Strengthening Australia's Cybersecurity Regulations and Incentives

Submission by the Australian Communications Consumer Action Network to the Department of Home Affairs

3 September 2021

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation

PO Box 639, Broadway NSW 2007
Tel: (02) 9288 4000 | Fax: (02) 9288 4019 | Contact us through the National Relay Service
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards communications services that are trusted, inclusive and available for all.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact:

Australian Communications Consumer Action Network

PO Box A1158,
Sydney South NSW, 1235

Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
Contact us through the National Relay Service

3 September 2021

Department of Home Affairs

6 Chan St

Belconnen ACT 2617

techpolicy@homeaffairs.gov.au

ACCAN thanks the Department of Home Affairs for the opportunity to contribute to its Strengthening Australia's Cybersecurity Regulations and Incentives consultation paper.

ACCAN agrees with the assertion in the consultation paper that, if the current lack of baseline cyber security precautions is not addressed, cyber criminals will continue to use simple, low-cost offensive tools available on the dark web to conduct cyber-attacks, even without needing a high level of technical expertise.

There is a lack of commercial incentives for Australian businesses to invest in cybersecurity, and the considerable privacy and security threats posed by Internet of Things devices. As a result, a robust and enforceable system of cybersecurity regulation is needed to prevent ongoing exposure of consumers to known cyber security threats.

ACCAN's responses to the discussion paper questions which are within our area of expertise are below.

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

ACCAN agrees that, in the Australian market, there are weak commercial incentives for businesses to invest in cybersecurity. One of the reasons for this is that businesses, both in Australia and worldwide, continue to underestimate the impact that security incidents can have not only at a technical level, but in terms of business risk. Recent public exchanges between Apple and Google regarding privacy and data protection are arguably the first indications that major technology manufacturers are taking notice.[1]

The business-level lack of understanding of the importance of cybersecurity measures also impacts consumers, as cybersecurity features are rarely prioritised in product design and manufacture. In addition, the limited transparency in the cybersecurity features of products on the market, and lack of regulation and enforcement controlling security features, means consumers are not currently making purchasing choices based on comparative in-built cybersecurity product features.

Currently, cybersecurity risks are often transferred to customers. ACCAN agrees government intervention would be effective in encouraging businesses to better manage cyber risk, hold businesses more accountable for consumer protection, and promote 'secure by design' principles.

[1] https://www.politico.eu/article/google-apple-privacy-regulators-gdpr-floc/

Increased transparency at point of purchase of cybersecurity features in products in the form of a star rating would allow consumers to make purchasing choices based on comparative security features and create commercial incentives for business investment in cybersecurity best practice. This would have the flow-on effect of ensuring consumers could have greater confidence in the cybersecurity features of all products on the market.

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

There is no question that an information asymmetry exists between technology manufacturers and product retailers on one hand and consumers on the other. Product manufacturers and retailers have more information about the cyber security in products than buyers. Lack of adequate consumer information and transparency, click wrap agreements and consent fatigue mean consumers are not genuinely reading and accepting Terms and Conditions. Most consumers do not read Ts & Cs or don't fully understand them and are thereby forced into agreeing by default to access the product or service.

Consequently, consumers are unaware of the safety, security and privacy risks posed in using internet connected devices, and thus are exposed to cyber threats they don't fully understand. In addition, where consumers do read the Ts and Cs in full, they are still not in position to decline as acceptance is a condition of access to the service.

It is also true that negative externalities – in this case, underinvestment by a business in cyber security - result in cyber security risk being passed down the supply chain from suppliers of technology to consumers who are less capable of managing cyber security risk.

These two factors mean that there is definitely a role for Government action on cyber security to provide greater protection to consumers. The cybersecurity threats posed by emerging technologies have clearly developed far more quickly than the regulation and laws controlling them. The introduction of comprehensive, enforceable regulation and penalties for breach are the key to increased consumer protections.

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

As the discussion paper outlines, Australia's privacy, consumer and corporations laws were not originally intended to address cyber security, which means the current regulatory framework has a number of limitations in effectively addressing cyber security threats.

