Australian Government

Department of Home Affairs

Draft Code of Practice: Securing the Internet of Things for Consumers

Summary of Public Consultation

November 2019 – March 2020

Contents

Executive Summary

This report summarises the outcomes of public consultation to inform development of Australia's *Code of Practice: Securing the Internet of Things for Consumers.* Your feedback could not have been clearer — the Code of Practice is a good first step to lifting the security of internet-connected devices for consumers. This message was consistent across the country and from all stakeholders groups.

While noting the cyber security in the Internet of Things (IoT) is a global challenge, you also told us that there are more steps that the Australian Government and industry can take to better protect Australian consumers from insecure internet-connected devices.

There were strong calls for the greater introduction of standards, whether on a voluntary or mandatory basis. There was a widespread view that baseline cyber security needs to be built into goods and services 'by-design' as most consumers aren't best placed to protect themselves.

Feedback also suggested that the Australian Government cyber security effort needs to align with international efforts to ensure a harmonious approach.

Summary of Consultation Process

The Australian Government conducted stakeholder consultation to support the development of the Code of Practice between 19 November 2019 and 1 March 2020.

The draft Code of Practice was posted on the Department of Home Affairs website on 19 November 2019. Home Affairs received a total of 39 formal written submissions. The submissions reflected the views of over 4640 organisations from all sectors, including critical infrastructure providers, cyber security companies, governments, domestic and international consumers and other not-for-profit advocacy groups.

A wide variety of stakeholders also took part in workshops held across the country. Workshops were held in most states and territories; Brisbane, Sydney, Melbourne, Perth, Adelaide and Canberra.

This was complemented by consultation on the 2020 Cyber Security Strategy that ran between 6 September 2019 and 1 November 2019. More than 1,000 people took part in the Strategy events held in each state and territory and more than 213 submissions were received on the Strategy; with many of the discussions and submissions making reference to the security of the Internet of Things.

Referencing note: this report is based on all feedback received throughout the consultation process. It aggregates messages from in-person workshops and both public and confidential written submissions. Though information from confidential submissions has been used to inform the summary, no direct references have been made. References are included as a non-exhaustive list of examples.

Your Feedback

The Code of Practice is a welcomed first step

Across the nation, there was consensus that the Internet of Things represents enormous potential benefits for governments, businesses and consumer. However it also represents a significant challenge in terms of cybersecurity.[1]

Many stakeholders noted the increasingly interconnected and co-dependent environment of the Internet of Things. As new 5G technologies come online, Australian consumers are largely unprotected against the risks these devices introduce into our everyday lives.[2] As a result, much of the feedback we received – both in person and via written submissions – was supportive of the Code of Practice as a good first step towards lifting the security of the Internet of Things in Australia.

The Consumer Electronics Suppliers Association noted that Australia is largely an importer of internet-connected devices.[3] Palo Alto Networks stated that they are pleased to see the Australian Government taking action to address IoT security, particularly as the number of internet-connected devices globally is set to reach 64 billion by 2025.[4]

The Consumer Policy Research Centre stated *'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'.

Cyber CX expressed that the Code of Practice is '*an important step forward in ensuring consumers are able to benefit from IoT devices in a secure manner. As internet enabled and connected devices become increasingly commonplace in Australian households and workplaces, it is timely for the Government to give careful consideration to the range of information security and privacy implications that will arise with the rapid uptake and adoption of the IoT'*.[5]

Cisco Systems Australia stated an effort such as this to introduce standards was encouraged.[6] Telstra also noted that the Code of Practice was an important first step '*in helping define and agree on the principles that will underpin a secure IoT ecosystem and build a baseline level of security across Australian industry, to maintain an ecosystem that is safe and trusted for consumers and businesses'*.[7]

Google and YouTube stated that, *'we think [the Code of Practice] offers a useful, principles-based approach to codifying best practice when it comes to device security. Adopting a principles-based approach allows businesses of all shapes and sizes to interpret the principle in the way that makes most sense for their products and business*'.[8]

Australian Industry Group stated *'we support a security-by-design approach supported by principles, with the ultimate objective of protecting Australia's cyber security'* and also welcomed a voluntary approach at this stage, stating *'we believe this approach will create a flexible environment for all stakeholders to shape and implement best practices in a collaborative manner'*.[9]

Although many respondents were supportive of the Code of Practice, some stakeholders pointed to its constraints. Some felt that the Code of Practice could be strengthened by adding more weight to consumer

---

[1] *Cisco Systems Australia Pty Ltd, IoT Alliance Australia, Office of the Australian Information Commissioner, Palo Alto Networks, raised in the majority of Code of Practice workshops held across the country.*
[2] *Amit Singh Gaur, Consumer Policy Research Centre, Cyber CX.*
[3] *Consumer Electronics Suppliers Association.*
[4] *Palo Alto Networks.*
[5] *Cyber CX.*
[6] *Cisco Systems Australia Pty Ltd.*
[7] *Telstra Corporation Limited.*
[8] *Google Australia Pty Ltd.*
[9] *Australian Industry Group.*

privacy,[10] increasing public awareness on cyber hygiene and device security,[11] giving more consideration to security at the network level,[12] providing more clarity on roles and responsibilities of device manufacturers and service providers,[13] adding a Principle on a Security Trust Mark[14] as well as increasing supply chain security.[15]

