

Submission to the Department Home Affairs – Strengthening Australia’s cyber security regulations and incentives

6 September 2021

Jeremey Burnett
Director — Digital Economy Resilience and Market Reform
Cyber, Digital and Technology Policy Division
Department of Home Affairs

By email: techpolicy@homeaffairs.gov.au

Dear Mr Burnett

The Consumer Policy Research Centre (CPRC) welcomes the opportunity to contribute to the consultation on ‘Strengthening Australia’s cyber security regulations and incentive’.

CPRC is an independent, non-profit consumer research organisation. Our mission is to improve the lives and welfare of consumers by producing evidence-based research that drives policy and practice change. Data and technology issues are a research focus for CPRC, including emerging consumer risks and harms and the opportunities to better use data and technology to improve consumer wellbeing and welfare.

The CPRC commends the Department of Home Affairs for its detailed review of Australia’s current cyber security landscape and for consulting on the opportunities that Australia can embark on now for ensuring a stronger digital environment for Australian consumers in the future.

Over the last three years, studies across CPRC’s data and technology research stream¹ have confirmed that consumers are overwhelmed with the explosion of data driven products and services. Information asymmetries, lack of accessible remedies and inadequate consumer protection frameworks, mean that while the choice of digital products and services has increased, frameworks to protect consumers in this booming digital environment have not adequately kept pace.

Below are CPRC’s response to various questions from the consultation paper.

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

Both negative externalities and information asymmetries create an urgent need for Government to take immediate and adequate action on cyber security. We agree with the statement in the consultation paper that, “... *market failures are unlikely to be corrected without action by government*”. This is evident, for example, in that no significant shift in

¹ See CPRC’s website – Data and Technology section under Reports and Submissions: [Data and Technology - CPRC](#)

industry has taken place since the release of the voluntary *Code of Practice: Security the Internet of Things for Consumers* in September 2020.

As other jurisdictions worldwide progress their cyber security legislation, without adequate intervention, the Australian Government risks Australia becoming a ‘dumping ground’ for subpar digital products and services, further exposing Australian consumers to cyber security threats. Our 2020 Data and Technology Consumer Survey² revealed that 94% of consumers already have high concerns regarding data breaches or hacks. The survey also highlighted Australian consumers’ strong belief that government should be responsible in ensuring that consumers are protected.

Information asymmetries exist for consumers across various markets, but none are as exacerbated as they are for consumers in the digital environment. Qualitative research conducted by CPRC between June and August 2021 found that online life can be a “double-edged sword” for Australian consumers.³ While consumers value the convenience and access to more products, the online environment can feel overwhelming, especially with the level of information and marketing they experience. Participants reported feeling that they need to be experts in products and services to successfully navigate issues and access remedies. The opportunity now is to help create a more accessible and meaningful framework through legislation and incentives that protect and empower consumers in a digital environment. This requires both minimum protections and guardrails, as well as adequate information to enable choice and accountability.

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

Australian consumers expect that the laws in place protect them from current and emerging harms, but the reality is that the gap between the current regulatory environment and consumer and community expectations is significant. Fairness and safety are two consistent expectations that are voiced by consumers through our research and these elements need to play a fundamental role in improving the enforceability of cyber security requirements. Regulation needs to shift to ensure that duty of care and liability is placed on businesses and not on the consumer.

This is especially necessary when it comes to complex products, services, and cyber security risks. The expertise required to assess risk is significant and beyond what would be considered reasonable for consumers themselves to assess. This digital environment will only become more complex as technology and time progress. Clear, predictable guardrails to prevent the proliferation of unsafe products as well as provide industry with sustainable, predictable policy regimes will be essential to enable innovation.

The consultation paper notes that there are at least 51 Commonwealth, state and territory laws that could be involved in the creation of cyber security obligations. A fragmented cyber security framework will continue to lead to confusion for businesses and create further gaps in consumer protection. There must be a clear pathway for businesses to understand their obligations and for relevant regulators to have clarity on their scope of and approach to enforcement.

² CPRC, “2020 Data and Technology Consumer Survey”, (December 2020), [CPRC 2020 Data and Technology Consumer Survey - CPRC](#).

³ CPRC, “Consumer Wellbeing Report: Phase 1”, Draft, Unpublished.

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?

