5 March 2020

Emerging Technology & Market Reform Team
Security Governance & Industry Branch
Cyber Security Policy Division
Department of Home Affairs

Via email: iot.policy@homeaffairs.gov.au

ACCAN thanks the Department of Home Affairs (the Department) for the opportunity to provide a response regarding the proposed voluntary *Code of Practice: Securing the Internet of Things for Consumers*.

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.

ACCAN welcomes the Federal government's move to introduce a voluntary Code to protect consumers from the potential security and privacy threats posed by IoT connected devices. In light of the limited incentives for market-based solutions to address poor IoT security, and the information asymmetry that exists between consumers and IoT device manufacturers, there is a need for greater consumer protection. Because IoT device manufacturers often focus on price competitiveness rather than 'security by design' features in their products, this opens up potential security and privacy threats for consumers in terms of confidentiality, integrity, access control and reflection capacity. The current rollout of super-fast fifth generation (5G) telecommunications technology in Australia, which will provide the optimal telecommunications platform on which to realise IoT's benefits, means regulation of IoT device security and privacy settings is now a high priority issue.

The consumer demand for IoT connected devices - smartphones, computers, tablets and an almost limitless range of other devices - is increasing. Recent research by Telsyte predicts the average Australian household in 2023 will have 37 devices, with around half being IoT at home devices, and an estimated 64 billion devices are likely to be connected to the internet globally by 2025. At a minimum a Code of Practice regulating the IoT platform is needed to manage the privacy and security risks which are the flip-side of the benefits of IoT technology – automation, efficiency and rapid communication. However, the important work of the Department of Home Affairs will have little effect if the Code remains voluntary, with

no penalties imposed for industry non-compliance.

In 2017, UNSW conducted an ACCAN–funded research project which exposed the large-scale lack of security built into smart at-home IoT devices. All of the IoT devices tested had serious security and privacy flaws, including sending unencrypted data, using weak passwords, and lacking the security settings needed to prevent hackers infiltrating their networks and controlling the devices remotely.

There are a range of potential solutions available to manage the risks consumers face as a result of poor IoT security, from education to legislation. ACCAN hopes the government's draft voluntary Code of Practice will establish a platform for consumers, suppliers, manufacturers, regulators and insurers of IoT devices to effectively implement its principles and come together to develop appropriate strategies to mitigate risks.

The individual Principles of the draft Code of Practice relevant to ACCAN's work are responded to below.

1. No duplicated default or weak passwords

ACCAN supports the principle that duplicated or default passwords should not be permitted. Through privacy by design, users should be forced to change default passwords before using IoT devices to restrict the risk to consumers of hackers infiltratingnetworks. This approach would be consistent with the Australian Privacy Act requirement to implement a 'privacy by design' approach to compliance.

2. Implement a vulnerability disclosure policy

Every IoT connected device tested in UNSW's 2017 ACCAN-funded research project revealed some form of vulnerability, and many allowed potentially serious safety and security breaches. Manufacturers must be obliged to inform consumers who purchase IoT connected devices of the risks inherent in their design and function, and a vulnerability disclosure policy may be one effective way to achieve this outcome.

ACCAN also recommends the introduction of a 'trust' label to be included on the product packaging of connected devices. A cyber security and privacy 'star rating' for IoT devices, similar to energy or water-efficiency ratings on household appliances, would support consumers to make more informed purchasing decisions. ACCAN is currently engaged in research with Deakin University to investigate the use of labels to help consumers understand which IoT devices collect data, how data is used, shared or monetised and the level of cyber security and privacy features built into the design and operation of IoT connected devices.

3. Keep software securely updated

Consumers expect that technical security is the manufacturer's, insurer's or regulator's responsibility.. Consumers assume that manufacturers or service providers will supply any

security software updates necessary to continue securely running their applications on smart-home devices. This is a reasonable consumer expectation. It can be likened to the scenario of a new car purchase, where consumers are not expected to have the skills of a mechanic to maintain the vehicle, but are reminded by in-built car software of when to have the car serviced by experts to keep it roadworthy.

ACCAN supports the principle that software on IoT devices should be securely updatable, with security software updates distributed via secure IT infrastructure, automatically applied by default and easily installed by consumers. ACCAN agrees that manufacturers should provide an end-of-life policy at the time of purchase to inform consumers when they will cease receiving security software updates, and that vendors should tell consumers if devices cannot be physically updated and when will no longer be fit for purpose.

4. Securely store credentials and security-sensitive data

ACCAN supports the principle that credentials should be stored securely on devices and services, and hard-coded credentials such as usernames and passwords should not be embedded in device software or hardware to prevent security breaches via reverse engineering.