In terms of cybersecurity and privacy regulation, the *Privacy Act 1988* was drafted in a pre-internet era and was not designed to control online technologies and threats. The fact that the cybersecurity regulations and incentives review is being conducted in concert with the current reform of the *Privacy Act* is essential to establish a comprehensive, complimentary regulatory framework. The existing Australian privacy regime has many gaps which mean consumers are not adequately protected against online privacy violations and a more robust privacy framework is needed.

The 'reasonable steps' an entity covered by the *Privacy Act* is required to take under Australian Privacy Principle 11 - "protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure" - is open to broad interpretation. In addition, the vast number of exemptions for entities who are not covered by the *Privacy Act* means there

are many circumstances in which online privacy protections are not afforded to consumers at all.

Furthermore, the user consent model that forms the basis of the *Privacy Act* and broader privacy regulatory regime and depends on consumers reading and accepting complex and lengthy Terms and Conditions, is ineffective. The power imbalance between the consumer on one side, and the internet service provider or seller of internet-enabled products on the other, means this consent-based model of privacy regulation is broken. Consumers are usually in a position where they are compelled to accept the Terms and Conditions if they want access to the products and services provided. Given the vast amount of personal data that such products and services collect, consumers are left vulnerable to significant cybersecurity threats and privacy breaches.

The application of the Australian Consumer Law to Internet of Things devices, which are a key access point for unauthorised cyberattacks and privacy breaches, also remains unclear. Australia's existing regulatory regime therefore leaves consumers vulnerable, with inadequate regulatory protection to either prevent or remedy cybersecurity threats and privacy breaches.

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

As outlined in the consultation paper, the lack of clarity, coverage and enforcement of cybersecurity regulation in Australia means that it is inadequate to offer genuine protection to consumers. Consumers need enforceable regulation with penalties to protect them from cybersecurity and privacy threats.

In terms of legal remedies, ACCAN agrees that there are limited legal options for consumers to seek remedies or compensation for cyber security incidents. We support both the reforms being proposed in the consultation paper- a clearer application of the *Australian Consumer Law* to digital products, including consumer guarantees, and the creation of a direct right of action for privacy breaches under the *Privacy Act*.

Clarity of coverage with regard to digital products under the ACL would provide a valuable redress mechanism for consumers who are affected by lax cybersecurity protections. A direct right of action would also deliver meaningful privacy protections to consumers by enabling them to approach manufacturers directly for a remedy – recovery of costs and in some cases compensation for damages or loss - bypassing the expensive judicial process.

A properly resourced oversight body such as the Office of the Australian Information Commissioner (OAIC) will also be needed to expeditiously process complaints handling, monitor breaches and enforce penalties, apply compulsory redress measures and conduct annual reporting on its activities.

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

ACCAN welcomes the invitation to provide feedback about the best way to encourage stronger cyber security risk management within large businesses. Consumers currently shoulder the most responsibility for their protection from cybersecurity threats, and this burden should be shifted away from the consumer back to government and the private sector, who have both the resources and capability to assess and prevent risk.

When a consumer is affected by a cyber security breach suffered by a service provider or is otherwise affected by a security weakness in the construction or operation of a device, then that consumer has suffered an impact that is quite possibly far in excess of the cost of the device or service.

After considering the options for governance standards for larger businesses outlined in the consultation paper, we endorse Option 2 - Mandatory governance standards for larger businesses. ACCAN submits that both Option 0 (Status Quo) and Option 1 (Voluntary governance standards for larger businesses) will be ineffective in delivering genuine protections for consumers.

Option 0 - Maintaining the existing status quo in Australian cybersecurity regulation would mean inconsistent adoption of cybersecurity standards continues, which would offer no benefit to consumers.

Option 1 - Introducing a voluntary standard, implementation of which would remain a business decision, provides too much leeway for businesses to choose not to adopt the standard if they assess the benefits as outweighing the costs. Even where businesses choose to implement a voluntary standard co-designed by business and government, ACCAN harbors concerns that it would offer little consumer protection. Based on past experience, a co-designed cybersecurity standard is likely to being skewed towards encouraging industry buy-in by reducing corporate costs and regulatory burden at the expense of robust consumer protections. The relatively low costs to design and implement a voluntary code, including funding oversight by the OAIC, will result in a mediocre standard of regulation.

