Internet of Things
Position Statement

June 2021

Contents

What is the Internet of Things?

Internet of Things powered smart devices and appliances provide consumers with optimal convenience. Voice enabled assistants like Alexa and Google Nest can remotely control all aspects of a smart home, from ambient indoor temperature to music playlists. Wearables like smart watches allow consumers to count steps, monitor heart rate, reply to messages, answer phone calls, keep track of social media and watch YouTube.

These functions are made possible using network connectivity that automatically collects and uses data to perform predictive functions.[1] Location data, demographic data, health data, behavioural data, voice and facial recognition data are all used to make devices and appliances 'smart' and deliver personalised experiences and utilities based on historic usage patterns and user preferences.[2]

In Australia, and worldwide, the demand for consumer IoT devices and appliances is soaring as they become more affordable and is predicted to increase exponentially. The ongoing rollout of 5G mobile technology in Australia, which will increase operational speed of IoT devices, means in 2023 the average Australian household will probably contain 18 IoT connected devices. By 2025 Australia's Internet of Things market is forecast to be worth a massive $5.3 billion.[3]

What consumers need from Internet of Things regulation

Australia's current voluntary, Code-based IoT regulatory framework offers consumers minimal protection, and there are limited market-based incentives for Australian IoT device manufacturers to fill this void.

Australian consumers need an enforceable Internet of Things regulatory framework that relieves consumers of sole responsibility for their privacy and security and holds IoT device manufacturers accountable for the operation and outcomes of their products.

Given the vast majority of IoT devices are manufactured offshore and are either imported for sale or purchased by consumers directly online, regulatory measures will need be applicable post-manufacture to capture all devices sold and used by Australian consumers.

Australia's IoT regulatory regime will also need to be aligned with comparable jurisdictions to ensure consistency of consumer protection measures globally.

An effective Australian Internet of Things regulatory regime will address:

- Cybersecurity
- Data privacy and informed consent
- Transparency and consumer information
- Device and network resilience
- Durability and fitness for purpose
- Accessibility
- Protection for vulnerable consumers

[1] www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/

[2] US Congressional Research Service, *The Internet of Things (IoT): An Overview*, 12 February 2020 – accessed at https://fas.org/sgp/crs/misc/IF11239.pdf

[3] ACMA, Internet of Things in media and communications: Occasional paper, July 2020

Cybersecurity

Manufacturers often prioritise price competitiveness and optimal consumer experience over in-built 'security by design' features, leaving smart homes with multiple IoT devices and appliances vulnerable to potential cyber threats and exposing them to significant risk of cyber-attack.

Due to lack of adequate security protection - non-existent or inadequate passwords, an inability to patch exploitable firmware, or holes in the authentication and data transfer ecosystem - security experts believe about 60% of the 30 billion IoT connected devices on the market are totally unsecured or can be hacked using brute force attacks.[4]

The ongoing rollout of 5G mobile technology in Australia, which will increase operational speed of IoT devices, means increasing numbers of devices will be connected to the internet and unsecured devices such as smart TVs, online security cameras, networked baby monitors and smart home devices will open more avenues for hackers to find "vulnerabilities" and get into networks.[5]

Devices and services should be required to only operate on the 'principle of least privilege' (POLP), restricting degrees of user access on a case-by-case basis, disabling unused device functionality, closing unrequired ports and restricting access to the local network unless the device needs to be managed remotely.

Software should be developed with optimal security features using penetration testing, and device manufacturers should be required to automatically update IoT devices with new security software that is easy for consumers to install.

Mandatory 'security by design' protocols in device manufacture, buttressed by tighter regulatory scrutiny and penalties for breach, should also be introduced.

Data privacy and informed consent

The information asymmetry between consumers and manufacturers means users may not be aware of the amount of data smart devices collect, making it impossible for consumers to provide genuinely informed consent.

