WHO IS RESPONSIBLE FOR AN INTERNET OF UNSAFE THINGS? LIABILITY AND CONSUMER INTERNET OF THINGS DEVICES UNDER THE AUSTRALIAN CONSUMER LAW

Authors

Dr Evana Wright, Faculty of Law, University of Technology Sydney
Professor David Lindsay, Faculty of Law, University of Technology Sydney
Dr Genevieve Wilkinson, Faculty of Law, University of Technology Sydney

Details for Correspondence

Dr Evana Wright
PO Box 123
Broadway NSW 2007

evana.wright@uts.edu.au
(02) 9514 3164

WHO IS RESPONSIBLE FOR AN INTERNET OF UNSAFE THINGS? LIABILITY AND CONSUMER INTERNET OF THINGS DEVICES UNDER THE AUSTRALIAN CONSUMER LAW

Abstract

Internet of Things ('IoT') devices are ubiquitous with connected devices found in a diverse range of fields, including industry, transport, agriculture, healthcare and the home. IoT devices pose challenges to security and privacy, and existing laws in Australia are insufficient to address the risks posed. The loss or damage from exploiting insecure IoT devices can include physical injury, damage to property, loss of data, invasion of privacy and exposure to future harms, such as theft or fraud. There is uncertainty about how the product liability and product safety regimes under the ACL apply to consumer IoT devices, especially where harm arises due to security vulnerabilities. This article explores the issues in applying the product liability and product safety regimes under the ACL to insecure consumer IoT devices and provides recommendations for reform to ensure that the ACL is responsive to emerging technologies and protects consumers from harm.

I INTRODUCTION

Internet of Things ('IoT') devices are ubiquitous with connected devices found in a diverse range of fields, including industry, transport, agriculture, healthcare and the home. Statistica estimates that there will be 15.9 billion connected devices worldwide by 2030,[1] with many of these found in the home. Consumer IoT devices include internet-enabled doorbells and security cameras to monitor the home, connected baby monitors that allow you to view your child from your phone, smart assistants that can turn on your lights, and connected appliances such as heaters, ovens and vacuums that may be turned on remotely. These devices are increasingly popular and are being adopted by consumers, who appreciate the convenience afforded yet may not understand the security and privacy risks posed by such devices.

Consumer IoT devices are vulnerable to security breaches. Internet-enabled doorbells and security cameras may be hacked with third parties able to access the camera, view private footage and speak to home occupants, such as those experienced by users of Ring doorbells and security cameras.[2] Hackers can exploit security vulnerabilities to access connected baby monitors to talk to children and capture images.[3] Connected vehicles can be hacked, allowing hackers to obtain control of a

* The research for this article was supported by a research grant from the Australian Communications Consumer Action Network (ACCAN) and the Australian Government.

[1] Statistica, *Number of Internet of Things Connected Devices Worldwide from 2019 to 2030, by Vertical* (Web Page, 17 March 2022) <https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/>.

[2] ABC News, 'New Security Warning for In-Home Smart Cameras' (YouTube, 13 December 2019) <https://www.youtube.com/watch?v=GnlIEQt_QFo&t=155s>; Paulius Ilevičius, 'Ring Hacked: Doorbell and Camera Security Issues' *NordVPN* (Blog Post, 23 December 2020) <https://nordvpn.com/blog/ring-doorbell-hack/>; Zack Whittaker, 'Amazon Ring Doorbells Exposed Home Wi-Fi Passwords to Hackers' *TechCrunch* (Web Page, 8 November 2019) <https://techcrunch.com/2019/11/07/amazon-ring-doorbells-wifi-hackers/>.