Option 2 - ACCAN submits that any effective governance standard must be mandatory, requiring compliance within a specific timeframe, and enforceable with compelling penalties for breach to ensure industry implementation and adherence. A mandatory standard will need to be introduced in tandem with business education and capability raising to ensure businesses have the skills needed to implement the standard effectively.

As the consultation paper notes, there is currently no regulator with the relevant skills, expertise and resources to develop and administer a mandatory cybersecurity standard for large business. It is important that any oversight body, whether it is an existing regulator such as the OAIC or a newly created body, is adequately resourced to perform this role. Any costs to strengthen corporate governance of cybersecurity must not flow on to consumers but should be covered by industry and government who are ultimately responsible for the safety of customers and citizens.

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?

As noted in the consultation paper, a voluntary Code of Practice has limitations in terms of coverage and enforceability, and these limitations have been acknowledged in countries such as the UK where a mandatory Code has been introduced.[2]

[2] https://www.mondaq.com/uk/security/1062182/uk-government-confirms-plans-to-bring-in-mandatory-cyber-security-requirements-for-connected-consumer-products

The development of a Code under the *Privacy Act* will be effective in promoting the uptake of cyber security standards in Australia only if it is both mandatory and enforceable, with penalties for breach and an effective complaints mechanism.

However, a Code developed under the *Privacy Act* will not offer improved regulation in isolation. A comprehensive approach, including sector-specific guidance, that compels adequate risk-based approaches by business is needed to mitigate consumer harm.

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

One way to encourage the uptake of cyber security best practice is through technical standards, yet Australia has been slow to adopt cybersecurity standards due partly to cost and low commercial and regulatory incentives for adoption. There are a range of technical controls which could be imposed by standards to improve cybersecurity protection including firewalls and gateways, secure configuration, access control, malware protection and patch management.[3]

Technical standards must be comprehensive and updated regularly. However simply articulating a series of controls can be counterproductive. A standards framework must be risk based and allow for a range of controls suitable to the (rapidly evolving) IT, OT or IoT systems at issues. This is the reason why standards such as ISO 27001 in tandem with ISO 27002 have been successful, why tier-1 Australian financial services organizations have so successfully defended their assets in line with APRA requirements, and why the Commonwealth government has used this approach with the Protective Security Policy Framework (PSPF).

Smaller business should be encouraged to use third party hosting and processing services that have adequately resourced cyber security programs to ensure that consumer information is adequately protected.

Mandating and enforcing technical security requirements in a standard, however, is just the first step in ensuring all consumers have access to improved cybersecurity protection. Barriers to accessing cybersecurity software, particularly for low-income consumers, will need to be considered as part of the rollout. Consumers on a budget can be reluctant to 'waste' their money and monthly bandwidth allowance on security software updates, so this process must be made cost effective for consumers.

Any cybersecurity software must be either a minimal or no-cost product that is easy to install to make it accessible to all consumers. Bandwidth allowances must be adequate and affordable to encourage consumers, including those on low incomes, to download cybersecurity software and patch updates. In addition, a consumer education program explaining why cybersecurity updates are important for the protection of personal information and security will be needed to encourage users to download and instal security software.

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?

---

[3] Vidler, J Seabrook T, Rashid A 2015, Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials, available at http://www. research.lancs.ac.uk/portal/en/publications/cyber-security-controls-effectiveness(a09a2d28-d121-41dc-86d6-cc24595d8968)/export.html.

Insofar as personally identifiable information as outlined under the Privacy Act is at issue, the requirements should be technology independent.

All forms of personal data should be protected by a code under the Privacy Act to achieve best cybersecurity outcomes including:

- Inferred personal information;
- De-identified information;
- Technical information;
- Pseudonymised information; and
- Anonymous information

It is important to note that the risk profile between consumers and business can be asymmetric. While large businesses may have the resources to provide adequate levels of data privacy protection, smaller organizations which may be exempt under the *Privacy Act* may not. However, this doesn't lessen the risk – or the impact of a compromise – on the consumer. This suggests that protection for the consumer rather than size of the business should be the determining factor.

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

One of the primary reasons consumers are vulnerable to cybersecurity threats via smart devices is that there is no enforceable framework for regulation and no market incentives to ensure devices are sold with in-built security by design features.

