accan

Connection and Protection: What consumers need from the Internet of Things

Position Statement

June 2021

Contents

What is the Internet of Things?

The Internet of Things (IoT) "brings the power of the internet, data processing and analytics to the real world of physical objects".[1] In simple terms, consumer IoT devices and appliances are everyday items - whitegoods, baby monitors, security cameras, smart phones, watches, TVs - that have had internet connectivity added to them. Consumers "interact with the global information network" via these devices "without the intermediary of a keyboard and screen".[2]

Both in Australia and worldwide the demand for consumer IoT devices and appliances is soaring as they become more affordable. At least 16 million Internet of Things (IoT) connected devices were installed in Australia in 2019,[3] and the ongoing rollout of superfast 5G mobile technology in Australia means that by 2023 it is predicted the average Australian household will contain 18 IoT connected devices. By 2025 Australia's Internet of Things market is forecast to be worth a massive $5.3 billion.[4]

Identifying the opportunities and challenges posed by IoT, and ensuring our regulatory framework is fit for purpose, is important to ensure Australia realises the full economic and social benefits of IoT.[5]

Consumer benefits and risks

IoT technology is designed to make the lives of consumers easier by performing tasks and providing services. For example:

- Smartphones or tablets are used by homeowners to remotely control all aspects of a smart home - appliances, thermostats, lights, and other devices.
- Smart voice assistants like Alexa and Google Nest set alarms, reminders, play music, answer questions, search the internet, and control smart home devices with a simple voice command.
- Smart refrigerators keep users informed about dwindling fridge supplies, while smart microwaves, ovens and washing machines monitor the energy they are using to reduce waste and save on bills.
- IoT enabled wearables like smart watches not only count steps and monitor heartrates but are interconnected with other smart devices to allow users to reply to messages, answer phone calls, keep track of social media and news or watch YouTube.

Despite the conveniences of IoT technology, the fact that personal data is collected in spaces traditionally regarded as private - the home and body – presents increased risks for consumers. As networks and adoption grows, the ubiquity of this technology will increasingly raise issues of consumer security, privacy, consent, transparency, reliability, accessibility, autonomy and safety.[6]

[1] Fruhlinger, J. 'What is IoT? The Internet of Things Explained', 1 May 2020, *Network World* – accessed at www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html

[2] Fruhlinger, op cit

[3] Ikeda, S. 'IoT-Based DDoS Attacks Are Growing and Making Use of Common Vulnerabilities', *CPO Magazine*, 25 March 2020 – accessed at www.cpomagazine.com/cyber-security/iot-based-ddos-attacks-are-growing-and-making-use-of-common-vulnerabilities/

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

[5] Ibid

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

IoT regulation in Australia

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.[7]

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 to be applicable post-manufacture to capture all devices sold and used by Australian consumers.

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

Cybersecurity

A typical smart home with many IoT devices is under significant risk of cyber-attack, with security experts estimating that 60% of the 30 billion IoT connected devices on the market worldwide are totally unsecured or can be hacked using brute force attacks.[8]

Because IoT device manufacturers often prioritise price competitiveness and optimal consumer experience over in-built 'security by design' features, they continue to sell products with lax password protocols and poor authentication and data transfer ecosystems. This leaves IoT devices and appliances unprotected against hackers,[9] making them the most vulnerable point in an interconnected system.[10]

Large-scale distributed denial-of-service (DDoS) attacks have increased dramatically since 2018, in parallel with the boom in consumer IoT devices. Cybercriminals have exploited unsecured in-home networks to launch multiple

[7] AI Ethics Principles

[8] 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

[9] Albergotti, R. 'How Nest, designed to keep intruders out of people's homes, effectively allowed hackers to get in', *The Washington Post*, 24 April 2019 – accessed at www.washingtonpost.com/technology/2019/04/23/how-nest-designed-keep-intruders-out-peoples-homes-effectively-allowed-hackers-get/

[10] Ikeda, op cit

botnet attacks from many sources simultaneously, shutting interconnected systems down and crashing websites like Amazon.[11]

The increased bandwidth and reduced latency of 5G networks will allow more IoT devices to become connected to one another and the internet, and the risk and impact of breaches of security and associated cyberattacks such as distributed denial of service (DDoS) will increase proportionally.[12] In future, millions of unprotected super high bandwidth consumer IoT devices could potentially be harnessed to launch DDoS attacks of unprecedented scale.[13]

Enforceable measures which should be implemented to improve the cybersecurity of IoT connected devices include:

