

Our ref: PRJ1005440

Contact officer: [REDACTED]

Contact phone: [REDACTED]



23 Marcus Clarke Street
Canberra ACT 2601

GPO Box 3131
Canberra ACT 2601

tel: (02) 6243 1111

www.accc.gov.au

27 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs
6 Chan Street
Belconnen ACT 2617

Submitted via: Department of Home Affairs [submission form](#)

**Australian Competition and Consumer Commission (ACCC) submission to
Strengthening Australia's Cyber Security Regulations and Incentives: A Call for Views
(Discussion Paper)**

The ACCC supports this review of regulations and incentives to strengthen cyber security. In summary:

- In our work in helping consumers (households and small business) to recognise and avoid scams, we see the destructive impact of cybercrime.
- While product labelling of internet connected (IoT) devices can only be part of the solution, it can help consumers make more informed purchasing decisions, and provide an incentive for business to improve cyber security of products.
- These incentives would also be strengthened by amending the Australian Consumer Law (ACL) to allow ACL regulators to take enforcement action against businesses for non-compliance with the ACL consumer guarantees, for example where an IoT device is not of acceptable quality due to its level of cyber security.
- However, ex post enforcement of the ACL can only play a small role in lifting Australia's cyber security baseline. Minimum 'security by design' requirements, which are enforced by a regulator with the appropriate expertise and resources, are needed to provide clarity for business and so that the burden does not disproportionately fall on consumers to ensure that the devices they purchase are secure.

Australia needs to lift baseline cyber security

The ACCC does not have a role in monitoring cyber security incidents but, through our work in relation to scams, we have seen the increasing impact of cyber security and cybercrime incidents on Australian households and small business. In 2020, the combined reported financial losses from scams was more than \$850 million of which \$339 million was reported to the Australian Cyber Security Centre.¹ Many scams involve or arise from disclosure of personal information. Data collected by the Office of the Australian Information Commissioner on notifiable data breaches shows concerted efforts by cybercriminals to access the personal information of Australians. Our 2021 scams report refers to the need for business and

¹ ACCC, [Targeting Scams: Report of the ACCC on Scams Activity](#) (June 2021) p 16.

government to protect personal information and increase cyber security to ensure Australia is more resilient to the threats posed by scams.²

Markets alone cannot deliver stronger cyber security

Although the ACCC cannot comment broadly on the core drivers of Australia's cyber security challenges, our digital platforms reports highlight some of the barriers identified in the Discussion Paper.

Our 2019 Digital Platforms Inquiry Final Report found that digital services are increasingly being provided to consumers at zero monetary cost in exchange for their data, and that consumers lack knowledge and control over the collection and use of their data.³ This reflects information asymmetry and the bargaining power of digital platforms, along with a lack of effective deterrence under existing consumer protection and privacy laws.⁴ While the report focuses on the impact on consumer choice (the ability to choose goods and services which meet consumers' personal preferences), the report also refers to the risk of data breaches and cybercrime from online transmission, storage and disclosure of data.⁵

Health checks for small business and IoT device labelling are part of the solution

Our engagement with small businesses about scams highlights the challenges they face in protecting themselves from cyberattacks including lack of budget, expertise and time.⁶ An Australian Government voluntary cyber security health check program for small business would be a useful resource which the ACCC could link to and promote as part of the ACCC's advice to small business on how to avoid scams.⁷

As set out in the ACCC's submission to the Productivity Commission's right to repair inquiry, product labelling schemes can also assist households and small business to make better informed purchasing decisions, and drive inter-brand competition.⁸ We recognise that product labelling is complex and that, in relation to IoT devices, further work would be needed to establish the design, prominence and obligations underpinning any labelling scheme. This should include consumer testing, and an assessment of the cost and possible market impact. However, labelling of IoT devices with information that consumers need to understand the security of the device (or, at least, the minimum period of security updates) would benefit households and small business in their IoT device purchasing decisions.

There needs to be stronger incentives for businesses to improve cyber security

As the Discussion Paper notes, the legal options for consumers to seek redress for cyber security incidents are limited.

As set out in the Discussion Paper, the ACL requires suppliers to meet certain guarantees in supplying goods and services to consumers. These include that goods (including digital goods) are of acceptable quality and fit for purpose, and that services (including digital services) are provided with due care and skill. Currently, consumer guarantees can only be enforced by individual consumers taking private action in small claims courts or tribunals.⁹ In

² Page 76.

³ These types of services extend beyond the digital platforms examined in this report. See, e.g. ACCC, [Digital Platforms Inquiry Final Report](#) (July 2019) p 449 and ACCC, [Customer Loyalty Scheme Review: Final Report](#) (December 2019) p 47.

⁴ Pages 22-26 and chapter 7.

⁵ Page 395.

⁶ E.g. ACCC, [Small business scams cybercrime forum](#) (2015).

⁷ E.g. ACCC scamwatch.gov.au: [Protect your small business](#) and accc.gov.au: Business rights & protections: [Avoiding scams](#).