In ACCAN's recently published policy position, *Connection and Protection: What consumers need from the Internet of Things*, we recommended several enforceable measures to improve the cybersecurity of IoT connected devices which may be of interest to the Department of Home Affair. These recommendations were:

- Requiring devices and services to only operate on the 'principle of least privilege' (POLP), restricting degrees of user access on a case-by-case basis to reduce the risk of attackers gaining access to critical systems or sensitive data, contain security compromises to their area of origin and stop them spreading to the system at large.
- Requiring use of appropriate privileges on software access, using a secure software development process, and performing penetration testing to protect connected devices against infiltration by hackers seeking to access a local Wi-Fi network to manipulate all connected devices.
- Requiring device manufacturers to disable unused device functionality, close unrequired ports and restrict access to web management to the local network, unless the device needs to be managed remotely via the internet.
- Requiring encryption in transit of any security-sensitive data, including any remote management and control, at the device or user interface level to prevent unauthorised infiltration by hackers. In the current unregulated system, IoT device manufacturers are not required to use encryption software and often omit this in favour of cost reduction, increased battery life, minimised memory requirements, ease of use and reduced device size.

- Requiring secure storage of credentials on devices and services, including not allowing hard-coded credentials such as usernames and passwords to be embedded in device software or hardware, to prevent security breaches via reverse engineering.
- Requiring users to change default passwords before using IoT devices to prevent duplicated or default passwords being used. Unique passwords would restrict the risk to consumers posed by hackers infiltrating networks. This approach would be consistent with the Australian Privacy Act requirement to implement a 'privacy by design' approach to compliance. Alternative authentication approaches, such as biometrics, should be encouraged as alternatives; this technology is already well established in consumer-level operating systems.
- Requiring device manufacturers to automatically update IoT devices with new security software, distributed via secure IT infrastructure and easily installed by consumers. Updating security software should not be the obligation of the consumer but should be the responsibility of the IoT device manufacturer. Consumers should also be encouraged by manufacturers to keep home network router software up to date and make sure all security patches and software updates for IoT devices are installed as soon as they are released.[4]

Under Australia's current voluntary Internet of Things Code of Practice,[5] device manufacturers are free not to include security features in the design of smart devices. There are no penalties if security features are not in-built, and so manufacturers often favour cost saving and optimal user experience over cyber safety. Enforceable regulation and a mandatory Code is needed to guarantee safety by design in smart device manufacture.

12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt 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?

ACCAN submits that the introduction of mandatory standards for smart devices is needed to protect consumers from cybersecurity threats, and we endorse the adoption of ETSI EN 303 645,[6] currently used in Singapore's smart device labelling scheme, as a mandatory security standard in Australia to regulate smart devices.[7] The 33 security requirements and 35 recommendations to manufacturers across 13 categories of security and privacy provide a comprehensive regulatory framework to protect consumers from harm.

Many of the requirements in ETSI EN 303 645 were also recommended by ACCAN in our recent position paper addressing the need for improved regulation of IoT devices in Australia. These include prohibiting universal default passwords; keeping software updated; minimising exposed attack surfaces; ensuring software integrity; ensuring that personal data is secure; making systems resilient to outages; making it easy for users to delete personal data; and making installation and maintenance of devices easy. Only if a device meets all these criteria is it considered capable of mitigating cyber threats and increasing consumers' privacy protection.

---

[4] https://accan.org.au/accans-work/policy-positions/1893-iot-policy

[5] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice

[6] https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard

[7] https://ims.ul.com/singapore-cybersecurity-labelling-scheme-cls-certification

ACCAN welcomes the introduction of these requirements in Australia, as well as the recommendation in the standard's data protection provision – i.e. that manufacturers provide consumers with clear and transparent information for each device and service about what personal data is collected and processed, how it is being used, by whom and for what purposes.

We note that the intended purpose of standard ETSI EN 303 645 is to offer protection to consumers in line with Europe's General Data Protection Regulation (GDPR), and this standard of protection is only reached if all 68 requirements and recommendations are implemented. Although the GDPR does not apply in Australia, it does set an important baseline for privacy and data protection that all territories worldwide should be aiming to reach. ACCAN therefore rejects the proposal that only the top three requirements of the standard should be adopted in Australia.

