Cyber Security Policy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600

30th October 2019

Australia's 2020 Cyber Security Strategy

Submission to the Department of Home Affairs

Emily Watson, Genna Churches, Lyria Bennett Moses, Monika Zalnieriute
Allens Hub for Technology, Law and Innovation
UNSW Faculty of Law, Sydney, Australia

About us

We work with the Allens Hub for Technology, Law and Innovation ('the Allens Hub') — an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this submission

This submission seeks to respond to the questions raised in the Department of Home Affair's call for views discussion paper regarding Australia's 2020 Cyber Security Strategy. As scholars working at the intersection of law and technology, we are delighted to participate in the consultation process. We have limited our response to those matters where our research may be relevant, namely, questions 2, 10 and 22. In making this submission we hope to highlight some issues raised in our research and discussed in the consultation session attended by Genna Churches. We are grateful for the opportunity to present our views and hope this submission will assist in informing the Government's approach to developing Australia's 2020 Cyber Security Strategy. The opinions expressed in this submission are the views of the authors, and do not reflect the institutional views or positions of Allens or UNSW Law.

Summary

In relation to the discussion paper on the 2020 Cyber Security Strategy, we make the following points:

1. The government has an obligation under the International Human Rights Legal Framework to ensure adequate education regarding cyber security literacy for all members of society.
2. Educational outreach should include but not be limited to the goal of growing the number of skilled professionals - the aim should be to increase cyberliteracy and promote a cultural shift in attitudes towards safe technology use.
3. Part of this educational focus should be developing critical consumers who understand the risks associated with ICT use, so that they can make informed decisions.
4. The regulatory environment for cyber security in Australia encompasses a range of laws and initiatives, which need to be understood and defined before assessment of their appropriateness can be conducted.
5. In light of overseas developments, the government should review the *Privacy Act 1988* (Cth).

Importance of Cyber Security Literacy

Question 2: Who is responsible for managing cyber risks in the economy?

The discussion paper acknowledges that the current balance of responsibility for managing cyber security risks falls heavily on end-users. The Australian government has thus far prioritised a "carrots to sticks" approach to cyber security related dealings with the private sector, which often results in individuals or small businesses bearing the brunt of the risk and consequences of cyber security risks.[1] The appropriateness of this balance is a key question for the 2020 Strategy which we do not attempt to consider in this submission as it falls outside the scope of our research.

Rather, we make the point that any system which places a large margin of risk on (generally under resourced) end-users must ensure broad education as a tool for managing risk. Education to increase Australian's cyber security literacy was a key goal of the 2016 Cyber Security Strategy and was consistently raised as an important goal in the roundtable discussion held on 18 September 2019. Although there appears to be consensus that a greater focus on education is needed, there are various opinions on the best focus and/or aim of educational outreach.

Government responsibility to educate

The International Human Rights legal framework stipulates that Australian government has a responsibility to ensure adequate education regarding cyber security literacy for all members of society. In particular, the International Covenant on Economic, Social and Cultural Rights which provides that education 'shall enable all persons to participate effectively in a free society'.[2] This education should reflect the fact that citizens participate in a society based on Internet connectivity and networked systems.

Access to government services has become increasingly digitised. If citizens are expected to utilise ICTs to access government services, then there may be a corresponding responsibility on the part of the government to educate and ensure that citizens can use said technology safely when accessing those services. This is compounded by the reality that the people requiring government services are often experiencing circumstances of disadvantage. A failure to educate on how to stay safe online could lead to further harms for those individuals.

---

1 Liam Nevil, 'Cyber Security Governance in Australia' in 14 Christian Leuprecht and Stephanie MacLellan (ed) *Governing Cyber Security in Canada, Australia and the United States* (Centre for International Governance Innovation, 2018) 14.

2 International Covenant on Economic, Social and Cultural Rights, opened for signature 16 December 1966, 993 UNTS 3 (entered into force 3 January 1976) Article 13.

Education for young students

Effective education at a primary and secondary level may prove the best forum for effecting long-term change. Early education can help influence and define long-term individual user habits. It can also influence business practices as students go on to work in various sectors which may lack dedicated ICT professionals. Although today's young Australians have grown up in a world which is saturated with digital technologies, the concept of a 'digital native' who has particular cognitive skills to effectively use ICT by virtue of their immersed upbringing is questionable.[3] Thus, schools must continue to provide students with cybersecurity education.