[3] Neil J Rubenking, 'Exclusive: Popular Baby Monitor Wide Open to Hacking' (27 February 2020) *PCMag* <https://au.pcmag.com/home-security-products/65761/exclusive-popular-baby-monitor-wide-open-to-hacking>; Dennis Romero, 'Stranger Hacks into Baby Monitor, Tells Child, "I Love You"' *NBC News* (online, 23 November 2019) <https://www.nbcnews.com/news/us-news/stranger-hacks-baby-monitor-tells-child-i-love-you-n1090046>.

car, causing the potential for physical damage.[4] Connected appliances can be exploited as part of broader system-wide attacks, such as in the case of the Mirai botnet using compromised IoT devices to launch distributed denial of service attacks.[5] The loss or damage arising as a result of exploiting insecure IoT devices can include potential physical injury, damage to property, loss of data, invasion of privacy and exposure to future harms, such as theft or fraud. Without regulation, manufacturers have little incentive to address security issues in consumer IoT devices.[6] Information asymmetries mean that consumers lack the information necessary to identify insecure devices. There is no incentive for manufacturers to address security issues in a market where purchasing decisions are typically focused on price.[7]

IoT devices pose challenges to security and privacy, and existing laws in Australia provide a patchwork of regulations that is insufficient to address the risks posed by consumer IoT devices. To date, specific IoT regulation has been limited with a voluntary Code of Practice as the primary response, but with consultation ongoing as to the broader question of regulating cybersecurity, including the security of consumer IoT devices.[8] Recent research funded by the Australian Communication Consumer Action Network ('ACCAN') has identified the need for law reform to address the specific risks posed by consumer IoT devices, including proposed reforms to the Australian Consumer Law ('ACL').[9]

There is uncertainty about how the product liability and product safety regimes under the ACL apply to consumer IoT devices, especially where harm arises due to security vulnerabilities. This article will explore the issues that arise when applying the current product liability and product safety regimes under the ACL to consumer IoT devices. First, this article defines consumer IoT devices and explains the unique features of consumer IoT devices that raise challenges for security, privacy and consumer protection laws. Second, the article provides an overview of the product liability regime under the ACL. Third, the article analyses the application of the existing product liability regime to consumer IoT devices. Fourth, the article reviews the current product safety regime under the ACL, and identifies how existing provisions dealing with product recalls and information standards may be used to better address the issues raised by consumer IoT devices. The article sets out recommendations for reform to ensure that the ACL is responsive to emerging disruptive technologies, such as IoT devices, and protects consumers from harm. The recommendations identified in this article will ensure that the ACL continues to meet the characteristics of effective product liability law, as identified by the Law Reform Commission in 1989, including that: manufacturers and suppliers bear the risk of losses caused by their goods; other potential causes of loss are accounted for; and the law provides 'the cheapest, most efficient means of determining compensation claims'.[10]

---

[4] Andy Greenberg, 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' (21 July 2015) *Wired* <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

[5] Joel Margolis et al, 'An In-Depth Analysis of the Mirai Botnet' in Juan E Guerrero (ed), *Proceedings — 2017 International Conference on Software Security and Assistance (ICSSA)* (Institute of Electrical and Electronics Engineers, 2018) 6.

[6] David Lindsay and Evana Wright, 'Regulating Security for the Consumer Internet of Things (IoT)' (2020) 3 *European Journal of Consumer Law* 541.

[7] David Lindsay, Genevieve Wilkinson and Evana Wright, *Regulating to Protect Security & Privacy in the Internet of Things (IoT)* (Draft Report, January 2022) 70.

[8] Department of Home Affairs (Cth), *Strengthening Australia's Cyber Security Regulations and Incentives: A Call for Views* (Discussion Paper, 2021) <https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf>.

[9] David Lindsay, Genevieve Wilkinson and Evana Wright, *Regulation of Internet of Things Devices to Protect Consumers* (Australian Communications Consumer Action Network, July 2022) <https://accan.org.au/grants/grants-projects/1781-regulation-of-internet-of-things-devices-to-protect-consumers>.

[10] Law Reform Commission, *Product Liability* (Report No 51, 1 June 1989) 22 <https://www.alrc.gov.au/publication/product-liability-alrc-report-51/>.