We agree that a code under the Privacy Act could assist in increasing the uptake of cyber security standards in Australia. We also agree that greater clarity of Australian Privacy Principle (APP) 11 with a focus on minimum standards instead of best practice could help drive positive change in handling of personal data. However, the code would need to avoid vague language such as “reasonable steps” and provide practical obligations that can be effectively measured and enforced. Our research shows that the opacity of how personal data is collected and used in a digital environment continues to be of high concern for Australian consumers. Our 2020 Data and Technology Consumer Survey revealed that 94% of Australian consumers do not feel comfortable with how their personal information is collected and shared online:

- Only 12% of consumers feel that they have a clear understanding of how their personal information is collected and shared.
- Only 6% of consumers are comfortable with how their personal information is collected and shared online.⁴

Inclusion of a code under the APP, however, cannot be done in isolation, as it will not provide adequate consumer protection. It also will not cover all actors in the supply chain, noting that most small business operators (business with an annual turnover of less than \$3 million) are not recognised as APP entities, and thus would be exempt from the code. Urgent economy-wide reforms are needed to protect consumers from data extraction and manipulation in an online environment, including:

- introducing an unfair trading prohibition
- strengthening unfair contract terms provisions
- introducing of a general safety provision
- reforming the Privacy Act to give consumers more control and agency over their data, including:
 - introduction of a direct right of action
 - requirement to gain consumer consent for data collection
 - procedures and processes that safeguard personal and sensitive information
 - implementing pro consumer defaults
 - strengthening privacy notice requirements
 - greater transparency of data collection practices
 - right to erasure mandatory deletion of information that leads to risk.

With other reforms also underway that specifically focus on opening up consumer data (e.g. Consumer Data Right and Australian Data Strategy), it will also be critical that a cyber security code for managing personal information adequately addresses the risks in greater portability of data.

⁴ CPRC, “2020 Data and Technology Consumer Survey”, (December 2020), [CPRC 2020 Data and Technology Consumer Survey - CPRC](#)

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?

In terms of data that should be covered by a code, the scope should not be limited to direct, identifiable data only. Currently, data is being collected, shared and used in Australia in a way which is not in line with consumers and community expectations. For example, our report, *A day in life of data*, specifically highlights the lack of focus on the operation of data brokers to date in Australia, despite their central role in exchanging and combining personal information and how easily deidentified pieces of data can be collated to reidentify people in the digital environment.⁵ The code should aim to create a safe and effective ecosystem for consumers to control and share their data, and where data transforms to open data, there should be protocols in place to mitigate the risk of reidentification via collection of deidentified data.

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

Currently, many physical products in Australia are subject to only ex-post regulation and do not require any form of certification or testing prior to being sold in the market⁶. Compliance is managed through surveillance and monitoring of samples across the market by regulators.⁷ This approach can only be maintained when the product set is small but with the variety and range of products and services continuously growing in the digital environment, this approach is unsustainable for smart devices. Due consideration needs to be given for cyber security in smart devices to potentially be regulated through a combination of both ex-ante and ex-post regulation.

One of the key insights at the Consumers International Digital Hive Summit in 2019 highlighted the need for consumer protection to begin at the product design stage and then reflected throughout the supply chain, not just at the point of purchase.⁸ A 'security and safety by design' approach is key to reducing the likelihood of substandard products and services entering the market in the first place, and then ex-post enforcement can assist in identifying and managing rogue actors who are likely operating in the low-value goods space. However, this is dependent on regulators having the capacity and capability to effectively monitor and enforce the market. Regulators may need to consider alternative surveillance frameworks that do not rely on in-house surveillance alone. There needs to be significant shift from the traditional surveillance mindset. Regulators will need to consider alternative frameworks such as leveraging partnerships with cyber security experts (including ethical hackers) and collaborating with international regulators to ensure surveillance is effective in detecting current and possible future cyber security threats in smart devices. Regulatory sandboxes can also provide the opportunity to work collaboratively with actors across the supply chain to test innovative regulatory requirements.

⁵ Richmond, B, "A Day in the Life of Data", CPRC (2019), [Research Report: A Day in the Life of Data - CPRC](#).