Global alignment is important

Many stakeholders raised the importance of global alignment. A large number of respondents highlighted that the security of our homes depends on the cooperation and collaboration between governments, industry, and citizens from all around the globe.[16]

The IoT Alliance Australia stated *'We commend the Australian Government for the creation of the Draft Code of Practice, and for its close alignment with the UK Government's code of practice. We believe it is important that such codes are aligned across the five-eyes nations, and we believe the creation of the code is an important step in improving IoT security for consumers (and businesses) in Australia'.*

Palo Alto Networks welcomed the fact '*that the Draft Code takes a global approach, aligning with the UK Government's Code of Practice for Consumer IoT Security, as well as European Telecommunications Standards Institute's Cyber Security for Consumer Internet of Things. Creating a unified approach is beneficial for global businesses'.*[17]

The Office of the Victorian Information Commissioner (OVIC) noted that international pieces of work such as the International Organisation for Standardization (ISO)'s ISO/IEC 27030 standard and SC 27 committee, can demonstrate the significance and importance of global IoT security and privacy. OVIC recommended the Code of Practice reference more international work on IoT security such as these, in order to give the Code of Practice additional weight.[18]

Other individuals and state governments were pleased to notice alignment with international guidance and domestic cyber strategies, recommending '*states and territories continue to coordinate closely*' and build upon the UK's and USA's approaches.[19]

---

[10] Australian Communications Consumer Action Network, Confidential Submission 3, Confidential Submission 4, Confidential Submission 10, Consumer Policy Research Centre, CryptoPhoto.com Pty Ltd, Darkmatter LLC, Kate Matthews-Hunt, Office of the Victorian Information Commissioner.
[11] Amit Singh Gaur, Consumer Policy Research Centre, Rajinder Rathor, Ross Wacker, Steven Abrahall.
[12] Cisco Systems Australia Pty Ltd, Iot Alliance Australia, Palo Alto Networks, Rajinder Rathor.
[13] Confidential Submission 5, Iot Alliance Australia, Telstra Corporation Limited.
[14] Australian Communications Consumer Action Network Communications Alliance Ltd, Australian Rail Track Corporation, IoT Alliance Australia, Steven Abrahall.
[15] Australian Industry Group, Communications Alliance Ltd, IoT Alliance Australia, Palo Alto Networks, Security Solutions.
[16] Australian Industry Group, Christian Heinrich, Confidential Submission 7, Confidential Submission 8, Consumer Electronics Suppliers Association, CryptoPhoto.com Pty Ltd, Kate Mathews-Hunt, Office of the Victorian Information Commissioner, Security Solutions.
[17] Palo Alto Networks.
[18] Office of the Victorian Information Commissioner.
[19] Confidential Submission 6, Confidential Submission 9.

More action is required

Mandatory standards

We received a number of calls for the Australian Government to introduce mandatory security standards for internet-connected devices. From across the nation, stakeholders told us that minimum standards need to be put into place as it is often the consumer, rather than the manufacturer, who suffers the greatest loss from these devices.[20]

Some stakeholders noted that many manufacturers cut costs by not supporting their devices with security updates and that it is hard to distinguish these from devices produced by more reputable manufacturers with better, ongoing support.[21]

Regulation

A large number of stakeholders called for stronger regulation which would enforce devices to be secure-by-design.[22] Many respondents suggested that compliance with these minimal requirements would need to be publicised clearly and transparently on products (e.g. through a 'traffic light system') for consumers.[23]

Some stakeholders also supported regulatory approaches to:

- The security and privacy lifecycle of devices;
- Vulnerability reporting and disclosure policy;[24]
- The transparency of data collected and used by devices;[25]
- Enforcement of regular internal and external audits;[26]
- Imposing penalties on non-compliance.[27]

Some took a different view, arguing that it was important for the principles to remain voluntary and that industry should be responsible for best cyber security practices and standards.[28]

Labelling scheme

A popular suggestion was that mandatory standards could include a labelling scheme for IoT devices, which would highlight the level of cyber security a product may have, helping businesses and consumers make more informed choices.[29] CryptoPhoto stated that '*it should be the job of companies that provide services to Australians to comply with and offer sensible cybersecurity protections'.*[30]

The need for effective public education and incentives for businesses were also raised by many stakeholders.[31] James Manner stated '*The code covers the basics of good engineering practice which is a step in the right direction. However, my fear is it will have little effect as the biggest driver of change is*