II THE INTERNET OF THINGS ('IOT')

This section provides an overview of the meaning of 'consumer IoT devices' for the purpose of this article. There is no single, accepted definition of the Internet of Things (or 'IoT'). However, the International Telecommunications Union ('ITU') provides the following technical definition: 'A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies'.[11] In more general terms, the term 'IoT' is typically understood to refer to products with embedded software that are connected to the Internet,[12] and that incorporate sensors that enable data to be collected, distributed and acted upon.[13] The Internet of Things has application in several fields including industrial IoT, agricultural IoT, healthcare IoT and consumer IoT. This paper is focused on the regulation of consumer IoT devices that might be subject to the ACL. The *Australian Code of Practice: Securing the Internet of Things for Consumers* ('*Australian Code of Practice*') describes the scope of 'Consumer IoT' as follows:

> Consumers may take many forms. Governments, businesses and individuals may all be consumers of IoT devices. This Code of Practice particularly focuses on consumer grade, internet connected devices and associated applications (e.g. wearable devices, and home appliances such as 'smart televisions' and refrigerators) ...[14]

This article addresses consumer IoT devices that fall within the scope of the *Australian Code of Practice*, focusing on consumer IoT devices for use in the home. For the purposes of this article, consumer IoT devices include internet-enabled video doorbells, smart door locks, smart home assistants, connected children's toys and baby monitors, and connected appliances, such as refrigerators or vacuums.

Certain differences between consumer IoT devices and traditional consumer products mean that consumer IoT devices raise specific challenges for security, privacy and consumer protection law. Consumer IoT devices are complex products made up of hardware, software and associated services,[15] often comprising components from a number of suppliers, such as manufacturers, software providers, third-party app providers and cloud service providers.[16] Furthermore, the nature of the device may also change over time due to the introduction of software updates.[17] In addition, the operation of such devices is particularly opaque, with consumers having little understanding of how the products operate in practice or how the operation of the product may change following the introduction of a software update.[18] The relationship between the consumer and the manufacturer is also different in the case of consumer IoT devices. Following the sale of a traditional consumer product, there is a limited role for the manufacturer in the absence of any product defect. In contrast, the manufacturer of a consumer IoT device often has an ongoing post-

---

[11] International Telecommunication Union, *Overview of the Internet of Things* (Recommendation No ITU-T Y.2060, June 2012) <https://www.itu.int/rec/T-REC-Y.2060-201206-I>.
[12] Natasha Tusikov, 'Regulation Through "Bricking": Private Ordering in the "Internet of Things"' (2019) 8(2) *Internet Policy Review* 1, 2.
[13] Tusikov, n 12, 2.
[14] Department of Home Affairs, Australian Signals Directorate and Australian Cyber Security Centre (Cth), *Code of Practice: Securing the Internet of Things for Consumers* (Report, 2020) 8 <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>.
[15] Consumers International, *The Internet of Things and Challenges for Consumer Protection* (Report, April 2016) 33 <https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>.
[16] Consumers International, n 15, 29.
[17] Guido Noto La Diega and Ian Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (2016) 7(2) *European Journal of Law and Technology* 1, 4.
[18] Consumers International, n 15, 28–29.

sale relationship with the consumer and the device by virtue of the provision of associated services and software updates.

IoT devices pose specific security challenges, typically due to the fact that they are 'always on' – that is, always connected to the Internet, and insecure consumer IoT devices may be exploited to cause widespread harm remotely. According to Hypponen's law, '[w]henever an appliance is described as "smart", it's vulnerable'.[19] Consumer IoT devices are vulnerable to security breaches due to their limited processing power, and a large number of insecure consumer IoT devices creates a large attack surface for malicious actors.[20] These malicious third parties may exploit the 'always on' nature of consumer IoT devices to inflict harm remotely, and such harm may not be limited to individual harm. The vulnerability of IoT devices may be exploited to use networks of insecure devices to launch large system-wide attacks.[21] For example, the Mirai malware exploits factory default usernames and passwords to infect consumer IoT devices to launch distributed denial of service ('DDoS') attacks, with the 2016 attack against the Dynamic DNS provider Dyn, the largest of its kind at the time, resulting in significant interruptions to the online services of major organisations, such as Twitter, PayPal and Netflix.[22] Insecure consumer IoT devices may result in both individual and system-wide harm, and the security vulnerabilities in such devices could be considered a 'safety defect', rendering a manufacturer liable under the product liability provisions of the ACL.

