THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Submission on the Australian Government's *Strengthening Australia's cyber security regulations and incentives* Discussion Paper

6 September 2021

Department of Home Affairs

Contact: **Simon Bruck**
President, NSW Young Lawyers

Ashleigh Fehrenbach
Chair, NSW Young Lawyers Communications, Entertainment and Technology Committee

Contributors: Avnoor Guron, Ashley Howard, Esha Kumar, Ashleigh Snowden, Rebecca Karpin (Editor), Anagha Bidkar (Editor) and Sheenae LeCornu (Editor)

Managing Editor: Taylah Spirovski

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
T +61 2 9926 0182
F +61 2 9926 0282
E ylgeneral@lawsociety.com.au
W www.younglawyers.com.au

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers Communications, Entertainment and Technology Committee (**Committee**) makes the following submission in response to the Discussion Paper on Strengthening Australia's cyber security regulations and incentives (**Discussion Paper**).

NSW Young Lawyers

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The Committee aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, confidential information and privacy, entertainment, and the media. As innovation inevitably challenges custom, the Committee promotes forward thinking, particularly with respect to the shape of the law and the legal profession.

Summary of Recommendations

1. **Question 5:** The Committee submits that the best approach to strengthening corporate governance of cybersecurity risk is a voluntary governance standard, which has been co-designed by the industry and structured around the ASIC's best practices for cyber resilience.
2. **Question 8:** The Committee submits that a cyber-security code under the *Privacy Act 1988* (Cth) would be an effective way to promote the uptake of cybersecurity standards in Australia, provided the OAIC is given adequate resources to administer the code effectively.
3. **Question 16:** The Committee submits that the best approach to encouraging consumers to purchase secure smart devices is a labelling scheme and mandatory standards which impose a minimum security standard.
4. **Question 17:** The Committee submits that a combination of a labelling scheme and mandatory standards for smart devices would be a practical and effective approach of ensuring consumer awareness and producers meet minimum security standards.
5. **Question 18:** The Committee submits it is likely that sufficient industry uptake of a voluntary label for smart devices will occur based on research about the voluntary Health Star Rating. The effectiveness of the voluntary labelling is dependent upon consumers having a sufficient range of products to compare the security ratings.
6. **Question 19:** The Committee supports the introduction of security expiry date labels, however, submits that an expiry date scheme will only be effective for consumers if accompanied by minimum cyber-security standards that ensure such labels are meaningful.
7. **Question 20:** The Committee submits that a mandatory labelling scheme should not extend to mobile phones as the mobile phone market is inherently different to other smart devices, such that complications would arise if a blanket labelling scheme were introduced.
8. **Question 21:** The Committee recommends that smart devices are labelled physically, but digital labelling should also be allowed in particular circumstances which are consistent with the existing electronics labelling criteria.

Part 1 — Set clear minimum expectations

4. Governance standards for large businesses

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

1. The Committee submits that the best approach to strengthening corporate governance of cybersecurity risk is a voluntary governance standard (Option 1 in the Discussion Paper), which has been co-designed by the industry and structured around the Australian Security Investment Commission's (**ASIC**) best practices for cyber resilience.
2. A voluntary governance standard would support the current developments around cybersecurity in different areas of law. For example, it is likely that director's duties regarding care and diligence under s 180 of the *Corporations Act 2001* (Cth) will evolve and include cybersecurity risks.[1]
3. ASIC has recently engaged in legal proceedings against RI Advice Group Pty Ltd.[2] The regulatory body successfully argued that RI Advice, in failing to implement 'policies, plans, procedures, strategies, standards, guidelines, frameworks systems, resources and controls, which were reasonably appropriate to adequately manage risk in respect of cyber-security and cyber resilience'[3] that RI Advice failed to uphold a range of its obligations under Part 7.6, Division 3 of the *Corporations Act 2001* (Cth).
4. Although this case relied on provisions directed at financial services licensees, it sets a precedent for other organisations governed by the *Corporations Act 2001* (Cth). It sets significant precedent as the first case brought by ASIC regarding cybersecurity risk.[4]
5. A voluntary standard would assist businesses and the court in determining what reasonable steps should be taken regarding corporate governance of cybersecurity risk. This would be helpful for corporations to anticipate and prevent future litigation from various interested parties including regulatory bodies, shareholders and consumers who may engage in class action suits.[5]

---

[1] James North and Richard Pascoe, 'Cyber security and resilience – it's all about governance' (2016) 3 (April) *Governance Directions* 146, 147.
[2] *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (No 2)* [2021] FCA 877.
[3] Australian Securities and Investments Commission, 'Originating process', Submission in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd*, VID556/2020, 21 August 2020, 2-3.
[4] Australian Government, *Strengthening Australia's cyber security regulations and incentives* (Discussion Paper, Department of Home Affairs, 13 July 2021) 13.
[5] James North and Richard Pascoe, 'Cyber security and resilience – it's all about governance' (2016) 3 (April) Governance Directions 146, 147.

