Consumer Policy Research Centre

Level 14, 10-16 Queen Street, Melbourne, Victoria 3000

ABN 23 100 188 752 T 03 9639 7600 W cprc.org.au

2 March 2020

Submitted online via homeaffairs.gov.au

Submission to Code of Practice – Securing the Internet of Things (IoT) for Consumers

Dear Department of Home Affairs

The Consumer Policy Research Centre (CPRC) welcomes the opportunity to comment on the draft *Code of Practice—Securing the Internet of Things (IoT) for Consumers*. While the Code is a voluntary suite of measures for industry, it is an important first step to protect Australian consumers from the potential harms of IoT devices.

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.

As recent ACMA research highlights, Australia has a high rate of internet connectivity, with 91% of Australian adults having an internet connection in the home at some time, an increase from 87% in 2018. Australians are using multiple devices to go online. Of those who are online, almost two in five Australian adults access the internet via five or more different types of devices, up from one in five adults in 2017. Fifty-six per cent use four or more types of devices. Use of voice-controlled devices is also increasing: 10% of Australian adults have a voice-controlled speaker connected to the internet, up from 5% in 2018. Fifty per cent of adults are using a smart device connected to the internet, with smart TVs the most common device (used by 39% of adults) followed by wearable devices (14%). Other smart home products, such as security cameras and smart whitegoods and energy systems, are less common, used by no more than 6% of Australian adults.[1]

The total number of smart home devices in Australian households is already very high and will only increase at rapid rates. One estimate cited by ACMA suggests there are already 16 million smart devices installed in Australian homes; 47 million devices are expected by 2022.[2]

There is accordingly a clear trend towards greater IoT device use, yet Australian consumers are largely unprotected against the privacy, security and safety risks these devices introduce into our everyday lives. As the draft Code of Practice notes, 'these devices are often developed with functionality as a priority, with security being absent or an afterthought'.

There is considerable opacity around the collection, sharing and use of data from IoT devices, which brings significant risks for users and is inconsistent with Australians' attitudes

[1] Australian Communications and Media Authority, *Communications Report 2018-19*, 2020, 77-78.
[2] Ibid 52.

to data use. CPRC's survey research shows the majority of Australians are uncomfortable about data being collected and shared with third parties, including device ID numbers (84%), location data (71%) and purchase history (69%). The majority of survey respondents also considered it unacceptable for data to be used to monitor online behaviour to target advertising (52%) and charge consumers individualised/differential pricing (88%).[3] These risks arise with IoT devices if people's day-to-day lives are surveilled through the 'smart home' and the data they exchange through device use.

Our research also shows that Australians want more transparency and control in relation to how industry collects, uses and shares their data, and they expect government to regulate industry conduct in this area. For example, 73% of survey respondents agreed that the government should give consumers options to opt out of what data they can provide, how it can be used, and if it can be shared with others. Only 10% of people considered it is the individual's responsibility to check how companies are using their data.[4]

CPRC therefore supports the Code of Practice provisions requiring industry members to:

- ensure that personal data is protected in accordance with data protection laws, and that consumers are provided with clear and transparent information about the data that is being used, how, by whom and for what purposes, for each device and service, including any third parties
- give consumers the opportunity to withdraw their consent to personal data use
- make it easy for consumers to delete personal data in any circumstance, including on transfer of ownership or disposal of the device. The right to delete personal data at any time is an important protection for family violence victim-survivors and other people whose personal safety is at risk
- securely store credentials and security-sensitive data such as usernames and passwords.

However, as highlighted in CPRC's submission to Australian Government consultation on the ACCC Digital Platforms Inquiry Final Report, a Code of Practice in isolation is not adequate to protect consumers. Policy and regulation development must be integrated across the Australian Government. Not only is there a need to better coordinate efforts across the various areas consulting on digital and data regulation, consultations and input must be reflective of the cross-sectoral and inter-disciplinary nature of the challenges being posed. For IoT devices to be fully considered from the perspective of consumers, policy and regulation must be viewed through many lenses concurrently, and at a minimum this should include:

- **Transparency** – reforms to the Privacy Act (as outlined in CPRC's response to the Digital Platforms Inquiry above) to require much greater transparency about what data is being collected, who it is shared with and what it is used for.

- **Choice and control** –

    - simple and adequate information must be provided at point of sale on IoT devices about potential risks or sensitive data being collected by devices to enable consumers to make informed choices. At present, it is simply not possible for consumers to understand what risks IoT devices may pose – undermining the efficacy of consumer choice in this market

[3] Phuong Nguyen and Lauren Solomon, *Consumer Data and the Digital Economy*, July 2018, 32-34.
[4] Ibid 36-37.

  - pro-consumer defaults must be set on IoT devices requiring consumers to opt-in to data sharing, with adequate warnings provided to consumers about what data will be collected, shared and used.

- **Safety** – a general safety provision should be introduced into the Australian Consumer Law so that unsafe IoT devices do not expose people to physical and other safety risks; this also builds trust and consumer confidence in a fast-moving digital marketplace.

- **Fairness** – as CPRC has raised in numerous submissions over the past two years, lasting principles must be introduced to increase protections for consumers in an increasingly complex data and digital marketplace. Policymakers and regulators developing codes and regulations will not be able to predict and regulate each new product entering the marketplace. A prohibition on unfair trading would deliver consumers added protections ensuring general standards of fairness apply to the design and deployment of IoT devices.

- **Standards** – as a general rule, standards applying to IoT devices should enable interoperability as much as possible to ensure that consumers are not exposed to 'lock in' or the bundling of products with a small subset of suppliers.

- **Consumer guarantees and right to repair** – improved protections under the Australian Consumer Law, and greater enforcement of existing consumer guarantee provisions, to guard against strategic and untimely obsolescence of IoT devices, and the misuse of upgrade processes to prematurely end a device's lifespan. Australia should also explore the introduction of a 'right to repair' given the expensive nature of many IoT devices and increasing moves by IoT suppliers to 'brick' devices through planned obsolescence – increasing costs for consumers and unnecessary e-waste.

We urge the Department of Home Affairs to more broadly seek input from consumer and privacy experts and collaborate with relevant consumer protection agencies on this review to ensure that consumers receive integrated protections, reflective of the broader challenges posed by emerging data practices and IoT devices.

For further consideration as part of this consultation, we refer you to two CPRC research reports, *A Day in the Life of Data* and *Consumer Data and the Digital Economy*.

We would be happy to discuss these reports or any of the other matters raised in this letter. To get in touch, please contact Emma O'Neill, Research and Policy Director, on 03 9639 7600 or at emma.oneill@cprc.org.au.

Yours sincerely

Lauren Solomon
Chief Executive Officer
Consumer Policy Research Centre