III PRODUCT LIABILITY UNDER THE AUSTRALIAN CONSUMER LAW

The Australian Consumer Law ('ACL') is set out in sch 2 of the *Competition and Consumer Act 2010* (Cth). The ACL provides a comprehensive suite of consumer protections, including statutory consumer guarantees, an unfair contract terms regime, statutory unconscionable conduct provisions, and a product liability regime dealing with safety defects in goods. The provisions of the ACL dealing with the liability of manufacturers for goods with safety defects reflect the product liability provisions under the *Trade Practices Act 1974* (Cth). The objective of the product liability regime is to ensure that the burden of costs arising as a result of safety defects is appropriately allocated to the party most able to bear them: manufacturers, suppliers or consumers. As the Law Reform Commission explained, while using market mechanisms to allocate loss usually promotes the proper pricing of goods, provides incentives to prevent goods from causing loss, and allows producers and consumers to make efficient decisions regarding the production and consumption of goods, in the absence of rights to compensation, the consumer would bear the cost of losses from faulty products.[23] However, manufacturers or suppliers should be liable for harm caused by their goods, as they are best placed, due to greater knowledge, to minimise risks and prevent unsafe goods from entering the market, especially compared to consumers who, due to insufficient information, must 'take goods on trust'.[24]

---

[19] Mikko Hypponen and Linus Nyman, 'The Internet of (Vulnerable) Things: On Hyponnen's Law, Security Engineering, and IoT Legislation' (2017) 7(4) *Technology Innovation Management Review* 5.

[20] Maire O'Neill, 'Insecurity by Design: Today's IoT Device Security Problem' (2016) 2 *Engineering* 48; Eliza Chapman and Tom Uren, *The Internet of Insecure Things* (Issues Paper, Australian Strategic Policy Institute, 2018) <https://www.aspi.org.au/report/InternetOfInsecureThings>.

[21] Margolis et al, n 5.

[22] Margolis et al, n 5; Sam Thielman and Chris Johnston, 'Major Cyber Attack Disrupts Internet Service Across Europe and US', *The Guardian* (online, 21 October 2016) <https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service>.

[23] Law Reform Commission, n 10, 13–15.

[24] Law Reform Commission, n 10, 16. See also Guido Calabresi, *The Costs of Accidents: A Legal and Economic Analysis* (Yale University Press, 1970).

Under the ACL, a manufacturer will be liable to compensate an individual if the manufacturer supplies goods that have a 'safety defect' and the individual suffers injuries because of that defect,[25] or where other goods, land, buildings or fixtures are destroyed or damaged because of the safety defect.[26] The liability of the manufacturer also extends to loss or damage suffered by a person other than the injured individual, where the loss or damage does not arise as a result of a business or professional relationship.[27] Central to the operation of the product liability regime is the definition of a safety defect. Section 9(1) of the ACL states that goods will have a safety defect 'if their safety is not such as persons generally are entitled to expect', with the other sub-sections of s 9 expanding on this, including a non-exhaustive list of circumstances that must be taken into account in determining whether there is a safety defect. It is worth setting out the section in full.

> (1) For the purposes of this Schedule, goods have a safety defect if their safety is not such as persons generally are entitled to expect.
> (2) In determining the extent of the safety of goods, regard is to be given to all relevant circumstances, including:
> a. the manner in which, and the purposes for which, they have been marketed; and
> b. their packaging; and
> c. the use of any mark in relation to them; and
> d. any instructions for, or warnings with respect to, doing, or refraining from doing, anything with or in relation to them; and
> e. what might reasonably be expected to be done with or in relation to them; and
> f. the time when they were supplied by the manufacturer.
> (3) An inference that the goods have a safety defect is not to be made only because of the fact that, after they were supplied by their manufacturer, safer goods of the same kind were supplied.
> (4) An inference that goods have a safety defect is not to be made only because:
> a. there was compliance with a Commonwealth mandatory standard for them; and
> b. that standard was not the safest possible standard having regard to the latest state of scientific or technical knowledge when they were supplied by their manufacturer.[28]

A Safety Defects and Consumer IoT

As set out above, manufacturers and suppliers have better knowledge of how to minimise the risk associated with their goods, when compared to consumers. This is particularly true for consumer IoT devices, where significant information asymmetries mean that consumers typically do not have a good understanding of how the goods function or any associated security vulnerabilities. This section will analyse the application of the product liability regime to consumer IoT devices, including important questions of whether security vulnerabilities may be considered a 'safety defect' for the purposes of s 9 of the ACL; whether the product liability regime addresses safety defects that the manufacturer may introduce by way of software updates for consumer IoT devices; and whether failure to release a software update could be considered a safety defect.