6. A voluntary standard co-designed by the industry is in line with the approach taken by other jurisdictions, such as Canada, Japan, and Israel.[6] The flexibility of the voluntary standard is also preferable to a strict mandatory system, which may discourage international corporations from operating within Australia.[7]
7. However, the implementation of a voluntary standard also comes with the risk of businesses not adopting it. A case study of compliance with a voluntary cyber-security standard amongst the petrochemical industry in the Port of Rotterdam found that a high rate of the firms surveyed had cybersecurity systems that were below standard.[8]
8. The study found that one of the main barriers to compliance was the lack of incentive. Businesses may not be willing or capable to invest in the development of cybersecurity protocols due to other economic factors. [9]
9. A voluntary governance standard which is co-designed by the industry may mitigate this risk to some extent. The voluntary governance standard would ensure that businesses become aware of the importance of cybersecurity measures whilst also allowing smaller, less resource-rich entities to develop cyber resilience practices at their own pace. Additionally, businesses may be motivated to participate in a voluntary standard to highlight that their directors understand the importance of cybersecurity measures, and to decrease the chances of litigation from various stakeholders.
10. In the Committee's view, a voluntary standard co-designed by industry is the best approach of strengthening corporate governance of cybersecurity risk when weighing the costs and benefits of such a measure to the relevant stakeholders.

---

[6] Regner Sabillon, Victor Cavaller & Jeimy Cano, 'National Cyber Security Strategies: Global Trends in Cyberspace' (2016) 5(5) *International Journal of Computer Science and Software Engineering* 67.
[7] Australian Government, *Strengthening Australia's cyber security regulations and incentives* (Discussion Paper, Department of Home Affairs, 13 July 2021) 22.
[8] Judith van Erp, 'New governance of cyber security: a case study of the petrochemical industry in the Port of Rotterdam' (2017) 68, 89.
[9] Ibid, 90.

5. Minimum standards for personal information

Question 8: Would a cyber-security code under the Privacy Act be an effective way to promote the uptake of cybersecurity standards in Australia? If not, what other approach could be taken?

1. The Committee submits that a cyber-security code under *Privacy Act 1988* (Cth) (**Privacy Act**) would be an effective way to promote the uptake of cybersecurity standards in Australia.
2. Currently, cyber-security is dealt with in the Privacy Act through Australian Privacy Principle 11 — security of personal information.[10] This principle requires entities covered by the Privacy Act to take steps, which are reasonable in the circumstances to protect personal information from loss, misuse, and unauthorised access, modification, or disclosure.[11]
3. Although this Principle allows for flexibility amongst different organisations with different needs and levels of personal information, this ambiguity may discourage entities from taking up cyber-security measures as they are not provided adequate guidance. A report from the Australian Computer Society noted that 'in a survey of close to 4,000 company directors in Australia, only half reported to be cyber literate.'[12] This is a concerning figure as decisions around the implementation of risk management strategies, and allocation of funding for such endeavours are made at the executive level.
4. A good example of a way in which cyber-security standards have been made more accessible is the Department of Home Affairs Internet of Things Code.[13] This code provides a set of 13 principles with in-depth descriptions and examples to assist the user. The code also directs users to other resources which may assist them, such as the Australian Government Information Security Manual.[14]
5. The Committee submits that a similar approach to a cyber-security code under the Privacy Act would encourage the adoption of adequate and consistent security measures for personal information.
6. However, the Committee submits that the Office of the Australian Information Commissioner (**OAIC**) may be underfunded and therefore ill-equipped to take on additional functions.[15]

---

[10] *Privacy Act 1988* (Cth) sch 1 cl 11.
[11] Ibid.
[12] Australian Computer Society, *Cyber security – Threats, Challenges and Opportunities* (Report, November 2016) 55.
[13] Australian Government, *Code of Practice – Securing the Internet of Things for consumers* (Report, 3 September 2020)
[14] Ibid, 5.
[15] Marcus Smith and Gregor Urbas, *Technology Law: Australian and International Perspectives* (Cambridge University Press, 2021) 47-48.