- Requiring devices and services to 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, contain security compromises to their area of origin and stop them spreading to the system at large.
- Requiring use of appropriate privileges on software access, using a secure software development process, and performing penetration testing to protect connected devices against infiltration by hackers seeking to access a local Wi-Fi network to manipulate all connected devices.
- Requiring device manufacturers to disable unused device functionality, close unrequired ports and restrict access to web management to the local network, unless the device needs to be managed remotely via the internet.
- Requiring encryption in transit of any security-sensitive data, including any remote management and control, at the device or user interface level to prevent unauthorised infiltration by hackers. In the current unregulated system, IoT device manufacturers are not required to use encryption software and often omit this in favour of cost reduction, increased battery life, minimised memory requirements, ease of use and reduced device size.
- Requiring secure storage of credentials on devices and services, including not allowing hard-coded credentials such as usernames and passwords to be embedded in device software or hardware, to prevent security breaches via reverse engineering.
- Requiring users to change default passwords before using IoT devices to prevent duplicated or default passwords being used. Unique passwords would restrict the risk to consumers posed by hackers infiltrating networks. This approach would be consistent with the *Australian Privacy Act* requirement to implement a 'privacy by design' approach to compliance.
- Requiring device manufacturers to automatically update IoT devices with new security software, distributed via secure IT infrastructure and easily installed by consumers. Updating security software should not be the obligation of the consumer but should be the responsibility of the IoT device manufacturer. Consumers should also be encouraged by manufacturers to keep home network router software up to date and make sure all security patches and software updates for IoT devices are installed as soon as they are released. [14]

Data privacy and informed consent

The Internet of Things creates more opportunities for the collection of consumer data than ever before. IoT devices collect consumers' location data, demographic data, health data, behavioural data, and voice and facial

[11] https://blog.nexusguard.com/threat-report/ddos-threat-report-2018-q2
[12] Ibid
[13] https://www.corero.com/blog/ddos-hackers-using-iot-devices-to-launch-attacks/
[14] https://iapp.org/news/a/australia-australia-legislates-for-privacy-by-design/

recognition data, all without the need for human intervention, to make them 'smart', using historical preferences and personal usage patterns to perform predictive functions.[15]

In an adequately regulated environment, collection and use of consumer data should be consensual, safe and secure. Manufacturers should be required to:

- actively seek informed consumer consent and allow them to withdraw consent at any stage without suffering adverse consequences,
- permit only the minimum amount of data required for functionality to be collected,
- provide consumers with effective and practical controls over ongoing data use, and
- ensure any collected data is safely stored. [16]

However, in many circumstances, consumer consent for the collection and use of data is not free and informed because:

- Consumers do not have time to read the full terms and conditions, or are simply fatigued by the consent process, and agree to "click wrap" agreements without understanding them properly.[17]
- Data is collected passively in public spaces without any overt consumer interaction,[18] capturing user preferences and usage behaviour, including location data, from personal mobile devices.[19]
- When consumers do consent to collection of their data they may feel compelled to consent, despite misgivings, in order to access certain services.[20]
- 'Bundled' consent to use group IoT devices such as Google Nest is given by a single individual on behalf of all members of a household.[21]
- Individuals are given no choice about which collections, uses and disclosures they agree to and which they do not.[22]

Inadequate consent processes and lax security protection for collected user data exposes consumers to a wide range of potential privacy infringements. These include exploitation of data by third parties without consumers' explicit consent; unauthorised use of aggregated data to identify, locate, track, or monitor an individual without their knowledge;[23] and misappropriation of stolen consumer data for illegal purposes such as identity theft, causing financial and emotional damage to consumers or their businesses.[24]

Enforceable measures which should be implemented to improve informed consent and data protection include:

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

[16] G3ict, *Internet of Things: New Promises for Persons with Disabilities*, July 2015

[17] www.claytonutz.com/knowledge/2018/august/click-wraps-the-way-of-the-future-but-make-sure-theyre-legal

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

[19] www.insightsassociation.org/issues-policies/glossary/passive-data-collection

[20] McKay, op cit

[21] www.ipc.nsw.gov.au/fact-sheet-consent-and-bundled-consent

[22] www.cbp.com.au/insights/insights/2019/november/what-is-real-consent-to-data-collection

[23] McKay, op cit

[24] Roberts, op cit

- Requiring device manufacturers to implement a properly informed, transparent, valid and lawful consumer consent procedure to proceed before personal data is collected and used, providing consumers with the opportunity to withdraw their consent at any time.
- Requiring device manufacturers to take appropriate measures to ensure collected consumer 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 into the design and operation of IoT devices.
- Requiring device manufacturers to delete a consumer's collected personal data on request. In the absence of a General Data Protection Right equivalent provision in the *Australian Privacy Act* and *Australian Privacy Principles*, consumers should be able to control the use and retention of their data.