5. Ensure that personal data is protected

In regulating the collection and use of customer data, manufacturers of smart devices should recognise that consumers have rights over that data. Accordingly, ACCAN supports the principle that manufacturers should explain clearly to consumers in simple, easy to understand, accessible language what personal data is collected and how it will be processed and handled, including sharing data with third parties such as advertisers. Similarly, ACCAN supports the principle that properly informed, transparent consumer consent to process personal data must be explicitly obtained in a valid and lawful manner, providing consumers with the opportunity to withdraw their consent at any time.

In cases where consent to collect and process a consumer's personal data is obtained, IoT device manufacturers need to take appropriate measures to ensure the data is protected from attack, both in storage and in transmission. Security preservation and loss limitation strategies, including automatically patching security software following incidents where a breach has occurred, must be built in to the design and operation of IoT connected devices.

6. Minimise exposed attack surfaces

ACCAN agrees that devices and services should 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. IoT connected devices are often not equipped with in-built 'security by design' features, which can result in a low-level user account, device, or application being compromised. Implementing the POLP will help contain security compromises to their area of origin, stopping them from spreading to the system at large.

ACCAN supports the principle that unused IoT device functionality should be disabled, unrequired ports closed and the web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet. These measures will help restrict unauthorised access to a system due to poor access controls and minimise opportunities for hackers to launch distributed denial-of-service (DDoS) attacks on IoT devices. Similarly, use of appropriate privileges on software access, using a secure software development process and performing penetration testing will improve the security of IoT connected devices against infiltration by hackers seeking to access a local Wi-Fi network and manipulate all of the devices connected to it.

7. Ensure communication security

The integrity of IoT devices can be compromised if the communication between the device and the user's service and its associated application can be intercepted and manipulated by attackers. ACCAN supports the principle that security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage, and that all credentials and securities should be managed securely.

8. Ensure software integrity

The security frailties built into IoT connected devices make them particularly vulnerable to software attacks. Because of the sensitive data IoT devices can collect, consumers with IoT devices connected at home are at risk of both privacy and security breaches. Most consumers assume that manufacturers or service providers will supply any software updates necessary to continue running their applications, and ACCAN agrees that updating security software should not be the obligation of the consumer but should be the responsibility of the IoT device manufacturer.

9. Make systems resilient to outages

ACCAN supports the principle that, taking into account the possibility of outages of data networks and power, resilience should be built into IoT devices and services. IoT devices and services should remain operating and locally functional in the case of a loss of network, without electronic security protocols - network security, application security and information security – being compromised. Uninterrupted power supply should be built into the design of IoT connected devices – for example, a backup battery or other emergency power source - to maintain operational continuity.

'Clean' recovery after a power or network outage is particularly important in the case of consumers with disabilities who may rely upon IoT devices to increase their independence. For example, consumers with limited mobility may automate their home with assistive technologies so they can turn lights on/off and control heating or cooling remotely. After power and network outages, IoT connected devices need to return to the features and functions installed by a customer so that they don't need to be reprogrammed. The resilience of IoT connected devices, and their ability to return to the settings installed prior to outage, is vital to adequately support independently-living consumers with disability.

11. Make it easy for consumers to delete personal data

Europe's GDPR (Art. 17) has enshrined the consumer right to delete personal data in 'the right to erasure' or 'right to be forgotten'. In 2015, the Australian Law Reform Commission (ALRC) similarly recommended that a "right to deletion of personal information" be inserted as an amendment to the Privacy Act as another APP, although this recommendation has never been implemented.

In the absence of a GDPR equivalent provision in the Australian Privacy Act and Australian Privacy Principles, Principle 11 of the Code is a positive step towards providing consumers with some limited ability to control the use and retention of their data. For consumers living with disability, consumer instructions on how to delete personal data from devices must be fully accessible to enable them to exercise the same control over the use and retention of their personal data.

12. Make installation and maintenance of devices easy

A distinct information asymmetry exists between consumers and manufacturers of IoT devices. ACCAN supports the principle that the installation and maintenance of IoT connected devices should follow security best practice, be easy for consumers to install and maintain, and that device installation instructions should contain clear, straightforward and accessible consumer guidance on how to securely set up a device and maintain it through its lifecycle.

To make installation and maintenance of IoT connected devices easy for people with disability, these devices should be sold with accessible settings fixed by default. Typically, devices are set to operate by default without accessibility features enabled. However, it is more practical for people without impairment to re-set a device to operate with no accessibility features than it is for someone with an impairment to set up accessible features on their device. IoT devices therefore need to be accessible 'straight out of the box'.

Conclusion

ACCAN again thanks the Department for the opportunity to provide a response regarding Australia's draft voluntary Code of Practice: Securing the Internet of Things for Consumers. We hope that consumer concerns and experiences will be prioritised within the actions of the Federal government's approach to regulating the Internet of Things in the interests of consumer protection, and encourage the Department to continue to engage with consumers and their representative bodies as the Code is implemented.

Sincerely

Stephanie Whitelock

Policy Officer