---

[20] Confidential Submission 3, Confidential Submission 6, Office of the Victorian Information Commissioner, Rajinder Rathor, Synod of Victoria and Tasmania, Uniting Church in Australia, raised in the majority of Code of Practice workshops held across the country.
[21] Confidential Submission 1.
[22] Australian Industry Group, Amit Singh Gaur, Rajinder Rathor, raised in the majority of Code of Practice workshops held across the country.
[23] Confidential Submission 6.
[24] Confidential Submission 3.
[25] Kate Matthews-Hunt.
[26] Amit Singh Gaur, CyberCX.
[27] Australian Communications Consumer Action Network.
[28] Australian Industry Group, Consumer Electronics Suppliers Association.
[29] Cisco Systems Australia Pty Ltd, Confidential Submission 1, Confidential Submission 7, Confidential Submission 9, CryptoPhoto Pty Ltd, IoT Alliance Australia, Steven Abrahall.
[30] CryptoPhoto Pty Ltd.
[31] Australian Industry Group, Confidential Submission 5, Confidential Submission 9, CryptoPhoto Pty Ltd, Digital Risk Innovation, Rajinder Rathor, Ross Wacker, Telstra Corporation Limited.

consumer behaviour. Without demand or awareness of security issues by consumers, there is no commercial imperative to improve product security'.[32]

[32] *James Manner.*

Specific Feedback on Principles

Principle 1 – No duplicated default or weak passwords

The Australian Communications Consumer Action Network '*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 infiltrating networks. This approach would be consistent with the Australian Privacy Act requirement to implement a 'privacy by design' approach to compliance.'*

Cisco Systems Australia Pty Ltd noted '*The reality of consumer devices is that passwords are forgotten. All devices at some stage need a recovery option, and in many cases the only reliable option is a default state. There is huge value in devices not being left in operation with default passwords. It is recommended this be altered to state that all administrative passwords be forced to be changed in order for a device to be operational. Multi-factor authentication is fast becoming a critical capability where users interact with services. This should be encouraged in the section*.'

Cyber CX highlighted *'There is a risk that this principle will be difficult to apply within the consumer space. One option would be to require consumers to reset a default password on first access.'*

FermyMate stated '*I do not find this appropriate from a development perspective, simple devices such as IoT microcontrollers which I have vast experience with, would be very cumbersome to develop that on a hard-reset would be unique usernames and passwords. This is unfeasible from a mass production perspective as would require unique firmware code to be burnt onto each device. The standard operation for IoT devices is a 3rd party setup such as on mobile phone is used prior to connection to the cloud service and therefore the connectivity from IoT end device to internet cloud is never using a default username/password combination*.*'*

Office of the Victorian Information Commissioner noted '*Principle 1 concerns the security of IoT passwords. To reduce the likelihood that a password reset process could be used to gain unauthorised access to an account, we suggest Home Affairs considers including a requirement that password reset processes reasonably authenticate users*.'

Palo Alto Networks '*agrees with this principle, which encourages device manufacturers to avoid factory default passwords that are common to multiple devices and/or are predictable (i.e. 2345678). Many consumers do not change these passwords, are unaware of how to change them or the passwords can be easily reset to default passwords, exposing not only the device but other devices on the network to cyberattack*.'

Telstra Corporation Limited recommended '*a minor revision to this principle. As the implementation of similar requirements for device passwords tends to be algorithmic and access to the algorithm can result in the regeneration of a 'unique' password, this Principle should be revised to state that passwords should be 'randomly generated'. In addition, where a consumer changes their password to one that is common, easy to guess or breach, the Device Manufacturers and Service Providers should not be held responsible*.'

Principle 2 – Implement a vulnerability disclosure policy

The Australian Communications Consumer Action Network (ACCAN) stated that '*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.'

Cisco Systems Australia Pty Ltd recommended that '*The key items this should address are a) a vulnerability point of contact and process for new vulnerabilities to be disclosed discussed, b) a vulnerability disclosure/publication with appropriate CVSS classification and c) a vulnerability remediation within an acceptable timeframe provided a product is within a published support lifetime for security fixes. Our example can be found here*.'

Jukka Rannila noted that '*There are different services for reporting different information technology problems/issues; for example 1) CERT – global and national teams 2) Common Vulnerabilities and Exposures (CVE) 3) Scamdex 4) The Spamhaus Project. At the moment there is just not one global system for informing all possible problems related to information technology. Proposal: There should be just one (Australian?) system for informing all possible problems related to information technology. At the moment there are too many global and local services for informing different information technology problems.'*

Christian Heinrich stated '*Data Validation must occur at both input and output rather than be limited to input received from the consumer only. The need to prioritise a Vulnerability Disclosure Program (VDP) should be lowered due to the increased noise of correspondence related to "low risk" vulnerabilities.'*

Palo Alto Networks '*is supportive of this principle and agrees that establishing clear processes by which researchers and/or third parties can report vulnerabilities for action is key in preventing cyberattacks. However, we note that vulnerability disclosures must be coordinated. Thus we recommend amending the language of this principle to "Implement a Coordinated Vulnerability Disclosure Policy."*

In coordinated vulnerability disclosure, vulnerabilities are reported to the owner of the information system, affording the organisation the opportunity to diagnose and remedy the vulnerability before detailed information is disclosed to third parties or the public. This helps to minimise opportunities for cyber criminals to exploit these vulnerabilities. As the complexity of, and dependency on, ICT products and services is increasing, and cyber criminals continue to become more sophisticated, vulnerabilities are also increasing. Cooperation between those who might find a vulnerability and those who can fix it is invaluable—and all societies reap the benefits of a more secure digital infrastructure.'