7. The OAIC 'failed to achieve seven of its eight performance goals for the 2019-20 financial year' and is experiencing a significant backlog in areas it oversees.[16] The oversight of an additional code for OAIC to administer may add to this issue. Additionally, the cost of implementing OAIC oversight may be more than the 'moderate' level which has currently been assessed under the Department of Home Affairs' evaluation.[17]
8. In the Committee's view, it is highly likely that a cyber-security code under the Privacy Act would be an effective way to promote the uptake of cybersecurity standards in Australia, provided the OAIC is given adequate resources to administer the code effectively.

Part 2 - Increasing Transparency and Disclosure

7. Labelling for smart devices

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

1. The Committee submits that the best approach to encouraging consumers to purchase secure smart devices is a labelling scheme (combining both Options 1 and 2) in addition to mandatory standards so as to ensure that any "expiry date" is in fact meaningful. The Committee's reasoning for this conclusion is elaborated on more fulsomely in the response to the further questions under this Part.

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

1. A combination of labelling and standards for smart devices would be a practical and effective approach which is supported by analogy in considering the benefits of the Energy Rating Label and the Health Star Rating discussed below.
2. The practical nature of labelling schemes can be seen by the Energy Rating Label,[18] which compares energy efficiency and the cost of consumption. Consumers are able to understand and choose between a lower cost product that will accumulate higher costs over time and vice versa.

---

[16] Denham Sadler, 'Privacy office is still 'severely underfunded', *InnovationAus* (Webpage, 13 October 2020) < https://www.innovationaus.com/privacy-office-is-still-severely-underfunded/>.
[17] Australian Government, *Strengthening Australia's cyber security regulations and incentives* (Discussion Paper, Department of Home Affairs, 13 July 2021) 28.
[18] Energy Rating, *The Energy Rating Label* <https://www.energyrating.gov.au/label>.

3. Similarly, the voluntary Health Star Rating (**HSR**)[19] allows consumers to compare the nutritional profile of other foods in the same category. A review in 2019[20] provided that Australian consumers are willing to pay more for a product that displays the HSR. In Australia, 70% of consumers recalled purchasing a product displaying a HSR, with almost two-thirds of these consumers stating it influenced their purchasing decision.
4. The same study shows a clear link between HSRs and the reformation of products. An analysis of 929 products with HSRs in New Zealand showed that 79% of these products were reformulated to change at least one key ingredient. Manufacturers are also choosing to display HSR on products that score more highly.
5. These studies demonstrate the effectiveness of labelling, not only in directing consumers towards healthier and more energy efficient products, but also in creating a competitive market that drives manufacturers to create better products.
6. A star rating system alone may not be the most effective option when encouraging consumers to purchase secure smart devices. However, the combination of a label with a minimum security standard and expiration date would ensure that all products meet minimum security standards including lower rated products which will still be available for purchase by consumers.

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

1. Based on the research surrounding voluntary HSRs, it is likely that sufficient industry uptake of a voluntary label for smart devices will occur.
2. The Committee accepts that the time required to achieve sufficient uptake would be much longer than if a mandatory labelling scheme were to be implemented. While that may hinder the effectiveness of such a scheme in the short-to-medium term, the Committee considers that to be justifiable to minimise the disruption to business and to consumer choice while the scheme is in its adoption phase.

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

1. The Committee supports the introduction of security expiry date labels, however, submits that efficacy would be significantly undermined for a significant portion of products if not accompanied by minimum cyber-security standards that ensure such labels are meaningful.

---

[19] Health Star Rating System, *About Health Star Ratings* <http://www.healthstarrating.gov.au/internet/healthstarrating/publishing.nsf/content/home>.

[20] MP Consulting, *Health Star Rating System Five Year Review Report* (February 2019) <http://www.healthstarrating.gov.au/internet/healthstarrating/publishing.nsf/Content/D1562AA78A574853CA2581BD00828751/$File/Health-Star-Rating-System-Five-Year-Review-Draft-Report.pdf>.

