Communications Alliance
Australian Mobile Telecommunications Association
Joint Submission

to the Department of Home Affairs

Strengthening Australia's cyber security regulations and incentives

An initiative of Australia's Cyber Security Strategy 2020
A call for views

(27 August 2021)
Ext. 2 September 2021

Contents

Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance.

Australian Mobile Telecommunications Association

The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile network operators and carriage service providers, handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry.

1. Introduction

Communications Alliance and the Australian Mobile Telecommunications Association (Associations) welcome the opportunity to make a joint submission in response to the Department of Home Affairs *Strengthening Australia's cybersecurity regulations and incentives, A call for views* paper (Consultation Paper).

Our members take cyber security, the protection of their networks and their customers data very seriously. In fact, it would be fair to say that our sector is among the most mature sectors with respect to cyber security. Notwithstanding, we welcome Government's desire to foster a whole-of-society and economy-wide approach to cyber security and such an approach ought to form the cornerstone to identify, and subsequently remedy, educational, skills and awareness gaps in this area that may exist today.

2. General observations

2.1. Broadly speaking, the Paper appears to make the claim that because a certain proportion of companies is unaware of some cyber security risks or chooses not to mitigate against those, this is evidence that these risks are incorrectly judged, or current resources devoted to addressing those are insufficient. The paper also makes the assumption that where companies deliberately take on the risk of cyber-attacks, the negative consequences would not be borne by them but instead by external parties, i.e. that there would be negative externalities.

2.2. We believe that the Paper has not presented sufficient evidence for either. Companies do assess cyber security risk, albeit maybe not in an explicit manner. Where companies do not invest resources in specific cyber risk management awareness or cyber risk mitigation exercises, this may well be the result of a calculated judgement that the risk, in their view, does not outweigh the costs for undertaking these activities – in other words, the risk-return ratio did not, in their view, warrant further action.

While one may argue that management may make errors of judgment with regards to that assessment, this would hold equally true for all other managerial decisions which are subject to potential error. Only if it could be demonstrated – by empirical evidence – that errors of judgement with respect to cyber security risk mitigation are far more common than any other managerial error, would it be acceptable to conclude that these risks are not being appropriately considered by companies.

2.3. The Consultation Paper notes, with reference to the critical infrastructure reforms currently underway, that Government's focus for the proposals contained in the Paper "is on all the other businesses that are not subject to sector-specific legislation."[1] Given this is the case and in order to avoid duplication with the extensive requirements that critical infrastructure asset holders will be subject to under the *revised Security of Critical Infrastructure Act 2018* (SOCI Act) and other already existing requirements such as the Telecommunications Security Sector Reform (TSSR) in the *Telecommunications Act 1997*, we recommend that all critical infrastructure asset holders ought to be exempt from any of the measures that flow from the proposals of the Paper.

2.4. The Consultation Paper asks the question how Australia's current regulatory environment could evolve to improve clarity, coverage and enforcement of cyber security requirements.

We believe it would be useful to:

- clearly identify (backed by empirical evidence) the areas of need for intervention through regulation/legislation and;

[1] p.14 Department of Home Affairs, *Strengthening Australia's cybersecurity regulations and incentives, A call for views*, Aug 2021

- where the need has been evidenced and assessed with a positive cost-benefit analysis, address those needs in a sequential manner and with sufficient time for industry to make the requisite changes, and;
- allow those changes to 'filter through' the supply chain and the respective environments before embarking on further changes in similar or even identical areas.

It appears that the desire to address a perceived or actual problem has resulted a multitude of reviews and reforms running in parallel or at with least partly overlapping timeframes. For example: the statutory review of the TSSR runs in parallel to the review of the SOCI Act, which both run ahead of the far-reaching recommendations made in the Richardson Review (largely accepted by Government) and which, so we understand, may now see the commencement of implementation. Simultaneously, companies in our sector are being asked to work through and implement various pieces of national security legislation.