Telstra Corporation Limited stated '*Telstra endorses and follows this principle. We provide a public point of contact where issues can be reported. We recommend this principle should also be amended to elaborate on how best to enforce the disclosing of vulnerabilities and ensuring they are rectified in a timely manner, perhaps through the creation of an explanatory supplement*.'

Principle 3 – Keep software securely updated

The Australian Communications Consumer Action Network (ACCAN) noted that *'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.'

The Australian Industry Group highlighted that '*Some companies may already implement the automatic update recommendation as a best practice in their products and services. However, there may be circumstances where users will need to take affirmative steps to deploy a security update e.g. an operating system update that includes a security update in amongst other changes. Clarity should also be provided around expectations specifically on critical security updates*.'

Cisco Systems Australia Pty Ltd recommended that '*Patching mechanisms should be automated for all consumer devices, requiring no user intervention or action for security updates to be applied.*'

Cyber CX noted *'When a device reaches its end-of-life, this should be clearly visible in the management interface. If vendors simply notify users via email or through the manufacturer's web site, there is a risk that consumers won't be aware and they could be left with a device that is vulnerable to exploitation.'*

The Consumer Electronics Suppliers Association stated '*An important element in reducing the risk is to build effective cyber security into devices. As many IoT devices operate in Class Licensed spectrum (public park) it is vital that appropriate protections are incorporated at the design stage*.'

FermyMate suggested '*The above statement contradicts itself. It states "Updates should also not change user-configured preferences, security or privacy settings without prior approval from the user"… followed by "..updates should be easy to implement and applied automatically by default". How can a feature change on functionality be implemented requiring consent and then be automatic by default? Either it's a manual with consent or automated approach?'*.

Google Australia Pty Ltd highlighted that *'this is definitely a best practice and one that we put into practice across all of Google's products and services. However, we note that there may be circumstances where users will need to take affirmative steps to deploy a security specific update. For instance, an Android operating system update that is accompanied by a security update may require user consent to install the additional security update. Can we also suggest that the requirement that updates should not change user configured preferences without prior approval make an exception for necessary security purposes? In addition, we think it makes more sense to refer to an end of life "support" policy; our thinking being that consumers are ultimately most concerned about obtaining support for their devices'.*

IoT Alliance Australia noted that '*It may not be possible for a device manufacturer to update software in a device where that devices sits behind a hub or gateway (such as a Smart Home), as the device may not be openly visible across the internet. This therefore requires Device Manufacturers and IoT Service Providers to work together to enable timely and secure updates to multi-layered IoT offerings such as Smart Homes, tracking/locator services and some smart toys*.

Principle 3 says "Software (including firmware) on IoT devices … should be securely updatable." We understand this to mean that where the capability exists in an IoT device or solution for software and/or firmware to be updated, then it must be done securely, and we support this.

However, we caution against inadvertently creating a mandate that all devices, regardless of their function or use, should have the ability to be updated. Any device capable of accepting either a software or firmware update remotely, has an increased attack surface. This then requires appropriate levels of security to prevent rogue actors updating the device or solution, thus adding complexity and cost.

We acknowledge that Principle 3 contemplates "constrained devices" (devices that cannot physically be updated), demonstrating the Department is aware that some devices can never be updated (potentially making them more secure). In the same way Principle 7 on communication security includes the phrase "appropriate to the properties of the security technology and usage" in acknowledgement that some devices (e.g. a weather sensor), we suggest words are added to the first sentence of Principle 3 to say "… should be securely updatable appropriate to the properties of the security technology and usage".'

Jukka Rannila stated '*Here I note that there can be several standards implemented in different systems when maintaining different systems'*

Office of the Victorian Information Commissioner highlighted '*One aspect of Principle 3 is the lifecycles of IoT devices. Lifecycle issues such as ongoing support for devices and end of life policies are of critical importance. For example, devices that cease receiving security updates can pose significant security risks, especially when the owners are unaware that updates have ceased. To highlight the importance of IoT lifecycles, we suggest Home Affairs considers separating the topic of lifecycles from Principle 3 and making it a standalone principle.*

Another part of Principle 3 involves providing a range of information to users: end-of-life policies, reasons for updates, notifications if updates will no longer be provided, and warnings when a constrained device is no longer fit for purpose. As consumer IoT devices are predominantly consumer goods, it is reasonable to expect that some devices will have multiple owners throughout their lifecycles. For this reason, we suggest this principle should encourage IoT manufacturers to endeavour to provide the above-mentioned information to the current owner of an IoT device, noting that the original owner will not necessarily be the current owner. To accomplish this, devices should have an easy way for users to transfer ownership of the device.