Transparency and consumer information

Ensuring the safety, security and informed consent of consumers who use IoT devices begins at the point of purchase. In the current IoT marketplace, IoT manufacturers know more about the risks and benefits of devices than the consumers purchasing them, preventing users from making informed purchasing decisions. However, under Australia's current regulatory regime there are no economic incentives for manufacturers to provide this information, and no regulatory framework to ensure that they do.

To remedy this situation, easy to understand, accessible information should be provided at the point of purchase, and the privacy and security features of IoT devices should be included on product packaging as part of the value proposition, to empower consumers to make informed choices when buying IoT devices. Manufacturers who include and advertise 'privacy by design' features in their products would be rewarded by increased sales, and this automatic feedback loop would provide an economic incentive for all manufacturers to follow suit.[25]

Enforceable measures which should be implemented to provide greater transparency, and facilitate more informed consumer purchasing decisions, include:

- A mandated privacy and security 'star rating', assessed by an independent regulatory body, on IoT product packaging at the point of sale.
- Complementary enforceable regulation to ensure IoT device manufacturers adopt 'privacy by design' principles and accept responsibility for the security of their products.
- Requiring the use of vulnerability disclosure policies by IoT device manufacturers to inform consumers who purchase IoT connected devices of the risks inherent in their design and function.

Device and network resilience

IoT systems and devices are relied upon by consumers for increasingly important purposes that ensure safety and save lives, and the consequences of a lapse in functionality or security posed by outages of data networks and power are potentially catastrophic. Resilience needs to be built into IoT devices, especially for those that perform essential functions, to guarantee uninterrupted network and power supply.

[25] Morgner, P, Freiling F. and Benenson, Z, Opinion: Security Lifetime Labels -- Overcoming Information Asymmetry in Security of IoT Consumer Products, June 2018

Device and network resilience is particularly important for consumers with disabilities who are dependent on IoT technologies for independent living. IoT connected devices must be capable of continuing to function in the event of a network or power outage. 'Clean' recovery to personalised settings following an outage is also essential, so that consumers with disabilities can continue to use their personalised devices without needing to reprogram them.[26]

Enforceable measures which should be implemented to ensure IoT devices are designed and manufactured to be resilient include:

- Requiring IoT devices to be manufactured with an uninterruptable power supply (UPS) – for example, a battery or other emergency power source - to ensure continuity of operation if there is a power outage.
- Requiring IoT devices to be manufactured with a built-in back-up system to ensure local continuity of operation if there is a loss of network, assessed on a case-by-case basis, proportionate to the intended use of the device and the needs of the user.27
- Requiring IoT devices to be manufactured with electronic security protocols - network security, application security and information security – that are not compromised by outages.

Durability and fitness for purpose

IoT devices should be durable and fit for purpose. Consumers have an expectation that the goods they purchase should last for a reasonable period. Instead, planned obsolescence - where a device is designed so that within days of a warranty period expiry, users find their devices cease to function and the cost of repair exceeds that of replacement – is commonplace.

New release devices quickly become incompatible with software updates and consumers are either left with expensive and useless purchases or are forced into a position where it is more cost effective to buy a new device. This increases sales for the manufacturer but has negative flow-on effects for not only the consumer but also the environment.

It also remains uncertain how the consumer law guarantee of 'acceptable quality' applies to IoT devices, and whether durability is a key element.[28]

Enforceable measures which should be implemented to ensure IoT devices are durable and fit for purpose, and to protect consumers from purchasing devices with short-term functionality, include:

- Requiring IoT device manufacturers to provide mandated regular operational software updates which are compatible with devices over a reasonable period, and don't require consumers to replace a device.
- Requiring the provision of an end-of-life policy at the time of purchase to inform consumers about whether security software updates can be installed and, if so, when automatic software updates will cease.

[26] G3ict, op cit

[27] 'Mapping Security & Privacy in the Internet of Things' – accessed at https://iotsecuritymapping.uk/code-of-practice-guideline-no-9/

[28] Manwaring, K. 'Six Things Every Consumer Should Know about the Internet of Things', *The Conversation* - accessed at https://theconversation.com/six-things-every-consumer-should-know-about-the-internet-of-things-78765

- Informing consumers at point of sale about the anticipated date of obsolescence when devices will no longer be fit for purpose.
- Requiring IoT device manufacturers to compensate consumers when they cease providing technical support for outdated technology.
- Subjecting IoT devices to basic performance standards equivalent to the consumer guarantees under the *Australian Consumer Law*.