Similarly, the Consultation Paper proposes a Security Code of Practice under the *Privacy Act 1988* (*Privacy Act*) when, so we understand, the next round of the review of the *Privacy Act* is likely to commence in the next few weeks. We also note that the Government committed to the development of a binding Online Privacy Code in the near future. With respect to consumer remedies, the Paper itself correctly points out the various other processes currently on foot that would impact on the issues raised in the Paper.

As previously noted, we are concerned that the Consultation Paper proposes yet another set of rules (voluntary or mandatory) for our sector which is already at risk of being subject to duplicative regimes under the TSSR and the SoCI Act. (Refer to our respective submissions to the Parliamentary Joint Committee on Intelligence and Security)

3. Governance standards for large businesses

3.1. The Consultation Paper proposes a voluntary or mandatory cyber security governance standard for large businesses.

3.2. Following on from our discussion above, we do not see merit in a mandatory governance standard for large businesses. Introducing such a standard would result in unnecessary red-tape and a 'tick-box' exercise, without clearly identifiable benefits.

3.3. We are not sure whether the introduction of a voluntary cyber security standard for large businesses will achieve the desired objective, given the large share of companies that are critical infrastructure asset holders and that, therefore, will be bound by statutory requirements, and noting that we expect all large companies irrespective of their sector to manage cyber security risk (refer to para. 2.1/2.2 above) within their overall business risk assessment processes.

If a voluntary governance standard was to be developed, it would certainly be useful for this standard to be co-designed with industry and without undue haste.

4. Security Code of Practice

4.1. The Consultation Paper raises the question whether a mandatory cyber security code for personal information under the *Privacy Act* ought to be developed.

4.2. We do not believe that such a code would be an efficient way to promote cyber security across the economy for the following reasons:

4.3. We understand from the Consultation Paper and from bilateral discussions and roundtables etc. that the focus of the Consultation Paper is

- "on […] widespread but lower sophistication threats, noting that Government is taking separate action to respond to sophisticated and persistent threats, including through updated critical infrastructure legislation."[2], and
- on smaller businesses who may not have the resources and required understanding to lift their security posture without assistance.

4.4. Against this background, we highlight (as also noted in the Consultation Paper) that the *Privacy Act* generally only applies to organisations with an annual turnover of at least $3 million. However, more than 93% of all Australian businesses are small businesses with an annual turnover of up to $2 million (the ABS uses different turnover brackets), meaning that the share of businesses with an annual turnover of $3 million or more will be even slightly higher. In other words, under the current *Privacy Act,* the contemplated measure would not apply to the vast majority of Australian businesses but would potentially create significant implementation and ongoing compliance costs for those captured by it, without necessarily providing the desired benefit.

4.5. It is also important to understand that a proposed code would only cover the protection of personal information. While there may be some 'spill-over' effects from a code that could potentially improve the protection of other information and devices, it can hardly be argued that this approach is likely to be the most effective measure to lifting the cyber security posture on an economy-wide basis.

4.6. As the Paper points out, the *Privacy Act* is currently under review. Indeed, the Issues Paper initiating the review released in October 2020 addressed data security as one of the issues for consideration and expressly asked the question: "Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?"[3]

Consequently, in our view, it is not useful to commence yet another process in this area prior to the conclusion of the review of the *Privacy Act* (and other associated processes). Doing so risks duplicative or, worse, inconsistent efforts in the same areas of concern.

4.7. Therefore, maintaining the status quo at this stage is a logical and reasonable proposition given

- the limited applicability of the *Privacy Act* with respect
  - to the organisations to which it applies, i.e. organisations with a turnover of $3 million or more;
  - to the data to which it applies, i.e. personal information only rather than having broader cyber security application; and
- the general obligation imposed by APP 11 already sets an appropriate and sufficient standard for the protecting of personal information (particularly considering that it applies to information that may be published or otherwise be in the public domain), i.e. personal information is not without protections and the need for a code would need to be tested irrespective of the limited applicability of the *Privacy Act*.