For devices such as IoT whitegoods, which may be used for decades, it is likely they will be used long after support for the device's software ceases. In cases where the lifecycle of an IoT device's hardware and the lifecycle of that device's software differ, organisations should ensure that measures are put in place to see that, where appropriate, information is adequately destroyed and that the device disconnects from unnecessary services. For example, data stored on a device may no longer be necessary after an online service ceases operating, and data stored in the cloud may not be needed after a device is retired. This is also relevant to Principle 6, in that connections to the cloud should be securely disconnected where appropriate.'

Palo Alto Networks agreed that *'The ability to update software (including firmware) on IoT devices is important in maintaining the security integrity of these devices. As noted in the Draft Code, it is important that these updates are 1) timely and do not impact functionality, and 2) easy to implement and applied automatically by default, removing the manual intervention required by consumers who often forget or do not understand the importance of updates. It is also critical that IoT device manufacturers communicate the end of life policies so that the consumer knows the minimum length of time for which a device receives updates and that the manufacturer warns consumers when the product will no longer be supported and what the consequences of this are*.'

Telstra Corporation Limited stated '*Telstra supports the intent of this principle, however recommends it would benefit from further clarity (perhaps in an explanatory supplement) in the roles of Device Manufacturers and Service Providers who will need to work together to implement this principle. Service Providers may find it difficult to bear responsibility for the updating of software for devices they do not manufacture, despite providing connectivity. Similarly, Device Manufacturers may not have the ability to directly communicate with their devices if they sit behind a gateway or some other type of network (i.e., the address of the IoT device may not be directly visible from the Internet).*

The principle also requires that the need for each update should be made clear to consumers. We note that where devices are on-sold by a service provider (for example, a smart-home solution) the Device

Manufacturer may have no knowledge of the contact details of the consumer to advise them of the need for an update. In addition, we suggest that 'timely' is not clearly defined and that it be replaced with "implemented to meet vendor's suggested remediation timeframes".'

Principle 4 – Securely store credentials and security-sensitive data

The Australian Communications Consumer Action Network '*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.'*

Cisco Systems Australia Pty Ltd recommended that '*Security sensitive information perhaps needs better definition. Passwords, credentials and encryption keys, as well as personally identifiable, or financial information must be included. Secure storage also should be defined. TPM chips are an example of a hardware mechanisms for storing keys and other information that can then be used to for encrypted storage that should be used for sensitive data. Hardware mechanisms such as this are important, however not all devices will be able to achieve this. Another key aspect that should be considered here that is missing is simple and effective removal of all data from a device and/or associated services. For consumers, this minimizes potential data loss when disposing.'*
Palo Alto Networks agreed that '*credentials should be stored securely within devices and on services, and that hard-coded credentials should not be embedded in device software or hardware, as they are easily discoverable via reverse engineering. We further recommend that devices contain the ability to restrict the access of manufacturers (whether original equipment vendors or contract manufacturers) to devices' credentials, personal information, and other sensitive information, to avoid supply chain attacks. Unfortunately, cyber adversaries, including nation states, have been known to try to infiltrate factories to plant "back doors" into devices. Consequently, devices should allow new consumers to have the ability to wipe vendors and manufacturers access, if the device's functionality allows such access.'*

Telstra Corporation Limited stated '*Telstra endorses this Principle. There are methods through which credentials can be stored on the device without being discoverable through reverse engineering; for example, signed certificates can be generated on a secure cloud platform, these certificates can then be securely shared with the vendor and installed onto the device as part of the manufacturing process*.'

Principle 5 – Ensure that personal data is protected

The Australian Industry Group recommended that '*This proposal should also consider including regular reviews on who has access to data and personal information, and to limit access to confidential and sensitive information. In addition, we recommend this principle specifies that password reset processes should not disclose unnecessary information to the individual requesting the reset until that individual has been reasonably authenticated. For example, in the case of a reset process that sends an SMS message to a mobile phone associated with a device, this device should not display the mobile phone number as the requester may not be the individual who owns the device*.'

The Australian Communications Consumer Action Network (ACCAN) noted that *'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.'