In addition, we note that after the requirements of the ETSI EN 303 645 have been implemented, manufacturers' products are tested by a third-party testing laboratory. Independent testing and rating by a third party, rather than by the device manufacturer themselves, should also be adopted in Australia to provide impartial and transparent oversight of the consumer protection regime.[8]

Furthermore, ACCAN submits that any cybersecurity standard introduced in Australia must be mandatory, and buttressed with enforceable penalties, to guarantee adoption by manufacturers, retailers and service providers.

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?

It is almost impossible to predict the costs of a mandatory standard, as costs will vary with the type of device and the use cases to which it will be applied. It is likely that businesses will pass on the costs to the consumer, in whole or in part.

The real question is what cost consumers are willing to bear for the risks that they are incurring, and this will vary among categories of consumers, with vulnerable and low-income consumers least capable of covering costs.

In considering the necessity of a mandatory (as opposed to voluntary) standard, government and business need to bear in mind that the impact of cyber security failures are likely to become more profound as ecosystems of interlinked IT, OT and IoT devices emerge. Cybersecurity failures will then have potential for serious physical harm to individuals and broader society, and impact national networks.

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

As the Department of Home Affairs has noted, consumers do not currently have the tools to easily understand whether smart devices are cyber secure as there is often a lack of clear, accessible information available to them. Even if they do have access to this information, most

[8] https://www.dekra-product-safety.com/en/what-is-etsi-en-303-645-cybersecurity-standard

buyers don't have the technical capability to determine or control the security of a product and it is costly and time-consuming for buyers to independently verify the security of products.

In addition, the lack of consumer information available about cybersecurity in smart devices means consumers are not making purchasing decisions based on comparative cybersecurity features. Mandatory labelling of cybersecurity ratings in smart products would create a market incentive for manufacturers to include safety features, as consumers are likely to purchase secure devices in preference to insecure devices.

ACCAN agrees that if the current status quo is maintained (Option 0) and no labelling scheme is introduced, insecure smart devices will continue to cause privacy, cybersecurity and online safety harms to Australians.

ACCAN submits that, based on Data 61 consumer research,[9] a 'star rating' or labelling scheme (Option 1) is likely to encourage consumers to purchase secure smart devices by enabling them to make informed purchasing decisions based on the security features available. Consumers would also need to be educated about the importance of cyber security features and how to judge the best options at point of purchase for a star rating or labelling system to be effective.

However, ACCAN submits that a labelling scheme needs to be mandatory to be effective. As the consultation paper acknowledges, it is uncertain whether there would be sufficient industry participation in a voluntary labelling scheme and even if it were, uptake would be a slow process requiring sustained government promotion. Without sufficient uptake of labelling, businesses with the lowest levels of cyber security would continue to have low incentives to improve cyber security. An effective, consistent labelling scheme must also be independently assessed or, if self-certified by the product manufacturer, subject to approval by an independent administrative body.

ACCAN submits that a mandatory expiry date label (Option 2) could also be adopted as part of a broader cybersecurity labelling scheme for smart products. This would provide balance, in that manufacturer liability may sharply decrease at the nominated date of expiry.

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

A combination of labelling and standards for smart devices would provide a sound level of protection for consumers. A labelling system would enable consumers to make informed purchasing decisions based on the security of devices on the market, and mandatory standards for smart devices – for example, an enforceable 'security by design' standard - would ensure all devices on the market had to meet a minimum level of cybersecurity protection.

Furthermore, this blend of nominated protection level, benefitting the consumer, and expiry date, benefitting the manufacturer will help to create competitive tension in the market.

---

[9] Data61 2020, *Results of the IoT Consumer Focused Survey*, unpublished report produced for the Cyber Security Cooperative Research Centre; Atif Ahmad et al., *Towards responsive regulation of the Internet of Things: Australian perspectives*, available at https://policyreview. info/articles/analysis/towards-responsive-regulation-internet-things-australian-perspectives.

18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? a. If so, which existing labelling scheme should Australia seek to follow?

Labelling of smart devices by industry will only be adopted if it is mandatory and enforced and buttressed with penalties for breach. A voluntary star rating system will not be adopted by industry as, in the current marketplace, consumers are more likely to choose affordability over security features if they don't understand the seriousness of cyber security threats and data breaches posed by insecure devices. There is no commercial incentive for any manufacturer to claim anything other than an industry-leading position.

