses security. Relevant standards support privacy and security.

Chapter 6: Standards for smart devices – Not answered

11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?
12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for 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?
13. [For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?
14. What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?
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?

Chapter 7: Labelling for smart devices - Not answered.

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? If so, which existing labelling scheme should Australia seek to follow?
19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?
20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?
21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

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?
    a. Further to our General Observations above, we do not believe voluntary incentives are likely to succeed. Drawing on our comments in responses 2, 5 and 7, responsible disclosure comes under the risk management responsibilities of company directors. Disclosing vulnerabilities is a significant part of managing their cyber risk internally and within their supply chains. As such, awareness and education on responsible disclosure is important for company directors.

Chapter 9: Health checks for small businesses - Not answered.

23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?
24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?
25. If there is anything else we should consider in the design of a health check program?

Chapter 10: Clear legal remedies for consumers - Not answered.

26. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?
27. Are the reforms already being considered to protect consumers online through the *Privacy Act 1988* and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

Chapter 11: Other issues - Not answered.

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

Authors

Helaine Leggat Attorney at Law, CISSP, CISM, CIPP, CIPT, GAICD

Managing Partner ICTLC Australia

E-mail: [redacted] | Twitter: [redacted]

Mobile: [redacted] | Phone [redacted]

ICTLC Australia PTY LTD | ABN: 86 163 763 522 | Address: Level 11, 456 Lonsdale Street – Melbourne VIC 3000 | Web: ictlegalconsulting.com/ictlc-australia | E-mail: info.aus@ictlegalconsulting.com | Twitter: @ictlc

Offices in Milan, Rome, Bologna, Amsterdam, Madrid, Helsinki and Melbourne. Partner law firms in 33 countries: Albania, Austria, Belgium, Brazil, Bulgaria, Canada, China, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Japan, Luxembourg, North Macedonia, Mexico, Moldova, New Zealand, Nigeria, Poland, Portugal, Romania, Russia, Singapore, Slovakia, South Africa, Sweden, Switzerland, Turkey, United Kingdom and United States.

Chloe Hatzis

Consultant ICTLC Australia

E-mail: [redacted] | Twitter: [redacted]

Mobile: [redacted] | Phone [redacted]

ICTLC **Australia** PTY LTD | ABN: 86 163 763 522 | Address: Level 11, 456 Lonsdale Street - Melbourne VIC 3000 | Web: ictlegalconsulting.com/ictlc-australia | E-mail: info.aus@ictlegalconsulting.com | Twitter: @ictlc

Offices in Milan, Rome, Bologna, Amsterdam, Madrid, Helsinki and Melbourne. Partner law firms in 33 countries: Albania, Austria, Belgium, Brazil, Bulgaria, Canada, China, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Japan, Luxembourg, North Macedonia, Mexico, Moldova, New Zealand, Nigeria, Poland, Portugal, Romania, Russia, Singapore, Slovakia, South Africa, Sweden, Switzerland, Turkey, United Kingdom and United States.