Cisco Systems Australia Pty Ltd said that '*Consumer privacy is of key concern. Consent should be separate to any other user acceptance and be positive consent requiring user action.'*

Darkmatter LLC stated '*Most of the consumer devices are now connected to internet and synced in to the related software applications that continuously updating. Regardless if the data are being encrypted, we need to make sure that consumer data are not being captured or backed up somewhere else. Part of the most marketing strategy now to broaden their business is to generate leads which mostly done through websites or even simply buying a sim card. Most of our fellow citizens are being scammed and it is still increasing its number.*'

The Office of the Australian Information Commissioner (OAIC) recommended that Principle 5 be amended to make reference to privacy by design and require privacy settings are set to privacy protective by default. They recommended Principle 5 be *'amended to include that notices directed at children are written at a level that can be readily understood by the minimum age of the permitted device or service user, children's consent should be obtained from the child's guardian, and express and up to date consent should apply to the collection of sensitive information including health information and biometric data'*.

OAIC also recommended that Principle 5 be *'amended to refer to data minimisation principles that apply to IoT service providers, mobile application developers and retailers, that they only collect the minimal amount of personal information required to carry out their functions or activities and take reasonable steps to destroy or de-identify personal information that they no longer need for any purpose for which the information may be used or disclosed under the APPs'.* They also stated *'The Department of Home Affairs should amend Principle 5 in the draft code to restrict the use of targeting, profiling and surveillance with IoT devices that are marketed at children'.*

The Office of the Victorian Information Commissioner noted '*Principle 5 includes a requirement that consent be valid, lawfully obtained, and can be withdrawn. While we strongly support this, we note that in order for consent to be valid, it must be a genuine, voluntary choice. If an individual must choose between giving consent or not being able to use a device they own, or if withdrawing consent renders a device inoperable, then that consent may not be voluntary and therefore invalid. Because of this, we suggest Principle 5 recommends that when consent is not provided or is withdrawn, devices remain as functional as possible without using personal information.'*

Palo Alto Networks *'supports the protection of personal data and notes that security is essential to enable privacy.'*

The Synod of Victoria and Tasmania, Uniting Church in Australia suggested that '*Under principle 5, children should not be able to provide their consent to be marketed to or for their data to be harvested for commercial purposes. The device or software provider should be required to verify that the user is not a child.*

Further, under this principle, if the service provider or retailer plans to sell a person's data to a third party, they should be required to obtain the consent of the person. The person should be informed of an estimate of how much their data will be sold for and for what purpose. The provision of services should not be contingent on a person consenting to allowing their data to be sold to third parties.'

Telstra Corporation Limited '*endorses and follows this principle*'.

Principle 6 – Minimise exposed attack surfaces

The Australian Communications Consumer Action Network (ACCAN) agreed 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.'

The Australian Industry Group noted that '*Depending on how aggressively the TOLA Act is invoked by law enforcement, security and intelligence agencies, it may be difficult to meet these principles.'*

Palo Alto Networks '*agrees with this principle, which recommends that devices and services should operate on the 'principle of least privilege'. We note that this principle is complemented by a Zero Trust architecture rooted in the principle of "never trust, always verify". Under the Zero Trust concept, an organisation should not automatically trust any unauthenticated activity inside or outside its network perimeters. Instead, an organisation must authenticate anything and everything trying to connect to its systems before granting access, including IoT devices. That level of granular control around key critical infrastructure and data allows for management of cyber risk much more effectively. We recommend Zero Trust as a best practice for operators to effectively secure a 4G environment that is IP end-to-end, which then allows a safe and secure transition to a 5G environment, where an open standards-based architecture will dominate.*'
Telstra Corporation Limited stated '*Telstra supports the intent of this principle, however recommends it would benefit from further clarity (perhaps in an explanatory supplement) in the roles of Device Manufacturers and Service Providers. For example, Service Providers may not be responsible for ensuring that unrequired ports on a particular device are closed as this is a function that the Device Manufacturers would most efficiently perform. Similarly, Device Manufacturers may not be responsible for reducing code in a gateway or network hub to the minimum functionality necessary for both devices and services to operate.*

We note that techniques such as penetration testing may be employed (and prove useful) where Service Providers want to ensure the Device Manufacturer has complied with security standards. Penetration testing should also be conducted by the Device Manufacturer so as to ensure the testing is most effective, as the manufacturer would have the best knowledge of the product, its functions, capabilities and vulnerabilities.'

Principle 7 – Ensure communication security

The Australian Communications Consumer Action Network (ACCAN) highlighted that '*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.'*

The Australian Industry Group noted that '*Depending on how aggressively the TOLA Act is invoked by law enforcement, security and intelligence agencies, it may be difficult to meet these principles*.'

Cisco Systems Australia Pty Ltd recommended that *'Encryption used should also be a non-proprietary, publicly accepted algorithm with key length of currently acceptable minimum standards Legacy/outdates protocols should be updates as part of the support lifecycle of the device*.'