⁸ ACCC, [ACCC submission to Productivity Commission's Right to Repair – Draft Report](#) (28 July 2021) p 7.

⁹ ACL Part 5-4. The ACCC has a limited ability to take representative action (s 277).

contrast to other provisions of the ACL, a failure to provide the remedies required under the consumer guarantees is not a contravention of the ACL.

Individual households and small businesses face considerable challenges in pursuing consumer guarantee claims in small claims courts or tribunals including the cost of obtaining legal advice and expert evidence. In the context of a digital good or service having inadequate cyber security, these challenges would be exacerbated by the need for technical expertise and the capacity to take action against what are often large overseas-based companies. Such proceedings are also likely to raise complex issues around: defining the 'good' or 'service' that has failed; which entity supplied the good or service to the consumer (e.g. manufacturer of the physical good, software developer, internet provider etc.); and the reasonable lifespan of software and support of the software over this lifespan. This burden would be beyond almost any consumer.

The incentives provided by the ACL for businesses to improve cyber security could be strengthened by enabling ACL regulators to take enforcement action against suppliers and manufacturers that do not provide the required remedies for non-compliance with the consumer guarantees. We support reforms that would make it a contravention of the ACL for:

- suppliers and manufacturers to fail to provide a remedy to consumers when legally obliged to do so under the ACL consumer guarantees; and
- manufacturers to fail to indemnify suppliers when legally obliged to do so, for remedies that the suppliers provide to consumers under the ACL consumer guarantees, where fault for a consumer guarantees failure actually lies with the manufacturer.

We also support the Department of the Treasury's consultation with states and territories on the ACL's application to digital products to ensure there are no unintended gaps. For example, the product safety provisions of the ACL apply only to 'consumer goods' and 'product related services'. The evolution of technology has led to increasing risks of injury or death from a cyber security breach of an IoT device. Greater clarity is needed:

- around what constitutes a recall under the ACL including suppliers using software updates to rectify a safety issue in a product; and
- to ensure the product safety provisions can address safety hazards that are caused by interconnected components such as artificial intelligence, the internet connection and data processing, particularly through cyber security breaches.

The United Kingdom (UK) is similarly reviewing its product safety laws to ensure that they are fit for the 21st century.¹⁰

More broadly, we also support the current Privacy Act Review and the need for strengthened privacy protections that can address evolving practices and technologies.¹¹ The recommendations in the Digital Platforms Inquiry Final Report included higher penalties for breaches of the Privacy Act and the ability for individuals to have a direct right of action, including the ability to bring class actions.¹²

Stronger ACL compliance incentives must be combined with other policy options

Even with the above reforms, the ACL can only play a small role in assisting to lift Australia's cyber security baseline. The regulatory response needs to include specific cyber security measures which are enforced by a regulator with the requisite cyber security expertise,

¹⁰ UK Office for Product Safety & Standards, [UK Product Safety Review: Call for Evidence](#) (March 2021).

¹¹ ACCC, [Review of the Privacy Act 1988: ACCC submission in response to the Issues Paper](#) (December 2020).

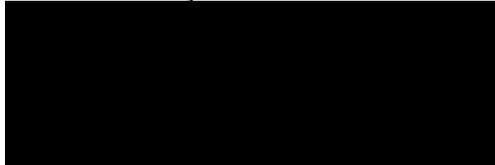
¹² ACCC, [Digital Platforms Inquiry Final Report](#) (July 2019) pp 474-476. The ACCC noted in relation to direct actions brought under the Privacy Act that a direct right of action should be accompanied by regular government monitoring to examine whether this resulted in undue difficulty for plaintiffs or undue business burden on regulated entities (p 474).

resourcing and specific mandate to improve cyber security in Australia. At a minimum, this requires a mandatory technical IoT standard to implement the principles in the Australian voluntary IoT Code of Practice¹³ relating to passwords, vulnerability disclosure policy and end-of-life policy (consistent with the UK's proposed approach).

The ACCC, through ex post enforcement of the ACL, cannot perform this role. Courts are not appropriate forums through which to develop minimum industry-wide technical standards, and cannot provide the clarity and certainty required by Australian manufacturers and suppliers. Nor can courts deal with policy issues such as alignment with international practice to minimise trade barriers. More generally, the ACCC is an economy-wide competition and consumer law enforcement agency. We can only pursue a small number of the matters raised with us, with any actions we take being determined in accordance with the priorities in our annual [Compliance and Enforcement Policy](#).

We support this review and the opportunity that it provides to address the increasing cyber security risk faced by Australian consumers. If you would like to discuss this submission, please contact [REDACTED] Executive General Manager, Consumer Product Safety Division, on [REDACTED] or at [REDACTED]

Yours sincerely

A large black rectangular redaction box covering the signature of Rod Sims.

Rod Sims
Chair

¹³ Australian Government, *Code of Practice: Securing the Internet of Things for Consumers* (September 2020).