⁶ See [Mandatory standards | Product Safety Australia](#)

⁷ See surveillance example: ACCC's product safety surveillance program: [Surveillance program | Product Safety Australia](#)

⁸ Key take-outs from CPRC Digital Hive Summit 2019: [Highlights from the #DigitalHive Summit - CPRC](#)

12. Would ETSI 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?

We agree that the implementation of standard ETSI EN 303 645 could significantly improve the protection offered to Australian consumers using smart devices. It is our understanding that the UK Government will be mandating the following three requirements from the standard:

- No use of universal default passwords (*Requirement 5.1 No universal default passwords*).
- Public point of contact for consumers to report vulnerabilities (*Requirement 5.2 Implement a means to manage reports of vulnerabilities*).
- Information at point of sale detailing an expiry date for software updates (*Requirement 5.3 Keep software updated*).⁹

Given that Australia currently ranks last in manufacturing self-sufficiency among all OECD countries¹⁰, many of the smart devices used by Australian consumers are likely to be designed and manufactured overseas. Where possible, alignment with international standards (voluntary or mandated) will ensure broader consumer choice. Bespoke regulation is likely to narrow consumer choice and increase product costs for Australian consumers.

However, ETSI EN 303 645 includes other requirements that are equally important for protecting consumers:

- Requirement 5.8 Ensure that personal data is secure.
- Requirement 5.9 Make systems resilient to outages.
- Requirement 5.11 Make it easy for users to delete user data.

The reason that these may not be mandated by the UK Government is because of other complementary regimes that exist within its jurisdiction. The General Data Protection Regulation (GDPR)¹¹ and the Data Protection Act 2018¹² include provisions for the right to erase personal data and protection of personal data in general. The UK General Product Safety Regulation¹³, which is equivalent to a general safety provision, requires, “...*all products to be safe in their normal or reasonably foreseeable usage and enforcement authorities have powers to take appropriate action when this obligation isn’t met*”. Given that Australia’s Privacy Act has not been updated since 1988 and there has been little to no progress by Treasury in introducing a general safety provision within the Australian Consumers Law (ACL) since it was first called for in 2018 by the ACCC¹⁴, implementation of requirements 5.1 to 5.3 of ETSI EN 3030 645 standard alone will not be sufficient in

⁹ UK Government’s media release on 21 April 2021: [New cyber security laws to protect smart devices amid pandemic sales surge - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge) and Final draft ETSI EN 3030 645 V2.1.0: [EN 303 645 - V2.1.0 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements \(etsi.org\)](https://www.etsi.org/standards-store/EN-3030645-V2-1-0-CYBER).

¹⁰ Stanford, Jam, “A Fair Share for Australian Manufacturing”, The Australia Institute – Centre for Future Work (July 2020), [A Fair Share for Australian Manufacturing - Centre for Future Work](https://www.austlii.edu.au/au/other/auia/pubs/afairshareforaustralianmanufacturing/).

¹¹ See Guide to the General Data Protection Regulation (GDPR): [guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/510478/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf).

¹² See UK Data Protection Act 2018: [Data Protection Act 2018 \(legislation.gov.uk\)](https://www.legislation.gov.uk/ukpga/2018/12/section/1).

¹³ See General Product Safety Regulations 2005 – Guidance for Businesses: [General Product Safety Regulations 2005 - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/general-product-safety-regulations-2005)

¹⁴ See speech by Rod Sims at the National Consumer Congress 2018: [2018 product safety and consumer protection priorities | ACCC](https://www.accc.gov.au/about-us/newsroom/speeches/2018-product-safety-and-consumer-protection-priorities)

mitigating cyber security threats for Australian consumers. As mentioned in our response to question 8, several urgent reforms need to be progressed simultaneously for cyber security regulation to be successfully implemented in Australia.

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

Trust is crucial in consumer's purchase of any smart devices. A key part of building consumer confidence and trust is reducing information asymmetry prior to the point of purchase. This will assist consumers in making an informed purchasing decisions for secure smart devices. Ultimately, information should be:

- clear and easy to understand
- be comparable across products
- available through a trusted source
- unbiased, ensuring any sponsored content is clearly distinguishable from genuine expert advice.

We continue to urge policy makers to develop and publish service quality ratings, where market stewards take a more active role in developing and publishing service quality ratings, informed by consumer testing, drawing on regulatory data. A good example of this is the ACCC broadband speed testing, which also led to specific guidance for internet service providers.¹⁵ It is positive to see that the consultation paper is giving due consideration to security ratings and upfront information on product longevity via software updates to nudge consumers in choosing more secure smart devices. However, we reiterate the limitations of relying on information remedies alone in these complex product and service markets.

