INTERNET ASSOCIATION OF AUSTRALIA INC
ABN 71 817 988 968
ARBN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

27 August 2021

To: Cyber, Digital and Technology Policy Division
Department of Home Affairs
Via electronic submission

Thank you for the opportunity to express the Internet Association of Australia (IAA) perspective on the *Strengthening Australia's cyber security regulations and incentives* Discussion Paper (Discussion Paper).

With the Covid-19 pandemic, Australia has well and truly transitioned to a digital economy. To fully take advantage of the significant benefits for Australians, whether in the form of new jobs, improved connectivity or stronger economic growth derived from innovation and improved efficiency and productivity, the risks emanating from cyber-attacks require that measures taken for prevention and mitigation are continuously improved. Such risks therefore should be addressed through innovative approaches to incentives for the adoption of strong cyber security practice broadly across the Australian economy. It can also ensure both consumer and business confidence are appropriately strong in today's digital age.

IAA supports Australia's commitment to ensuring cyber security. Having said that, we are mindful of the complex regulatory environment arising from competing cyber security requirements, especially for smaller internet service providers (ISPs). Many of IAA's members are small to medium internet service providers addressing the small business and retail sectors.

Chapter 2: Why should government take action?

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

Lack of time, knowledge and perceived cost are the main factors which prevent the adoption of cyber security practices in Australia. Resource constraints limit the ability of smaller businesses from applying cyber security best practice. The Australian Cyber Security Centre (ACSC) Small Business Survey[1] notes that 97% of small-to-medium businesses have less than 20 staff. This implies many lack dedicated staff who can effectively understand, plan for, and respond to cyber security risks and incidents. Small business may also lack trust in providers, seeing a lack of value for money.

Limited cyber security education and knowledge, of both consumers and small business, is an important factor. We recognise a range of cyber security education initiatives and resources are provided by the OAIC, ACSC and Digital NSW. However, such initiatives need to be more specifically targeted, and promoted, with broader messaging and outreach and could better utilise the many internet service providers in the market to deliver cyber security messages and services.

Chapter 3: The current regulatory framework

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

Australia's current cyber security framework contains competing compliance priorities and complex regulation. Multiple pieces of legislation exist at both the state and federal levels, and different cyber security regimes

[1] ACSC 2020, *Cyber Security and Australian Small Businesses*, p. 10

exist within and across industries. For smaller internet service providers (ISPs), examples include the *Security Legislation Amendment (Critical Infrastructure) Bill* 2020*, Surveillance Legislation Amendment (Identify and Disrupt) Bill* 2020*, Telecommunications and Other Legislation Amendment (Assistant and Access) Act* 2018 (TOLA), the *Telecommunications Sector Security Reforms* (TSSR) and more. Each requires ISPs to commit to different policies and processes ensuring cyber security. For smaller organisations, or those which are starting out, this complex regulatory environment can impose a significant burden of compliance.

Another concerning aspect is Australia's anti-encryption stance, as displayed within TOLA. Encryption is a necessary aspect of facilitating a safe and secure online environment by ensuring data security, identity management and the protection of devices from unauthorised access. Encryption technologies allow data to be encoded so private and/or sensitive data of users can be protected. It is technically impossible to create backdoors for law enforcement agents to access data which cybercriminals cannot. Analysis commissioned by the Internet Society[2] also concluded that TOLA increased business uncertainty by undermining the security of digital services and products. Therefore, policies which undermine encryption do not ensure cyber security, they undermine it.

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

Avoiding duplication of cyber security requirements will be instrumental in ensuring the current regulatory environment is clear enough for businesses to understand and practical to implement. As mentioned in the previous question, telecommunications providers are already covered by multiple pieces of cyber security legislation which each have different complex requirements and reporting arrangements, and in many cases to different regulators. From the Virtual Forums hosted by the Dept of Home Affairs, we understand there is recognition that policies stemming from this Discussion Paper will not apply to businesses already covered by the *Systems of National Significance* (SoNS) requirements. However, the reality is that existing requirements from legislation developed by Home Affairs contribute to the overall regulatory burden, especially for smaller telecommunications providers.

Home Affairs should consider the effects of its anti-encryption stance on cyber security practices more broadly, especially as it could facilitate a radical disconnect between national security policy and that required to ensure cyber security. Additionally, we would encourage Home Affairs to also engage productively with industry stakeholders affected by cyber security regulation as cyber security regulation is drafted. This is not perceived as a reality in the national security level legislation developed so far.

Australian cyber security policies should also reflect internationally recognised technical standards, such as International Organisation for Standardisation (ISO). Doing so can ensure that Australian businesses can take advantage of proven cyber security approaches and economies of scale in producing resources or obtaining services based on those standards. Making those standards freely available where required under legislation can also remove the financial imposition on smaller organisations.

Chapter 4: Governance standards for large businesses

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

IAA would support mechanisms that look beyond insurance to strengthen corporate governance of cyber security risks. Although signing up for insurance to limit the impact of cyber security risks is a sound approach, there is limited evidence of its effectiveness, especially considering the cost of its uptake, the restrictions on coverage and the need for improved quantitative measures around its effectiveness[3]. Instead, incentives which encourage businesses to embrace proven cyber security practices will be a more effective mechanism.