2. Security flaws in smart products cannot be completely prevented and even well-designed systems may need to be continuously repaired.[21] Without a minimum standard to support the expiry label, there is the risk that a product could be released without all the necessary security updates, or that what updates are released over time are insufficient to address vulnerabilities that become known.[22] A minimum standard would ensure that products on the market are being released to a uniform safety standard for consumer use.
3. Given the broad range smart devices which are available at relatively affordable prices, including smart water bottles, smart fridge cams and smart egg trays, it is unlikely that consumers will carefully consider security expiry dates for each and every smart device with which they interact regularly, and lower cost, and single function devices are likely to suffer most from this neglect. These lower cost devices may in turn result in the creation of a risk gap.[23] Therefore, a combination of mandatory standards and the labelling scheme will be the most effective approach to reduce the baseline risk across the entirety of a consumer's network of devices, whereas the benefits of labelling alone are likely to be of only marginal benefit in multi-device households.

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

1. The Committee submits that a mandatory labelling scheme should not extend to mobile phones as the mobile phone market is inherently different to other smart devices, such that complications would arise if a blanket labelling scheme were introduced.
2. In Australia, the average mobile phone user replaces their smart phone every 3 years. Technological advancements result in phones no longer being fit for purpose and becoming obsolete. A security expiry date on mobile phones will not yield the same results as other smart devices that are part of less dynamic markets where the device is intended to be used for much longer.
3. Further, unlike simpler smart devices, mobile phones almost invariably operate based upon software created by numerous providers. That is, the phone may have a base operating system made by one company (e.g. Android), modifications to that operating system made by the particular phone manufacturer, and then consumer selected applications created by many companies.

---

[21] Philipp Morgner et al, *Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products* (Research Paper, Department of Computer Science, School of Business, Economics and Society, Friedrich-Alexander-Universitat Erlangen-Nurnberg, 26 June 2019).
[22] Ibid.
[23] Andrew Laughlin, 'More than 100,000 wireless security cameras in the UK at risk of being hacked, *Which?* (Web Page, 12 June 2020) <https://www.which.co.uk/news/2020/06/more-than-100000-wireless-security-cameras-in-the-uk-at-risk-of-being-hacked/>.

4. As an example of why this is a relevant issue, a software library created by Google suffered an error during 2020 which was eventually patched.[24] However, until each individual application in the library made their own updates, the particular application was still vulnerable.[25] A security label will not be effective for smart mobile devices unless it details all of the parties involved at an operating system level and all of the companies selling mobile devices that use that system.[26]
5. As such, it would be almost impossible for a manufacturer to guarantee a particular cyber-security "expiry date" for a mobile phone. That difficulty would invite manufacturers to specify unrealistically short "expiry dates" with a goal of minimising liability, even if significantly less than the time that updates would actually be provided, adding further pressure to device obsolescence as discussed above. Such an outcome would not assist consumers.

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

1. The Committee recommends that smart devices are labelled physically, but digital labelling should also be allowed in certain instances. This can be done by following the existing labelling criteria for electronics.
2. The Australian Communications and Media Authority sets out labelling rules for telecommunications equipment and radio-communications equipment, breaches of which can incur large fines.[27] A labelling scheme for smart devices that incorporates the following rules would be beneficial:
    i. A label on the surface of the product must be a permanent feature of the product and not likely to fall off, be washed off, or fade;
    ii. If a product has a built-in display, it may be shown electronically rather than on the surface; and
    iii. If it is not practical to apply to the surface of the product then the label can be attached to product packaging.
3. If a star rating label system were implemented, it would need to be a physical label so consumers can look to the rating at the time of purchase as a means to quickly compare to other products.

---

[24] Zak Doffman, If These Apps Are Installed On Your Phone, You Can 'Easily' Be Hacked, *Forbes* (Web Page, 3 December 2020) <https://www.forbes.com/sites/zakdoffman/2020/12/03/if-these-apps-are-on-your-samsung-huawei-xiaomi-or-google-phone-you-can-be-hacked/?sh=37f0b5c33d8c>.
[25] Ibid.
[26] Ibid.
[27] 'Step 5: label your product', *Australian Communications and Media Authority* (Web Page, 13 December 2019) < https://www.acma.gov.au/step-5-label-your-product >.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Concluding Comments

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions, please contact the undersigned at your convenience.

Contact:

[redacted]

Simon Bruck

President

NSW Young Lawyers

Email: [redacted]

Alternate Contact:

[redacted]

Ashleigh Fehrenbach

Chair

NSW Young Lawyers Communications, Entertainment and Technology Committee

Email: [redacted]