Clear, simple notification of data collection practices is needed to enable all consumers - including those who have a disability or come from a non-English speaking background – to provide genuinely informed consent to the collection and use of their data with a full understanding of the security risks and loss of privacy entailed.

Consumers should also be able to continue to use IoT products and services even if they refuse, or after they withdraw, consent.

[4] Roberts, G. 'Australian security cameras hacked, streamed on a Russian-based website', ABC News, 24 June 2020 - accessed at www.abc.net.au/news/2020-06-24/security-cameras-hacked-streamed-on-russian-website/12380606

[5] Ibid

Transparency and consumer information

Manufacturers need to be given economic incentives to provide information about the level of security provided by IoT devices. The introduction and enforcement of a 'star rating' or 'trust' label on packaging of IoT connected devices is needed to provide consumers with comparative information and enable consumers to reward manufacturers who have in-built 'security by design' features by choosing to purchase their products over others.[6]

Consumer consent should not be a substitute for IoT manufacturers accepting responsibility for the privacy and security of their products.[7] Device manufacturers should be obligated to build privacy features into the design of IoT products, take appropriate measures to protect collected data from attack in storage and transmission, and delete a consumer's collected data on request.

Device and network resilience

The threats to security and functionality posed by outages of power and data networks mean resilience needs to be built into IoT devices and services by IoT device manufacturers and IoT service providers.

IoT devices should be designed so that they continue to operate without an internet connection, have electronic security protocols that remain uncompromised and include an in-built power source and back-up system to allow them to continue to operate locally.

IoT devices should also be designed to default to their customised settings after an outage or power failure, to ensure continual support for consumers with disability who rely on IoT devices to live independently.

Durability and fitness for purpose

Planned obsolescence occurs when a device expires within days of a warranty period ending and the cost of repair exceeds that of replacement. It also occurs when new release devices quickly become incompatible with software updates, meaning consumers are left with expensive and useless purchases.

Durability should be guaranteed for consumers purchasing expensive IoT enabled devices, consistent with consumer law product guarantees.

IoT device manufacturers should be required to provide mandated regular operational software updates which are compatible with devices over a reasonable period, that do not require consumers to replace a device.

Consumers should also be compensated by manufacturers if they no longer provide technical support for outdated technology.

[6] Morgner, P, Freiling F. and Benenson, Z, 'Opinion: Security Lifetime Labels -- Overcoming Information Asymmetry in Security of IoT Consumer Products', 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018

Accessibility

The potential for IoT technology to support independent living for people with disabilities can only be fulfilled if devices and appliances are easily accessible and are sold with accessible settings fixed by default 'straight out of the box'.

Protection for vulnerable consumers

The personal information collected by IoT devices can be accessed by third parties, or 'hacked' by cybercriminals, and misused or aggregated for unauthorised purposes.

Unregulated child specific IoT enabled products such as toys and baby monitors pose privacy and security threats for the children and parents who use them. Victims of domestic violence are at risk from predators who use the granular data collected by their devices to stalk their movements.

As IoT adoption grows, in-home IoT devices with microphones and sensors will increasingly collect consumers' personal information and record their activity,[8] increasing their vulnerability to external surveillance and misuse of their data.

IoT device manufacturers need to assume responsibility for the protection of vulnerable consumers through increased transparency about security risks, improved data collection notification practices, and introduction of age-specific consent requirements.

Device settings should be simple to understand and easy to configure to enable consumers to make informed decisions about privacy settings on IoT devices, and users should be periodically notified of what data is being collected and shared and be given the option of withdrawing consent without penalty.[9]

Built-in 'security by design' features which anticipate risk trajectories for vulnerable consumers would offer optimal protection from the threats of stalking and unauthorised surveillance.

[8] www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/

[9] IBM Policy Lab, *Five Technology Design Principles to Combat Domestic Abuse*, 28 May 2020 – accessed at www.ibm.com/blogs/policy/design-principles-to-combat-domestic-abuse/