The Australian curriculum currently addresses ICT education through its Digital Technologies learning area and the general ICT capability. The Digital Technology learning area is a compulsory subject from Foundations to year eight which aims to develop student's 'knowledge, understandings and skills of the underlying concepts of information systems, data and computer science,' to enable them to design and create digital solutions.[4] The ICT capability is not a formal subject, but one of seven general capabilities identified in the Australian curriculum. General capabilities are taught across all curriculum areas and 'act as "lenses" through which teachers look at content' when planning lessons.[5] The Australian Curriculum, Assessment and Reporting Authority ('ACARA') describes the aim of the ICT capability as ensuring students 'learn to use ICT effectively and appropriately' and includes cybersecurity considerations such as 'limiting the risks to themselves and others in a digital environment'.[6] In short, ICT capabilities focus on being able to use ICT appropriately and effectively, while Digital Technologies focuses on understanding how ICT's operate to enable creation of ICTs.

It is important to recognise this distinction between the expertise needed to design an ICT system and the knowledge needed to use such technology well.[7] Digital Technologies as a subject provides a foundation for further ICT study and may promote the future development of skilled ICT professionals (a key concern of the discussion paper). However, most citizens will not require the level of technical knowledge necessary to understand the design of complex technologies. Everyone should have the knowledge necessary to use ICT safely. Thus, it is important to ensure teachers have adequate resources and training to incorporate the ICT capability focus, including cybersecurity into their subjects. Additionally, focus should be

---

3 Paul Kirschner and Pedro De Bruyckere, 'The myths of the digital native and the multitasker' (2017) 67 *Teaching and Teacher Education* 135.

4 'What's the difference between ICT Capability and Digital Technologies' *Digital Technologies Hub* (Infographic) <https://www.digitaltechnologieshub.edu.au/docs/default-source/resource-bank/dthub_infographic-a3-inhouse.pdf>.

5 Misty Adoniou, 'What if we had asked teachers to do the curriculum review?' (16 October 2014) *The Conversation* <http://theconversation.com/what-if-we-had-asked-teachers-to-do-the-curriculum-review-33027>.

6 Australian Curriculum, Assessment and Reporting Authority, 'Information and Communication Technology (ICT) Capability' *Australia Curriculum* (Webpage) <https://www.australiancurriculum.edu.au/f-10-curriculum/general-capabilities/information-and-communication-technology-ict-capability/>.

7 In the context of AI and education see, Lyria Bennet-Moses, 'Helping future citizens navigate an automated, datafied world' (Occasional Paper Series, Education: Future Frontiers, NSW Department of Education, April 2019) 7.

placed on teaching not just safe but "healthy" technology use to help students 'develop technical, critical and cultural literacies with technology.'[8]

Understanding the regulatory environment

Question 10: Is the regulatory environment for cyber security appropriate?

One challenge that Australia faces in *evaluating* the regulatory environment for cyber security is first *understanding* that environment. Unlike some other jurisdictions, such as Germany, Australia does not have specific legislation for cyber security. However, a number of laws provide incentives for good cyber security practices, disincentives for criminal or poor practices and/or require minimum standards be met. These include corporate law, criminal law, consumer law, privacy law, security laws, as well as common law in the areas of contract, negligence, property, torts and administration. Together with partners at the University of Melbourne and elsewhere, and through the Cyber Security CRC,[9] we are currently researching the threads that, together, comprise Australia's legal framework for cyber security. We believe this work is a crucial preliminary step to answering the question about the appropriateness of the regulatory environment.

In addition to substantive laws, the strategy's interaction with other government initiatives or strategies – including the development of international standards, the work of ASIC and the ASX with corporations, the ACCC's digital platforms enquiry and the Artificial Intelligence Ethics Framework – needs to be considered. The 2020 Cyber Security Strategy will need to integrate with all of these initiatives to be effective. Failure to consider these interactions may result in overlap and confusion, and further contribute to the piecemeal approach to the appropriate legal framework for cyber security in Australia.[10]

Question 22: To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

We agree that a lack of 'cyber awareness' drives poor consumer choices. Without cyber awareness education, consumers will be less well placed to make safe decisions about their actions online or decisions to purchase particular products (such as internet-connected devices).