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

We agree that a combination of labelling and standards would be a practical and effective approach in reducing the impact of cyber security threats to consumers. Clear labelling which provides key security information prior to the point of purchase can help consumers distinguish between products that are either more or less secure, with the aim to aid better purchasing decisions.

Effective standards would help ensure that what is available for sale in the marketplace incorporates minimum security expectations and has been developed with the intention of safety and security in mind, especially if standards impose a mindset of 'security by design'. This would also assist in alleviating the burden from consumers to become 'experts' to be able to decipher between secure and non-secure smart products or needing to actively seek out clearer information from alternative sources.¹⁶

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

A mandatory expiry date labelling scheme that is consistently applied across all smart products would provide consumers with a clear comparative information when choosing between different devices. Depending on the product and its intended use, consumers would

¹⁵ See ACCC's broadband speed webpage: [Broadband speeds | ACCC](#).

¹⁶ See Mozilla's guide to safe and secure connected products: <https://foundation.mozilla.org/en/privacynotincluded>

assist consumers to identify whether the product will suit their needs. However, the example label on page 39 of the consultation paper only notes the year of expiry (i.e. Cyber protection until 2025). The label should articulate a clearer timeframe (e.g. Cyber protection until Dec 2025 or Cyber protection until end 2025) to avoid ambiguity of when product may no longer be supported. Also, a consumer education campaign would need to support the implementation of any labelling scheme to ensure consumers are aware of and understand the risks of using a product past its cyber protection expiry date.

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

Mobile phones should remain in scope for any mandatory labelling scheme as it is one of the most used smart devices by consumers in Australia. Our 2020 Data and Technology Consumer Survey indicated that location apps and GPS devices were the most used internet-connected devices, followed by smart assistants and exercise health trackers. This is no surprise as many of these features are accessible via smart phones, which Deloitte reported that in 2020, 92% of Australians had direct access to a smart phone.¹⁷ In comparison, other smart devices are still not as prominent in Australian households. Our 2020 data and technology consumer survey revealed that less than 8% of Australians currently use the following internet connected devices:

- Smart household appliances (7%)
- Smart home security system (6%)
- Smart thermostat (2%)
- Smart baby monitor (2%).¹⁸

In addition to assisting consumers distinguish between genuine and grey market products, covering mobile phones in the mandatory labelling scheme would also reduce the ambiguity of how long a phone would be supported with critical software updates. Qualitative research conducted by CPRC between June and August 2021 revealed that consumers feel betrayed when smart phones stop receiving relevant software updates, suddenly rendering them obsolete.¹⁹ Once again, having information upfront would ensure consumers can make an informed decision prior to purchase.

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

It is not just beneficial but critical that any information that would be available to a consumer prior to purchase in a physical setting, should also be available in a digital setting – and importantly needs to be consistent across different marketplaces. Our 2020 consumer data survey revealed that the frequency of engagement in online shopping is steadily increasing with 61% of respondents visiting online shopping websites on a monthly basis, if not more frequently (28% visiting at least once a week – up from 21% in 2018).²⁰ The trend towards online shopping was further echoed in our Consumers and COVID-19 survey data²¹ which

¹⁷ Deloitte, “Digital Consumer Trends 2020 – Unlocking lockdown”, (2020), [Digital Consumer Trends 2020 | Deloitte Australia | Technology, Media & Telecommunications, Mobile, Trends](#).

¹⁸ CPRC, “2020 Data and Technology Consumer Survey”, (December 2020), [CPRC 2020 Data and Technology Consumer Survey - CPRC](#).

¹⁹ CPRC, “Consumer Wellbeing Report: Phase 1”, Draft, Unpublished.

²⁰ CPRC, “2020 Data and Technology Consumer Survey”, (December 2020), [CPRC 2020 Data and Technology Consumer Survey - CPRC](#).

²¹ CPRC, “Unfair Trading Practices in Digital Market: Evidence and Regulatory Gaps”, (March 2021), [Unfair Trading Practices in Digital Market: Evidence and Regulatory Gaps - CPRC](#).

indicated that by September 2020, 28% of consumers were spending more time online shopping for personal items in comparison to a pre-COVID month. With more consumer engagement in the online retail space, consumers need to have confidence with the purchases they are making online.