Accessibility

For many people with disabilities, IoT smart home systems offer more than just optional convenience. These consumers are dependent upon such systems to enable them to live independently. Using an accessible smartphone interface and voice activated assistants, IoT technologies and in-home devices can perform functions for people with disabilities that would otherwise be difficult or, for some, impossible.

For example, a person who is blind can remotely monitor and control the thermostat, turn lights on or off and activate alarm systems, or a person with a mobility-related disability can have his door automatically unlock when he approaches it.[29]

The potential for IoT technology to support independent living for people with disabilities can only be fulfilled, however, if the devices and appliances are made accessible. IoT devices should be designed and manufactured with the needs of these consumers in mind and sold with intuitive and simple accessibility settings set by default 'straight out of the box'.

Device manufacturers should also be required to provide accessible information on data collection practices and the security by design features included in IoT devices, including instructions on how to withdraw consent or delete collected data, so that consumers with disabilities can exercise the same control over their personal information as consumers without disability.

Protection for vulnerable consumers

Inclusion of privacy protection and security measures in IoT devices is particularly important for more vulnerable consumers, including children, domestic violence victims and seniors.

Children

IoT devices in the home such as networked toys, virtual in-home assistants and smart televisions have the capacity to collect and retain large amounts of data and metadata - photos and videos, location data and behavioural information - on all consumers, including children. This information can then be shared, with or without authorisation, with third parties, presenting significant privacy and security risks.[30]

Parents and guardians currently shoulder the most responsibility for protecting children from online infringements of their children's privacy and safety.[31] But as a growing number of IoT devices containing microphones and sensors are installed in the home, and the collection and monitoring of children's personal information by

[29] G3ict, op cit

[30] Haber, E. *The Internet of Children: Protecting Children's Privacy in A Hyper-Connected World*

[31] https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking

commercial third parties increase,[32] device manufacturers need to be held accountable for children's online privacy and safety.

Enforceable measures which should be implemented to protect children using IoT devices from oversurveillance and security threats include:

- Improved notification and transparency of what children's data is collected and how it is used.
- Requiring a parent, guardian or other responsible adult to act as proxy when consenting to the collection of children's personal data.
- Ensuring privacy settings in IoT devices are intuitive to use to make it easy for parents to delete their children's personal data.
- Requiring built-in 'security by design' features to protection children from oversurveillance and privacy and security threats.
- Ensuring tighter regulatory scrutiny and online safety standards for child-specific products like toys and nd baby monitors.[33]

Domestic violence victims

98 percent of Australian domestic abuse support workers report they have clients who have experienced technology-facilitated abuse.[34] If not securely protected the granular data collected by IoT devices, including location data, can be used by abusers to stalk victims.

Enforceable measures which should be implemented to protect victims of domestic violence from technology-facilitated abuse include:

- Ensuring products are secure, only collecting and sharing necessary data, to minimise the risk of malicious misuse of information.
- Designing IoT products to prevent misuse and abuse by anticipating potential risk trajectories for victims who use IoT devices and services.35
- Ensuring privacy settings are easy to understand and intuitive to configure, and that default privacy settings are designed based on the needs and capabilities of a diverse user base.
- Enabling users to actively make informed decisions about their privacy settings on IoT devices by providing regular notifications about what data is being collected and shared and providing them with the option of withdrawing consent at any stage without penalty.
- Making it easy for individual family members to subscribe and unsubscribe from joint IoT devices, such as Google Nest, to empower all users with joint control.36
- Mandating in-built 'security by design' in the manufacture of IoT devices.

[32] www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/
[33] Ibid
[34] http://accan.org.au/grants/current-grants/813-empowering-women-to-end-digital-abuse
[35] Tanczer, L. Neira, I. Parkin, S. Patel, T. and Danezis, G. *Gender and IoT Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse*, University College London, November 2018 - accessed at www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf
[36] 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/

Seniors

Finally, although many see coercive control as an issue mainly impacting women who are victims of domestic violence, coercive control can occur in any relationship where there is a power imbalance, as in the case of elder abuse. The same enforceable measures designed to protect victims of domestic violence could be used to protect seniors from IoT technology facilitated abuse.[37]

[37] Ibid

References

ACMA, Communications Report 2018-19 – accessed at https://www.acma.gov.au/publications/2020-02/report/communications-report-2018-19

ACMA, *Internet of Things in media and communications: Occasional paper*, July 2020

ACMA, *Artificial intelligence in communications and media: Occasional paper*, July 2020

Albergotti, R. 'How Nest, designed to keep intruders out of people's homes, effectively allowed hackers to get in', *The Washington Post*, 24 April 2019 – accessed at www.washingtonpost.com/technology/2019/04/23/how-nest-designed-keep-intruders-out-peoples-homes-effectively-allowed-hackers-get/