Palo Alto Networks '*agrees with this principle and the importance of encrypted communications while in transit. However, we suggest that to ensure true communication security, the Principle also includes a reference to the security imperative of having complete visibility of all threats. ISPs and network owners need to have visibility of threats on their network, including the ability to detect and address malicious encrypted traffic in transit, to be able to enforce a preventative security action. This can complement the use of proper end–to-end encryption (IPSEC). IPSEC should be expected on critical segments of the network, as it provides security against tampering of data travelling through the network. However, IPSEC does not provide visibility into whether the encrypted traffic passing through the encrypted tunnel is malicious or not.*

Cybersecurity threats regularly traverse mobile/ISP networks, including those leveraged by IoT devices. Cybercriminals continue to introduce and update new attack tools, such as using automation and exploit toolkits, leveraging the cloud, attacking mobile operators' infrastructure, communication tunnels, and also their end users (consumers and enterprises). Networks are a vantage point leveraged by attackers, and until we improve our ability to detect and prevent threats passing through these networks, the volume of attacks will only increase.

We would also recommend that companies consider segmenting their networks where IoT devices are deployed. Companies which apply micro-segmentation of devices based on device risk profiles are more likely to avoid cross-infections between IT and IoT systems. Through segregating and limiting the ability of legacy, low-patched and generally high-risk devices to communicate with other IT assets, companies can avoid threats spreading across their networks.'

Telstra Corporation Limited stated '*Telstra endorses and follows this principle and agrees that Service Providers and Device Manufacturers, where appropriate to the technology and use-case, should secure the communications that transit their networks, including the encryption of data in transit and the secure management of credentials and certificates.'*

Principle 8 – Ensure software integrity

The Australian Communications Consumer Action Network (ACCAN) noted '*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.'*

Cisco Systems Australia Pty Ltd highlighted that '*Software and firmware that is downloadable verifiable cryptographically, and verification mechanisms performed prior to any loading.'*

Telstra Corporation Limited '*supports the intent of this Principle. We suggest amending this Principle to include a statement about checking the integrity of software updates. An example of this is ensuring that patches are signed.'*

Principle 9 – Make systems resilient to outages

The Australian Industry Group suggested '*This principle may require support capabilities being implemented in the broader network ecosystem to monitor devices for resilience, availability and end-to-end observability, and to deploy self-healing measures in case of observed failure.*'

Cisco Systems Australia Pty Ltd stated '*The consumer space has varying requirements for resiliency. Mandating resiliency mandatory comes with potentially an unnecessary cost. These are device/service features that may be completely unnecessary. If any verbiage needs to be here, perhaps transparency about the resiliency capabilities is more suited to being a requirement.'*

Telstra Corporation Limited noted that *'Telstra supports the intent of this principle, however we recommend it would benefit from rewording the principle slightly to make it clear the default assumption should be that devices will struggle to restore cleanly and correctly. In our experience, many smaller devices may not have the ability to be restored, especially tiny devices which can be thrown away, for example, an RFID tag on product packaging or a delivery box. As such, resilience planning by the Service Provider should assume devices may fail and go rogue. The focus should be on how to restore the service, possibly including replacing and rebuilding devices, from that baseline.'*

Principle 10 – Monitor system telemetry data

The Australian Communications Consumer Action Network '*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.

Cisco Systems Australia Pty Ltd highlighted '*The value of telemetry data for security purposes is undeniable. In many cases, vendors collecting telemetry data, however may be more of a risk than not monitoring the telemetry. We suggest this be moved to requirements around logging of access, especially administrative access.'*

Cyber CX suggested *'This should be opt-in. User should be able to know exactly what data is being transmitted and have the ability to easily disable the function when they wish.'*

Telstra Corporation Limited stated that '*Telstra supports the intent of this principle, however recommends it should only apply to the Service Provider. Monitoring telemetry data for security anomalies requires advanced capabilities such as pattern matching to determine when it has been compromised. Even something as straight-forward to detect as when a device has been co-opted into "bot-army" for a DDOS attack, requires a reasonable level of sophistication, analytical capability and power consumption, when often the device (e.g., a sensor) is trying to achieve both low-cost and low power consumption.*

We recommend this principle should mainly apply to Service Providers, who are better placed to monitor telemetry data for signs that the IoT service or device has been compromised, although it may be possible for device manufacturers to monitor for anomalies in some instances.'

Principle 11 – Make it easy for consumers to delete personal data

The Australian Communications Consumer Action Network noted that '*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.'

The Australian Industry Group recommended that '*The scope of this principle should be broadened to contemplate de-identification rather than simply deletion – de-identification is important for business retention of data. As the principle currently reads, the scope could be misinterpreted or taken beyond cases of personal device transfer of ownership*.'

Cisco Systems Australia Pty Ltd stated '*This is an important issue that belongs in section 4, or appropriate section managing deletion of ALL data from device and related services. However when it comes to cloud data, data ownership and removal can be covered in the personal data protection section 5.'*

The Office of the Australian Information Commissioner suggested '*Consideration be given to amending Draft Principle 11 to require devices and services to be configured to enable the easy and secure transfer of personal information to another device or service when there is a transfer of ownership or as directed by the individual*.'