[2] Internet Society 2021, *The Economic Impact of Laws that Weaken Encryption*
[3] CyberCX, 2021 Cyber Trends Analysis

Chapter 5: Minimum standards for personal information

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 cyber security code as embedded within the Privacy Act could be an effective mechanism for encouraging business to adopt cyber security standards, especially as it would reasonably include clear guidelines for reducing cyberthreats. IAA would advocate for an approach which begins with minimum base requirements, and if compliance is not achieved then consider transitioning to mandatory approaches. This point will be particularly important for smaller businesses, who want to ensure compliance from cyberthreats, but often find it difficult in the face of increasingly complex obligations and risk. The code should also be industry-led, technology neutral and be applied on a risk-based approach, for positive outcomes to be recognised.

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

Businesses need to be encouraged to use strong encryption of personal and private data. As a process, encryption encodes data so it can only be read by the receiver and sender. Although this may reduce convenience, it can ensure that data is protected effectively. Other effective mechanisms which businesses should be encouraged to use include backups, firewalls, anti-virus and anti-malware software and multi-factor authentication.

What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

Technologies and sectors which handle personal, financial and healthcare data should be prioritised if a cyber security code under the *Privacy Act* 1988 code is created. However, there should be clear guidelines on how the prioritisation of specific technologies, sectors or types of data will operate in practice. Consistency across other pre-existing approaches will also be approaches, for example will it be similar to the criteria of the Notifiable Data Breach Scheme, which applies to any organisation or agency which the *Privacy Act* 1988 covers, or will it use different criteria, systems and processes?

Chapter 6 and 7: Labelling and mandatory legislation for smart devices

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

IAA would be open to supporting a labelling scheme or a code for IoT devices that is industry led, adaptable and in line with existing international cyber security mechanisms. We recognise in the Discussion Paper, the implementation of ETSI EN 303 645 as a mandatory standard for consumer grade smart devices, in line with the UK is recommended. Although we agree incentives for smart device producers to implement cyber security measures are low and steps to improve this are required, a mandatory standard may be too prescriptive, especially considering smart devices are multifaceted. For example, risks posed on smart devices such as smart home appliances are different to the risks present on devices facilitating network infrastructure itself. Both face different cyber security threats and require alternative mechanisms to reduce such threats. As such, having voluntary labelling or recommending a technical standard for industry to implement for smart devices can be a useful first step to strengthening cyber security without too much regulatory burden.

Chapter 8: Responsible disclosure policies

Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

IAA is in support of voluntary guidance to encourage Australian businesses to implement responsible disclosure policies. Protection for security researchers that disclose vulnerabilities appropriately would also assist in ensuring the best possible software is available to the Australian market. The ISP industry considers the prompt release of patches for vulnerabilities to be crucial to effective operations.

Chapter 9: Health checks for small businesses

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?

In the Discussion Paper (p.47), it is outlined that small businesses struggle to implement best cyber security practices, because of limited financial, time and human resources. The experience of our members, who are smaller telecommunications providers, is similar to this, however while the majority do hold strong capability in cyber security they may not have time to apply to mere box ticking exercises. Any cyber security health program can only provide support to smaller businesses if it is a simple and effective process for ensuring they meet genuinely important requirements. Thus such a system would need to be practical, effective, up to date, and well recognised.

Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

Small businesses could benefit from a health check program, as it may increase confidence for consumers that the business has the right processes in place to protect their information and data.

However, proactively engaging with small businesses will be a vital aspect of this process, through ensuring any program was practical, up to date and effective. The Department of Industry, Innovation and Science predicted that 5,400 businesses would participate in the Small Business Health Checks in 2019, however, only 35 subsidised checks occurred[4]. As such, incentives which can encourage smaller businesses to embrace the health check will be important.

Incentives which could encourage smaller businesses to participate in a health check program include refundable tax credits, cheaper insurance premiums and protection against [privacy-related] lawsuits if they participate. IAA would encourage government partnerships with organisations such as insurers, banks, accountants and peak bodies, as well as ICT service providers, to ensure information about the health checks is available through accessible locations.

If there anything else we should consider in the design of a health check program?

An important factor which needs to be considered is how external ICT providers, which small businesses tend to use to set up their communications and IT services, can be incorporated into the health check program. The ACSC report concluded that 41% of medium-sized businesses outsource their ICT[5], so perhaps certification in relation to ICT providers or how the service provider industry can be further stimulated should be reviewed. Such a program should avoid conflicts of interest where the same provider also certifies the end product, meaning a third party would be used.

Chapter 10: Clear legal remedies for consumers

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? 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?

The fundamental purpose and principles of the Australian Consumer Law (ACL) mean that it should be effective when applied to insecure IoT devices, as that insecurity, in itself, should render the product potentially as 'not fit for purpose'. It would appear that the application of the ACL has been difficult for consumers in the context of products lacking in cyber security, especially when it comes to attributing the cause of a particular case of identity theft, for example. Examples of poor security have been seen in numerous products available on the market, yet enforcement is clearly absent in the absence of court or tribunal test cases. IoT products, for example, often do not describe their functions well on external packaging making it

[4] ZDNet 2019, *Canberra forecast 5,400 small business cyber health checks, but only 35 happened*.
[5] ACSC 2020, *Cyber Security and Australian Small Businesses*, p. 14

difficult to determine what the product is designed to do and what it is supposed to be connected to prior to purchase. Overseas cases such as the class action taken against Standard Innovation Corporation[6] show avenues to consumer remedy that do not seem available to Australian consumers, even for the more egregious cases such as this. IAA would support fair and evenly applied access for Australian consumers to such remedies available to other traditional products.

Once again, I would like to thank you for providing us with the opportunity to contribute to the *Strengthening Australia's cyber security regulations and incentives* Discussion Paper.

About the Internet Association of Australia

The Internet Association of Australia Inc (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running and lowest cost Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia

[6] SMH, 15 March 2017 We-Vibe sex toy manufacturer settles US class action for almost $4 million