1 Reasonable expectations of the public

The definition of safety defect under s 9 of the ACL places reliance on the general expectations of the public. It is important to note that the public's expectation is not assessed with regard to the actual knowledge or expectation of the consumer. Instead, the inquiry is directed to the 'objectively assessed legitimate expectation' of the public as to the safety of the good.[29] This standard is

[25] ACL s 138(1).
[26] ACL s 140(1), 141(1). The other goods must be 'of a kind ordinarily acquired for personal, domestic or household use or consumption' (s 140(1)(c)) and the land, buildings or fixtures must be 'ordinarily acquired for private use' (s 141(1)(d)).
[27] ACL s 139.
[28] ACL s 9.
[29] *A v National Blood Authority* [2001] 3 All ER 289, [31]. See also *Wilkes v DePuy International Ltd* [2017] 3 All ER 589, [69]–[70].

problematic in relation to consumer IoT devices. As discussed above, there are information asymmetries between manufacturers/suppliers of consumer IoT devices and consumers. Consumers are often unaware of the security risks posed by consumer IoT devices and, accordingly, cannot make informed choices as to product security. Extending this further to the general 'public' and taking into account the existing information asymmetries, it is unclear what the legitimate or reasonable expectation of the community might be in relation to the security of consumer IoT devices.

Butler explains the failings of the consumer expectations test in relation to insecure software and complex digital products, such as consumer IoT devices, as follows:

> The consumer expectations test is likely the most difficult to apply to insecure software defect claims because the test is poorly suited to address defects in complex systems. Consumers, especially those purchasing IoT devices, do not typically understand how their devices function, their role in the internet ecosystem, or the significance of any security vulnerabilities embedded in those systems. A purchaser of a DVR (or a webcam, or a 'smart' refrigerator) likely does not have any expectations about how the software in that device will function. So long as the device carries out the tasks that the user expects, the user is not likely to think about what software is embedded in the device or how the software was developed. If a device has been hacked and is simultaneously being used as part of a botnet to attack servers of a major news site or gaming company, the user may not even be aware of that fact.[30]

The complex nature of IoT devices makes it challenging to define what may be considered a 'safety defect' for the purposes of the product liability regime. While the public may have a general understanding of the risk of software vulnerabilities, they may not understand what software vulnerabilities exist or whether they may be exploited.[31] Even if a consumer IoT device is hacked, it does not always mean that the security measures were so inadequate as to constitute a safety defect.[32] Assuming there is a reasonable expectation as to the existence of security features, what security features would be considered critical such that their absence would constitute a safety defect?[33] Consideration should also be given to whether the failure to release software updates to address existing security vulnerabilities, or to engage in post-sale monitoring of security vulnerabilities, would constitute a safety defect for the purpose of the ACL. The continuing relationship between the consumer and the manufacturer/supplier should be sufficient to impose a post-sale duty upon the manufacturer to release updates and monitor and rectify security vulnerabilities.[34]

The importance of securing consumer IoT devices as a critical element of product safety has been recognised by the development of the voluntary *Australian Code of Practice*, as well as other industry standards, such as the European Telecommunication Standards Institute ('ETSI') baseline technical standard for smart devices, EN 303 645. Moreover, in Australia, the Department of Home Affairs is engaging in consultation as to whether Australia should adopt ETSI EN 303 645 as a mandatory standard for smart devices.[35] However, given the highly specialised nature of such