---

8 John Buchanan et al, 'Preparing for the best and worst of times' (Analytical Report, Sydney Policy Lab, University of Sydney and Education: Future Frontiers, NSW Department of Education, January 2018) 41.

9 The Cyber Security Cooperative Research Centre (Cyber Security CRC) has been granted $50 million over the next 7 years by the government to continue its work connecting industry, government and research organisations to deliver industry-driven cyber security research outcomes, see <https://www.cybersecuritycrc.org.au>.

10 See eg, Karen Keogh, Chelsea Gordon, Patricia Marinovic, 'Global developments in cyber security law: is Australia keeping pace?' (2018) 42 *Law Society of NSW Journal* 82, 82.

If consumers are educated there is a strong possibility that they can exercise a discretion not to use a particular provider's product.[11] Movements such as #DeleteFacebook have shown that there is a correlation between users 'switching off' from Facebook and the increasing public awareness of Facebook's business practices, including data harvesting and paid promotions masquerading as 'news'.[12] With Facebook being the most distrusted brand in Australia for 2018, the trend of increased awareness and distrust can be seen in Australian consumers as up to one in four Australians considered closing their account following the Cambridge Analytica scandal and two in five were 'nervous' about social media companies accessing their personal information.[13] This demonstrates the importance of education in assisting consumers with choosing products and companies which protect their data, are honest in what they do with personal information and promote their products in a transparent way. Overall, education allows people to determine if the product is safe and/or aligns with the users' assessment of the trustworthiness of the business or product.

Data protection

Arguably, strengthening Australia's data protection regime is an essential step in reducing cyber security risk. The current Commonwealth mandatory data breach reporting regime[14] is inadequate as compared with the levels of protection in Europe.[15] Australian privacy laws are also patchwork (nationally) and are failing to protect consumers from excessive harvesting of their personal information. International examples, such as the GDPR in Europe [16] can provide guidance but would need to be adapted to the Australian legal context.

Another idea worth exploring is the use of trust/safety labels. A comparative analysis of Australia's cyber security policy with that of the EU identified the lack of criteria supporting standardisation and development of trust marks/safety labels as 'a major area of weakness

---

11 Studies show Facebook users do not understand how 'newsfeeds' work, see, Aaron Smith, 'Many Facebook users don't understand how the site's news feed works', *Pew Research Centre* (Webpage, 5 September 2018) <https://www.pewresearch.org/fact-tank/2018/09/05/many-facebook-users-dont-understand-how-the-sites-news-feed-works/>.

12 See, eg, Andrew Perrin, 'Americans are changing their relationship with Facebook', *Pew Research Centre* (Webpage, 5 September 2018) <https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>.

13 Jennifer Dudley-Nicholson, 'What Google, Facebook and Twitter really know about you', *The Daily Telegraph* (online), 20 April 2018 <https://www.dailytelegraph.com.au/technology/what-google-facebook-and-twitter-really-know-about-you/news-story/e77b00f7e010afc0f634335cbf31fad1>..

14 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).

15 See, eg, Genna Churches, Monika Zalnieriute and Graham Greenleaf, 'NSW Needs a Strong Mandatory Data Breach Scheme: Submission to Inquiry into NSW Adopting a Mandatory Reporting Scheme for Data Breaches' (2019) *UNSWLRS* 19-69 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3442660>.

16 See, eg, *General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, OJ 2016 L 119/1; see also the new privacy protections enacted by the *California Consumer Privacy Act of 2018* § 1.81.5. [Cal. Civ. Code § 1798.100–1798.199].

that should be a priority' for the Commonwealth government. [17] The development of trust marks, safety labels and standards more generally can also form part of a public education regime by advising consumers about secure technologies including which technologies are more trustworthy.[18]

However, the role of privacy law reforms and trust/safety labels in the overall cyber security legal framework will, as noted above, require a more comprehensive understanding of the various elements of that framework and their relationships to each other.

[17] Matthew Warren and Shona Leitch, 'Australian Cyber Security Policy through a European Lens' (Conference Paper, CCWS 2018 : Proceedings of the 17th European Conference on Cyber Warfare and Security, 28-29 June 2018) 494.

[18] Matthew Warren and Shona Leitch, 'Australian Cyber Security Policy through a European Lens' (Conference Paper, CCWS 2018 : Proceedings of the 17th European Conference on Cyber Warfare and Security, 28-29 June 2018) 494.