  As the recent determinations by the Australian Information Commissioner and Privacy Commissioner against Uber Technologies, Inc. and Uber B.V demonstrate, the Commissioner also has the required powers (and uses those) where she finds that an organisation has failed to appropriately protect the personal data of

[2] p.6, Department of Home Affairs, *Strengthening Australia's cybersecurity regulations and incentives, A call for views*, Aug 2021
[3] p.52, Attorney-General's Department, *Privacy Act Review Issues Paper*, Oct 2020

> Australians. In her recent determination, the Commissioner found "the Uber companies breached the *Privacy Act* by not taking reasonable steps to protect Australians' personal information from unauthorised access and to destroy or de-identify the data as required. They also failed to take reasonable steps to implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles."[4]

4.8. We suggest that the Department considers alternative approaches to achieving an improved cyber security protection for organisations, especially smaller businesses, across the economy.

Targeted harm reduction ought to be at the centre of this approach, i.e. targeting specific harms that have shown to be of particular detriment is likely to be more effective and achievable than an unrealistic aim of near-complete risk elimination.

With view to larger organisations, we believe it would be more useful to provide clear guidance to Boards on areas of focus in relation to the management of specific cyber security risks than adding another layer prescription for compliance with APP 11.

It would also be useful to give consideration as to how the advancements already made in and strengths of the critical infrastructure sectors could be used to propagate cyber security-related messages and approaches across the economy.

4.9. It might also be an option to consider a voluntary code promulgated by, for example, ASIC which focuses on protecting IT system and any information held privately irrespective of whether it relates to a natural person. Such a code could perhaps expand on REP 429 as the general regulation of corporations with general application such as the Essential 8.

5. Security standard for smart devices

5.1. The Paper defines smart devices as "sometimes referred to as consumer Internet of Things (IoT) devices, are products that are given extra functionality to connect to the internet. Examples include smart lights, smart TVs, smart watches and baby monitors, as well as the equipment that connects these devices, like Wi-Fi routers."[5]

While this definition would encompass smart phones and tablets as these devices connect to the internet, we interpret the definition and its reference to IoT devices and subsequent examples such that the intention is to exclude smart phones and tablets for the purpose of the discussion around security standards and labelling. This is reasonable as these devices are already subject to a variety of international standards. We are, therefore, concerned with any notion as expressed on page 32 of the Paper to potentially include mobile phones into the scope of the discussion.

We do not support any additional Australian security standard or labelling scheme for these devices.

5.2. The *Australian voluntary Code of Practice: Securing the Internet of Things for Consumers (Code of Practice)* was only released in September 2020. It appears premature to conclude less than one year after release – and during a pandemic – that the Code of Practice has failed as a voluntary measure. We recommend considering efficient and effective avenues for awareness raising, including through industry associations, online marketplaces and ombudsman schemes, prior to moving to mandatory requirements.

---

[4] https://www.oaic.gov.au/updates/news-and-media/uber-found-to-have-interfered-with-privacy/ as accessed in August 2021

[5] p.29, Department of Home Affairs, *Strengthening Australia's cybersecurity regulations and incentives, A call for views*, Aug 2021

5.3. If Government indeed deems a mandatory standard is required, we believe the scope ought to be confined to consumer IoT devices, excluding mobile phones and tablets. For avoidance of doubt, connected cars also ought to be excluded.

Any mandatory standard should also only apply to devices with

- direct connectivity to the internet (i.e. not those that join via Bluetooth or LoraWan through access management software); and
- with sufficient processing power to enable them to host a botnet attack and/or sufficient functionality to place the user at physical or financial risk.

The latter point is of particular importance as widening the scope to 'dumb' smart devices (i.e. for the purposes of the debate, devices that generally do not provide many avenues to place the user at risk but may offer the capability, when hacked, to pose risks to networks) would complicate and delay the implementation of any standard and unnecessarily focus attention away from the desired objective, i.e. the protection of consumers from harm.