'Amazon 'thwarts largest ever DDoS cyber-attack'', BBC News, 18 June 2020 – accessed at https://www.bbc.com/news/technology-53093611

Australian Council on Children and the Media, *Apps Can Track*, 2021 – accessed at https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking

Australian Government Department of Home Affairs, *Code of Practice: Securing the Internet of Things for Consumers* - accessed at www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

Australian Government Department of Industry, Science, Energy and Resources, *AI Ethics Principles* – accessed at www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

Australia's Cybersecurity Strategy 2020 – accessed at https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Brookes, J. 'Disruptive Potential Emerges For IoT In Australia's Industrial Internet', *Which 50*, 11 May 2020 - accessed at https://which-50.com/cover-story-disruptive-potential-of-iot-in-australia-could-be-stymied-by-regulation

Ducket, C. *New Australian cybersecurity strategy will see Canberra get offensive*, 6 August 2020 – accessed at www.zdnet.com/article/new-australian-cyber-security-strategy-will-see-canberra-get-offensive/

Fagella, D. *Artificial Intelligence Plus the Internet of Things (IoT) – 3 Examples Worth Learning From*, 23 October 2019 – accessed at https://emerj.com/ai-sector-overviews/artificial-intelligence-the-internet-of-things-iot-3-examples-worth-learning-from/

Ghosh, I. 'AIoT: When Artificial Intelligence Meets the Internet of Things', *Visual Capitalist*, 12 August 2020 – accessed at https://www.visualcapitalist.com/aiot-when-ai-meets-iot-technology/

Ikeda, S. 'IoT-Based DDoS Attacks Are Growing and Making Use of Common Vulnerabilities', *CPO Magazine*, 25 March 2020 – accessed at www.cpomagazine.com/cyber-security/iot-based-ddos-attacks-are-growing-and-making-use-of-common-vulnerabilities/

Internet Society, *Policy Brief; IoT Privacy for Policymakers*, 19 September 2019 – accessed at https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/

Maher, J. 'Hacker Takes Over Couple's Smart Home, Plays Vulgar Music And Raises Temperature to 90 Degrees', *Newsweek*, 23 September 2019 – accessed at www.newsweek.com/google-nest-hack-milwaukee-1460806

‘Mapping Security & Privacy in the Internet of Things’ – accessed at https://iotsecuritymapping.uk/code-of-practice-guideline-no-9/

McKay, D. *State of the Art in Data Tracking Technology*, Consumer Policy Research Centre, November 2019

Morgner, P, Freiling F. and Benenson, Z, *Opinion: Security Lifetime Labels -- Overcoming Information Asymmetry in Security of IoT Consumer Products*, June 2018

Paul, F. ‘IoT has an obsolescence problem’ - accessed at https://www.networkworld.com/article/3279729/iot-has-an-obsolescence-problem.html

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

Sivaraman, V. Gharakheili, H. and Fernandes, C. *Inside job: Security and privacy threats for smart-home IoT devices*, May 2017 - accessed at https://accan.org.au/files/Grants/UNSW-ACCAN_InsideJob_web.pdf

Tan, J., Leung, L. and Bräutigam, T. *Singapore Introduces Cybersecurity Labelling Scheme*, April 2020 – accessed at www.twobirds.com/en/news/articles/2020/singapore/singapore-introduces-cybersecurity-labelling-scheme

Tanczer, L. Neira, I. Parkin, S. Patel, T. and Danezis, G. *Gender and IoT Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse*, University College London, November 2018 - accessed at www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf

Targett, E. ‘AWS Hit With a Record 2.3 Tbps DDoS Attack, *Computer Business Review*, 13 June 2020 – accessed at www.cbronline.com/news/record-ddos-attack-aws

Telsyte, *Australian IoT@home market cracks $1BN, paving the way for IoT-commerce services*, 14 May 2019 - accessed at www.telsyte.com.au/announcements/2019/5/14/australian-iothome-market-cracks-1bn-paving-the-way-for-iot-commerce-services

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

Whitakker, Z. ‘After a spate of device hacks, Google beefs up Nest security protections’, *Tech Crunch*, 2 June 2020 – accessed at https://techcrunch.com/2020/06/01/google-nest-advanced-protection/

Winder, D. ‘Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach’, *Forbes*, 2 July 2019 – accessed at https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/#715578c7411c

Women’s Legal Services, *Technology Facilitated Stalking and Abuse*, 2014 – accessed at http://accan.org.au/grants/current-grants/813-empowering-women-to-end-digital-abuse