The introduction of a mandatory labelling scheme will ensure all manufacturers are subject to the same standards and comparisons, and that comparing products based on security features is a necessary factor considered by consumers in choosing smart devices. A feedback loop from consumers, who choose to purchase secure devices over insecure devices, will create a commercial incentive for manufacturers to include security features in their products.

Any voluntary star rating system where manufacturers and retailers of smart devices are solely responsible for judging their own security standards is open to bias. For such a scheme to be both accurate and effective, an independent oversight body will be needed to assess products and provide a star rating. Alternatively, where a manufacturer self-certifies, this certification will need to be approved by an independent oversight body, buttressed by severe penalties for failure to be accurate and comprehensive in self-certification.

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

Security expiry dates should be part of a broader mandatory labelling scheme. Although the consultation paper presents these two options as an either/or system of labelling, ACCAN submits that both a mandatory star rating and mandatory security expiry date should be included in product labelling to provide consumers with adequate information to make informed purchasing choices.

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

A mandatory labelling scheme should cover mobile phones and other smart devices, as these devices are vulnerable to hacking and unauthorised access to a wide range of personal information.

Furthermore, smart devices provide vulnerable entry points for hackers to infiltrate the private in-home networks of consumers and exploit these entry points to conduct en masse cybersecurity attacks which have much broader impacts. It is crucial that smart devices should be included in a mandatory labelling scheme to control both individual and large-scale cybersecurity attacks and privacy breaches.

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

Due to the large volume of purchases that are made online, particularly in the context of COVID lockdowns, it is important that manufacturers should label smart devices both digitally and physically. If smart devices were to only have 'star ratings' or labelling on physical packaging, this would exclude online customers from making informed purchasing decisions based on the

security features in smart devices. It is essential that labelling is included in online marketing material, as well physical packaging, to capture all consumers purchasing smart devices.

Digital marking provides benefits that go beyond consumer information. For example, myGov now allows for citizens to authenticate using digital certificates on their mobile phones. It is therefore arguable that not only should mobile phones include mandatory labelling, but the` ability to access sensitive services should be contingent on those devices having an adequate level of security, which could be determined using a "star rating" system combined with expiry date.

Voluntary guidance would not offer sufficient incentives to encourage Australian businesses to implement responsible disclosure policies. Mandatory standards buttressed by enforceable penalties are needed to ensure Australian businesses implement responsible disclosure policies.

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

Voluntary guidance would not offer sufficient incentives to encourage Australian businesses to implement responsible disclosure policies. Mandatory standards buttressed by enforceable penalties are needed to guarantee transparent disclosure by industry.

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?

A health check program would only be effective if it led to the remediation of the problems that it uncovers.

Hackers relentlessly scan for targets, both large and small, meaning that fraudsters and others are aware of potential victims. Such a health check program will not close the gap but it will lessen the potential attack surface.

There are established practices for supply chain security that could be adapted for use by small businesses. For example, a security ratings approach or possibly a shared assessments model that provides an easily-understandable and regularly maintained certification rating could be utilized by 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?

Small-businesses are often resource-starved. It is unlikely that any scheme could succeed without a commercial incentive.

A successful model may have the following features:

- Incentives for participating in such a scheme, such as reduced liability for scheme participants and tax deductibility for costs (including remediation of vulnerabilities).
- Disincentives for non-participation, such as full liability and tax levies for non-participants and for participants who do not address serious vulnerabilities.

ACCAN would prefer an incentive rather that disincentive model for small businesses.

25. Is there anything else we should consider in the design of a health check program?

A health check program needs to be easy for consumers to access and use.

The incentives and disincentives for using the program must be compelling.

A health check program must also be independent. Self-certification of health is wide open for abuse and fraud. Most small business would not have the expertise to make an informed and honest assessment.

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?

The legislation and Codes governing cybersecurity regulation should be reviewed within a year of its operation and updated as circumstances change and new threats arise.

In conclusion

We would welcome the opportunity to engage further the Department of Home Affairs on this important consultation.

Sincerely

Wayne Hawkins

Director of Inclusion

ACCAN