5.4. If a mandatory standard was to be adopted, following the UK example and focusing on the top 3 requirements of ETSI EN 303 645 would be a proportionate response, assuming that the top 3 requirements are:

1) banning universal default passwords (but excluding items 5.1-3 to 5.1-5 of ETSI EN 303 645)
2) implementing a means to manage reports of vulnerabilities (but excluding items 5.2-2 and 5.2-3 of ETSI EN 303 645)
3) providing transparency on for how long, at a minimum, the product will receive security updates (but excluding items 5.3-1 and 5.3-2 of ETSI EN 303 645)

Note that the exclusions of the items above equally follow the UK example, i.e. the UK Code of Practice does not mandate the top 3 requirements of ETSI EN 303 645 in their entirety, but only specific parts thereof.

However, we note that these requirements are appropriate for devices with a reasonably substantial processing capacity and power source. These requirements may not be suitable for some small, low powered and long-life devices used in IoT systems.

Any imposition of mandatory requirements should only apply to devices that can place a user, system, network or data at risk. (However, note our earlier comments in relation to focussing on the desired objective of protecting users from harm rather than networks.) If the nature of the device and its function precludes any risk to any of the above, the mandatory obligation should not apply.

6. Labelling scheme for smart devices

6.1. The Consultation Paper proposes either a voluntary labelling scheme (a star rating is being suggested) or a mandatory scheme in form of an expiry date label.

6.2. Similar to our observations on scope for a smart device standard, we highlight that we do not believe mobile phones and tablets ought to be included into the considerations for the labelling scheme. Although an original equipment manufacturer could certify a device for sale, once that device has been sold, it becomes part of an ecosystem where the original equipment manufacturer has no control over future apps and services that may be downloaded or provided to that device. We are concerned that a security label could provide a false sense of security to consumers. This argument holds true for other smart devices, but we believe the risk is by far the most significant for mobile phones and tablets.

6.3. Overall, we believe that the breadth of smart devices envisaged for a labelling scheme is challenging. We recommend further consideration be given to a more risk-based approach and potentially some empirical evidence on the prevalence of different device categories in consumer households.

6.4. We raise serious concerns about the proposed mandatory expiry label:

We do not believe that a mandatory scheme is warranted without giving the voluntary Code of Conduct sufficient time to be adopted and/or without first trialling a voluntary labelling scheme. It would also be prudent to wait until first-hand experience and empirical evidence emerges from jurisdictions that have implemented labelling schemes, such as Singapore and Finland.

It is also worth noting that, if Government did decide to mandate the top 3 requirements of ETSI EN 303 645 (analogously to the UK), then Provision 5.3-13, ("The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period") could be complied with – and it is likely that this is the method of choice given the environment – by publishing online information and resources.

A printed expiry date on a device as proposed in the Consultation Paper is not useful or even dangerous:

- given the very dynamic environment that the device is operating in, how would a device manufacturer reasonably be able to make a claim that a device is secure for a specific period? How would the manufacturer possible take into account latest technological developments on security and be in a position to make such a claim? Such an approach may also disincentivise manufacturers to continue to invest into upgrading security.
- how would 'secure' be defined for the purpose of the claim? No device will ever be 100% secure and it should not be marketed as such. We see significant issues in relation to the misleading and deceptive conduct provisions of the *Competition and Consumer Act 2010*. (We would not be surprised if the example label produced in the Consultation Paper would be deemed misleading by the ACCC.)

Similar concerns apply to a star rating.

6.5. We support a voluntary scheme, co-designed by industry, to make available, e.g. through a QR code, online resources that inform the consumer about the security features of the device, including the unique model of each device and its manufacture date and whether or not the software on the device is maintained by updates online.

Given the nature of the device, i.e. a smart device connecting to the internet, it is reasonable to assume that the consumer can avail themselves of online resources for such information. This also allows businesses to flexibly update the information.

6.6. It could be considered to require manufacturers to declare if software support for the device is less than the expected lifetime of the device, and how long that support period is.

6.7. We support the use of a voluntary certification scheme for evaluating and communicating the level of security provided for a limited scope of consumer IoT devices.

7. Responsible disclosure policies

7.1. The Consultation Paper contemplates either voluntary guidance to increase the uptake of responsible disclosure policies or (mandatory) regulatory means to achieve this outcome.