As an example, it was positive to see that the mandatory standards on button batteries and products containing button batteries which was introduced in 2020 included specific warnings which were recommended to be featured online in the product description. A similar approach could be applied to labelling of smart products. However, these are recommendations only and are not mandated, nor enforced. As we have raised in previous submissions²², including our most recent submission in August 2020 to the ACCC on Digital Platforms Inquiry into online retail marketplaces, we urge Government to hold online marketplaces to a much higher accountability that is at par with bricks and mortar stores.²³

26. 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?

The ACL in its current form places undue burden on consumers to identify exact cause of harm and to seek an effective remedy. We agree with the various challenges noted in the consultation paper, especially with applying consumer guarantees to seek recourse, which is often challenging to apply for physical products but is further exasperated in a digital environment due to the extensive information asymmetries. The ACL also takes a very linear view of the supply chain, which causes further challenges as digital actors can move fluidly in and out of the supply chain, making it difficult to identify whether a cyber security incident was caused by a specific product, software update or an amalgamation of two digital products.

Unlike physical products that can only cause physical harm where cause and consequence are direct and visible, digital products and services, especially smart devices, have the potential to cause both physical and digital harms²⁴. It is difficult to ascertain what the long-term impacts may be, but it is reasonable to assume that consumers are likely to experience flow-on negative impacts due to a cyber security incident. This is further exacerbated in situations where a consumer may not even be aware that they have been subject to a cyber security incident. These scenarios create a challenging environment for consumers to seek recourse via the ACL in its current form. A general safety provision, as mentioned previously in the submission, would help increase consumer protection and address some of the challenges that consumers are likely to face when using digital products.

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?

Please see our response to question 8 where we call for a variety of urgent reforms that need to take place in addition to the revision of the Privacy Act 1988 to create a fairer and safer market for Australian consumers.

²² CPRC, "Unfair Trading Practices in Digital Market: Evidence and Regulatory Gaps", (March 2021), [Unfair Trading Practices in Digital Market: Evidence and Regulatory Gaps - CPRC](#).

²³ See submission: [Submission to ACCC: Digital Platform Services Inquiry – Online Marketplaces - CPRC](#).

²⁴ OECD (2016), "The Internet of Things: Seizing the Benefits and Addressing the Challenges", *OECD Digital Economy Papers*, No. 252, OECD Publishing, Paris, <https://doi.org/10.1787/5jlwvzz8td0n-en>.

28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

Digital Ombudsman

There must also be effective dispute resolution pathways to enable consumers to seek redress for when things go wrong in the digital environment. As consumers increase their engagement online and with more digital products and services, a Digital Ombudsman needs to be adequately resourced to meet Benchmarks for Industry-based Customer Dispute Resolution²⁵ to ensure consumers can effectively resolve any disagreements that will arise.


Strategies embedding blockchain technology

The consultation paper currently does not touch on the potential of blockchain technology to help assist in reducing cyber security risk. The OECD notes:

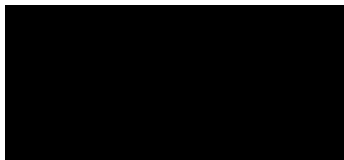
“The benefits of blockchain technology could therefore go further: assisting consumers and businesses alike by improving transparency in the supply chain and allowing participants to view and share information swiftly and confidently, and possibly bringing new angles to various issues facing actors in supply chains across the world, including for example the “country of origin” labelling or reliability of certifications.”²⁶

There is real opportunity as we build key consumer protection measures in the cyber security space to consider how blockchain technology could be embedded into business practice and in enforcement initiatives. Specifically for smart devices, blockchain technology can help establish differences between normal and abnormal occurrences in a network and help block suspicious activity.²⁷

Further engagement

We would welcome the opportunity to work with the department and sharing further insights from our consumer research projects. For further discussion regarding our research and the contents of this submission, please contact Chandni Gupta, Policy and Program Director at .

Yours sincerely



Lauren Solomon
Chief Executive Officer
Consumer Policy Research Centre

²⁵ See [Benchmarks for Industry-based Customer Dispute Resolution | Treasury.gov.au](#)

²⁶ OECD (2018), "Consumer product safety in the Internet of Things", *OECD Digital Economy Papers*, No. 267, OECD Publishing, Paris, <https://doi.org/10.1787/7c45fa66-en>.

²⁷ Arnold, A, "4 Promising Use Cases of Blockchain in Cybersecurity", (30 August 2019), [4 Promising Use Cases Of Blockchain In Cybersecurity \(forbes.com\)](#)