---

[30] Alan Butler, 'Products Liability and the Internet of (Insecure) Things: Should Manufacturer's Be Liable for Damage Caused by Hacked Devices' (2017) 50 *University of Michigan Journal of Law Reform* 913, 927.
[31] Benjamin C Dean, *Strict Product Liability and the Internet of Things* (Report, Center for Democracy and Technology, 16 April 2018) 20 <https://cdt.org/insights/report-strict-product-liability-and-the-internet-of-things/>.
[32] Lucas M Amodio, 'The Intersection of Product Liability Law and the Internet of Things' (4 January 2021) *Boston College Intellectual Property and Technology Forum* 1, 12.
[33] Dean, n 31, 20.
[34] Butler, n 30, 928.
[35] Department of Home Affairs (Cth), n 8, 29.

codes of practice or industry standards, these are not likely to be relevant in informing the public's reasonable expectations about safety.

The meaning of 'safety defect' as it relates to consumer IoT devices needs to be clearer, and the Australian Competition and Consumer Commission ('ACCC'), as the applicable regulator, should consider the following two options. First, the ACCC should provide consumer guidance on what may constitute a 'safety defect', including guidance on the community's 'reasonable expectations' of safety. Second, consumers could be better guided on the meaning of a 'safety defect' with respect to consumer IoT devices if the ACCC begins a test case. Typically, the party who has suffered the loss or damage exercises the right to bring an action for goods with a safety defect.[36] However, there is scope for the regulator to bring an action under pt 3-5 of the ACL. The regulator may, 'by application, commence a defective goods action on behalf of one or more persons identified in the application who have suffered the loss or damage in relation to which the action is commenced.'[37] Action by the ACCC, through a test case, may be the best course of action to obtain greater certainty as to the meaning of 'safety defect' when dealing with consumer IoT devices and to safeguard the rights of consumers. The regulator's involvement may be beneficial where the safety defect arises in relation to a consumer IoT device manufactured by a company that is not present in Australia, or where there is a significant power imbalance between the manufacturer and the consumer.

2 Defects existing at the time of supply

A claim under pt 3-5 of the ACL must relate to a safety defect that existed 'at the time when the goods were supplied by their actual manufacturer'[38] and, under s 142(a), it is a defence against a product liability claim under the ACL if the defect arose after the good was put into circulation. Section 142(a) provides that:

> In a defective goods action, it is a defence if it is established that:
>
> a. the safety defect in the goods that is alleged to have caused the loss or damage did not exist:
>
> i. in the case of electricity – at the time at which the electricity was generated, being a time before it was transmitted or distributed; or
>
> ii. in any other case – at the time when goods were supplied by their actual manufacturer.[39]

Given that such connected devices are constantly updated, the 'no defect at time of supply' defence may limit the ability to make claims for safety defects in consumer IoT devices. Connected devices, such as consumer IoT devices, are often subject to compulsory software updates and security vulnerabilities may be introduced via such updates. The resulting continuing relationship between the manufacturer/supplier and the consumer means that the manufacturer's liability should extend to safety defects that come into existence after the goods were originally supplied by their actual manufacturer.

For example, consider where a security vulnerability in a smart lock leads to unauthorised access and damage to private property. Smart locks allow consumers to access their property using a pin code or mobile device. Consumers are generally entitled to expect that a smart lock functions to control access to a property. Provided the security vulnerability is present at the time of sale, manufacturers should be liable for unauthorised access that results in damage. However, what if

[36] ACL s 138.
[37] ACL s 149(1). Note that the regulator 'may only make the application if it has obtained the written consent of the person, or each of the persons, on whose behalf the application is being made.' (s 149(2)).
[38] ACL s 142(1)(ii).
[39] ACL s 142(a).

the security vulnerability arises after the date of supply by the manufacturer, perhaps as a consequence of a security flaw in a software update that the manufacturer distributed after the goods were originally supplied? Would the software update itself be considered a 'good' separate from the consumer IoT device and therefore covered by the product liability regime? Or would a consumer be prevented from bringing an action for a safety defect because the defect arose after the time the manufacturer supplied the goods, even where the safety defect was due to the manufacturer's actions? Given the control that manufacturers have over the development and distribution of software updates, and the fact that, in some cases, updates are installed automatically or required to be installed by the consumer to ensure the continued operation of the device, the responsibility of the manufacturer should extend to cover safety defects that arise as a consequence of any updates.