Office of the Victorian Information Commissioner stated '*Principle 11 states that devices and services should be configured so that personal information can be easily deleted. We strongly agree with this principle as it provides customers with greater control over their personal information. However, to ensure devices are properly sanitised, we suggest that this principle specifies that data should be securely and permanently deleted when the ownership of a device is transferred, or by request if the user's device is stolen or misplaced. As noted above, this would require device manufacturers to provide users with an easy way to transfer ownership of devices.*

In addition, rights to have personal information deleted are often accompanied by rights to access personal information. Access rights can provide autonomy to consumers and enhance the transparency of how their personal information is being handled. As such, we suggest this point also includes providing mechanisms for consumers to access and export their personal information.'

Telstra Corporation Limited '*supports the intent of this principle, however recommends it would benefit from further clarity (perhaps in an explanatory supplement) in the roles of Device Manufacturers and Service Providers, especially in more complex solutions such as a smart home comprising multiple devices, a hub or a gateway. Deleting customer data, initiating a "factory reset" or requesting removal of data from the cloud (especially in the case of a mobile app) can be difficult and confusing for consumers, and clear instructions for consumers to follow should be provided*.'

Principle 12 – Make installation and maintenance of devices easy

The Australian Communications Consumer Action Network (ACCAN) noted *'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'.'

The Australian Industry Group recommended that '*This principle may require support maintenance procedures that are executed by taking the device out of service and being augmented by a similar capability.'*

Cisco Systems Australia Pty Ltd suggested '*We suggest this reads "Make installation and maintenance of devices easy and secure". Upkeep of devices to current secure minimum should be a focus*.'

FermyMate highlighted '*This statement is non-sensible as it makes no reference to the reference material for "best practices by Australian Government on usability". Are you wanting IoT manufactures to be IRAP/ PCI DSS/ ISO9001/ISO27001? Please specify the best practise guide standards required to be compliant against.'*

The Office of the Victorian Information Commissioner stated '*Principle 12 concerns making it easy to install and maintain IoT devices, requiring minimal steps to do so. While this approach may offer convenience to consumers, suboptimal default privacy or security settings could lead to users who do not change the default configurations being exposed to greater risk.*

The concept of 'privacy by design' suggests that IoT devices should deliver the maximum degree of privacy by default – if individuals do nothing, their privacy should not be interfered with, and they should not be required to take action to protect themselves. In line with this, we suggest that the Code of Practice require that default privacy and security configurations should be set to deliver the highest degrees of protection, with an emphasis on this when devices are designed to be used with minimal step up.'

Telstra Corporation Limited said '*Telstra endorses and follows this Principle. We offer a variety of products that can be classed as belonging to the IoT category and provides clear and straightforward guidance on how to set up these devices securely, as well as instructions on how devices can be updated throughout their lifecycle. Auto-update should be built in wherever possible.'*

Principle 13 – Validate input data

Christian Heinrich stated *'13. Validate input data" should be within the top 3 to address the large number of vulnerabilities within CWE-707: Improper Neutralization.'*

Cisco Systems Australia Pty Ltd noted '*This is just one part of secure coding guidelines. This section should be expanded to require more secure coding techniques.'*

Google Australia Pty Ltd suggested *'we suggest a re-articulation of the first sentence of the description of this principle to make the suggested implementation of the principle clearer.'*

Telstra Corporation Limited '*endorses this principle*.'

Other

Digital Risk Innovation stated *'Location of data: There has been widespread discussion on data storage location for IoT networks. I suggest that you include the generally acknowledged value of storing data as close to the device as possible (which will vary depending on the purpose of the network). This can significantly reduce the data security challenge for IoT Service Providers, as protecting and especially understanding obligations in relation to centralised data from a large number of devices can become a privacy and security headache.*

Avoiding IoT domestic abuse: IoT devices in the home can be used as tools of abuse, through remote manipulation of home heating, cooling, security, and other services. The footnoted webinar suggestions two precautions to address this:

1. *All devices enabling remote control of critical services within the home should provide the option for local override. This is both a security and a safety priority.*
2. *Home devices should keep a log of remote access with information such as date, time, and source of access. This is a sensible security precaution.'*

IoT Alliance Australia recommended '*We recommend adding a new principle to the Code of Practice requiring the IoT Service Provider to adopt a cyber supply chain risk management framework. This should be in accordance with ISO28000*.'

Telstra Corporation Limited suggested '*The Code should include an additional Principle which outlines who is responsible for the security of IoT devices where the IMSI is from an overseas manufacturer. Roaming IMSIs can introduce added risk to the confidentiality, integrity and availability of the data or the service, as traffic may be routed through Service Providers in the country of origin as a part of the agreed connectivity model with Australian Service Providers. An example is an overseas Service Operator providing SIMs for devices use in Australia that connect with the networks of Australian Service Providers; an additional Principle is required which provides a guideline for who would bear responsibility for risks associated with roaming devices would help clear up expectations and help support continued growth in the IoT space*.'