7.2. Communications Alliance does not support regulatory approaches to support increasing responsible disclosure. This area is still relatively unexplored and ought to have the opportunity to see further development in an unregulated environment.

7.3. Clear guidance for businesses that have not developed an understanding of what may be required for responsible disclosure and awareness raising of the availability of any existing and newly developed guidance would be a useful step to increase the uptake of such policies.

7.4. We also note that legal uncertainties for those researching and disclosing vulnerabilities (as alluded to in the Consultation Paper) need to be clearly addressed if responsible disclosure is to play a greater role in Australian cyber security. If those in the knowledge of a vulnerability have to fear being accused of hacking, there is little incentive (or rather a disincentive) to disclose the existence of the vulnerability, let alone to do so in a timely manner.

8. Cyber security health checks for small businesses

8.1. Given the large share of small businesses in the Australian economy and their potential lack of cyber security awareness and skills, we support a voluntary cyber security health check for small businesses.

8.2. Our members by and large do not fall into this category and we recommend intensive consultation with this respective sector to gain a good understanding of the needs and capabilities of small businesses, e.g. through consultation with the Australian Small Business and Family Enterprise Ombudsman.

8.3. However, from our perspective, we believe it would assist if the general subject of cyber security was broken up into different workable subject areas. The bundling of a range of different topics makes more difficult to identify the real issues. Potential groupings could be:

- zero-day malware;
- known malware;
- scams;
- insider risks; and
- human error.

Each of these have different relevance to:

- configurations and set up of systems;
- management of permissions privileges;
- use of third-party services, ensuring they are safe;
- background checks and training of personnel;
- responding to a breach, how to triage, what to do; and
- internal systems for testing, management, reporting of incidents and remediation of systems.

8.4. The publication of detailed case studies identifying the cause and possible means of prevention of particular instances of cyber security breaches may also be of assistance for small businesses.

8.5. We also note that auDA is currently finalising a joint project, called *.auCheck*, with the Australian Strategic Policy Institute (ASPI) to help promote the uptake of common internet (security) standards in Australia, and thereby contribute to a more safe and secure .au domain.

.*auCheck* provides a free suite of open-source tests that helps users check whether websites, mail domains and connections are set up adequately and correctly for HTTPS, TLS (encryption) and certificate authenticity; alongside DNSSEC (protection against DNS hijacking), DMARC, DKIM and SPF (protection against phishing). Users of .*auCheck* are provided with test results that allow them to start a conversation with their service providers and make sure service offerings are up-to-date and fit-for-business.

It would be worth exploring if such a tool could be integrated into a small business health check.

8.6. With respect to the suggested development of a tick-mark, we note that any tick-mark involving costs for the businesses that wish to use the tick-mark has the potential to create anti-competitive effects where businesses that do not have the resources to afford using the tick-mark attract fewer customers/sales than those who can invest in the tick-mark certification. Therefore, any tick-mark certification ought to be free of charge and not involve hidden costs.

9. Legal remedies for consumers

8.7. The Consultation Paper discusses the potential need for clearer legal remedies for consumers for cyber security incidents. The Paper also correctly points to processes already on-foot that will, through a wider lens, address these issues, namely the planned reforms to the consumer guarantees under the *Australian Consumer Law* and the review of the *Privacy Act*.

8.8. We have already provided a response to the Attorney-General's Department, *Privacy Act Review Issues Paper*, released in October 2020, and will continue to engage with the review of the *Privacy Act*.

We believe that these two processes (reform of the consumer guarantees, review of the Privacy Act) are better placed to address any perceived or actual shortcomings in legislation.

10. Conclusion

The Associations look forward to continued engagement with the Department and other relevant stakeholders on this important topic.

We welcome further discussion on this topic that takes into account existing processes already on foot and advances any further regulations, if necessary, with a view to where meaningful consumer protections can be achieved against the background of any applicable cost benefit analyses.

For any questions relating to this submission please contact Christiane Gillespie-Jones on [redacted] or at [redacted].

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507