This issue is under consideration in Europe in the context of the proposed reform of the *Directive on Liability for Defective Products* ('*Product Liability Directive*').[40] The *Product Liability Directive* is a valuable comparator for Australian purposes as it formed the basis of the product liability regime under the ACL.[41] Accordingly, the *Product Liability Directive* contains a similar defence to that set out in s 142(a) of the ACL, providing that a producer will not be liable for a defective product where 'it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterward.'[42] The European Commission has recently published an impact assessment, stating that the Directive was 'unclear about who should be liable for defects resulting from changes to products after they are put into circulation'.[43] While the impact assessment identified a need for further research, the report did propose an option for reform to extend strict liability to address 'defects resulting from changes to products after they have been put into circulation (e.g. software updates or circular economy activities like product refurbishments)'.[44] A similar approach should be considered in Australia to address this gap in the law by extending the product liability regime to cover safety defects that arise as a consequence of changes made to goods after they have been supplied by the manufacturer, such as software updates released by the manufacturers or related parties. Consequently, the defence in s 142(a) of the ACL should be amended to introduce a new sub-section that provides for liability to remain with the manufacturer for safety defects that arose after the time the goods were originally supplied in circumstances where products were subsequently modified or updated by their manufacturer or an associated service provider. Such a provision may be limited to connected devices, such as consumer IoT devices, or could conceivably extend to digital products more generally.

3 Determining liability when a consumer IoT device involves components

[40] *Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products* [1985] OJ L 210/29 ('*Product Liability Directive*').
[41] Law Reform Commission, n 10.
[42] *Product Liability Directive*, n 40, art 7(b).
[43] European Commission, *Inception Impact Assessment: Adapting Liability Rules to the Digital Age and Circular Economy* (Report No Ref Ares(2021)4266516, 30 June 2021) 2 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en>.
[44] European Commission, n 43, 4. A proposal for a Directive on Liability for Defective Products was released for consultation in September 2022. The proposed Directive would make manufacturers liable for defects arising as a consequence of software updates introduced after the product has been made available in the market. Manufacturers would also be 'liable for damage caused by their failure to supply software security updates or upgrades that are necessary to address the product's vulnerabilities in response to evolving cybersecurity risks.' See European Commission, *Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products*, (COM(2022) 495 final, 28 September 2022) Recitals 37-38 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Product-Liability-Directive-Adapting-liability-rules-to-the-digital-age-circular-economy-and-global-value-chains_en>. The consultation period for the proposed Directive closed in December 2022.

Liability for safety defects under the ACL rests with the actual or deemed manufacturer[45] of the good. However, it is a defence under the product liability provisions if it can be established that:

> [I]f the goods that had the safety defect were comprised in other goods – that safety defect is attributable only to:
>
> i. the design of the other goods; or
> ii. the markings on or accompanying the other goods; or
> iii. the instructions or warnings given by the manufacturer of the other goods.[46]

The defence excuses the liability of a component manufacturer where a finished product is defective due to an act or omission of the manufacturer of the finished product, such as careless assembly, using an unsuitable component or the provision of incorrect instructions. In such a case, the manufacturer of the finished product should be liable for any safety defect.

Identifying whether a specific component product causes a safety defect is complicated in relation to consumer IoT devices. As discussed above, consumer IoT devices are complex products that combine hardware, software and associated services. As observed by Dean, 'complex supply chains for the design, manufacture, assemblage, shipping, and sale of these technologies' may complicate the issue of determining and assigning responsibility for defective products.[47] The consumer is unlikely to be aware of, or unable to easily determine, which party in a complex supply chain should be liable for safety defects. It is unreasonable to place such a burden on the consumer. The principles of good product liability regulation, as discussed above, require the apportionment of cost and liability arising in relation to defective products to the party best placed to bear the burden. If a product liability claim involves a consumer IoT device with components, consumers should therefore only be required to bring an action against the ultimate manufacturer or supplier of the finished product, instead of those responsible for components. This would be a more cost-effective and appropriate balancing of rights and responsibilities. It would require the manufacturer or supplier of the finished product to identify and apportion liability for defective products or component products.

B What is the Harm?

Under the ACL, a manufacturer is liable to compensate an individual if the manufacturer supplies goods that have a safety defect and the individual suffers injuries because of the defect, or where other goods, land, buildings or fixtures are destroyed or damaged because of the safety defect.[48] The manufacturer's liability also extends to the loss or damage suffered by an individual other than the injured individual, provided that the loss or damage does not arise as a result of a business or professional relationship.[49] The loss or damage envisaged under the ACL is purely physical. That is the loss that may arise from injuries to an individual or damage to physical property, such as goods, buildings and land.

However, the nature of the loss that may arise due to a safety defect in a consumer IoT device is not limited to physical loss or damage. The most common type of loss or harm that is likely to arise as a result of an insecure consumer IoT device is the loss of data or some other non-physical harm, such as distress arising due to an invasion of privacy. This loss or damage may also involve future, unknown harms – such as financial harm – that may crystallise once a hacker or other third

[45] ACL s 7.
[46] ACL s 142(d).
[47] Dean, n 31, 12–13.
[48] ACL ss 138(1), 140(1), 141(1).
[49] ACL s 139.

party uses the information, such as identity information, obtained via an insecure consumer IoT device at some later date.

There have been a number of high profile stories involving the hacking of insecure Ring doorbells in the United States ('US'). These illustrate the kinds of loss or damage that consumers may suffer due to insecure consumer IoT devices. These cases involve situations where Ring products, including doorbells and security cameras, were hacked, with the hackers speaking to occupants, including children.[50] The class action complaints arising out of these cases have identified numerous examples of hacking, including threats and demands for ransoms. They allege that Ring products are insecure due to a failure to implement basic security measures, such as two-factor authentication or strong passwords.[51] The complainants in these cases claim that, in addition to not being able to use the Ring devices as intended, they have suffered emotional distress and have been exposed to increased risk of theft and fraud in the future. Such emotional distress and future loss or damage would not be covered under the existing product liability provisions under the ACL.

Other cases in the US provide examples of the limitations of existing legal principles when seeking redress for insecure IoT products, particularly when attempting to establish harm. For example, owners of Toyota cars attempted to bring a class action against Toyota Motor Corporation, claiming that their vehicles were vulnerable to hacking due to security vulnerabilities, allowing third parties to take control of their vehicle. None of the plaintiffs established that their vehicles had actually been hacked. Instead, they claimed that 'they would not have purchased their [vehicles] or would not have paid as much as they did to purchase them' had they known about the security vulnerabilities.[52] This case raises the issue of potential future harm. The consumer has purchased a product that, due to security vulnerabilities, continues to pose a risk of future harm, including potential theft, fraud or physical injury. However, the case was dismissed on the grounds that the plaintiffs lacked standing due to the 'lack of injury flowing from the asserted potential hacking issue'.[53] The potential future harm was seen as too speculative, with the plaintiffs failing to establish that they 'face a credible risk of hacking'.[54]

Another case where claims for product liability were dismissed for lack of standing on the grounds of speculative future damage involved car manufacturer Chrysler and alleged insecure infotainment centres.[55] In this case, vehicles produced by Chrysler were vulnerable to hacking via their component 'Uconnect' infotainment centres produced by Harmon International. The ability to remotely take control of the vehicles via the Uconnect system was demonstrated by researchers and documented by reporters in an article published in WIRED.[56] There was no other evidence that a car had been hacked other than the test case car that was the subject of the article. The plaintiffs in this case alleged that the cars were defective as they were 'exceedingly hackable', that they would not have purchased their car had they known of the defect, and that the defect had

[50] See *John Baker Orange on Behalf of Himself and All Others Similarly Situated v Ring LLC and Amazon.com Inc* (CD Cal, Case No 2:19-cv-10899, 26 December 2019) ('*Orange v Ring LLC and Amazon.com*'); *Ashley LeMay, Dylan Blakely, Tania Amador and Todd Craig v Ring LLC* (CD Cal, Case No 2:20-cv-00074, 3 January 2020) ('*LeMay et al v Ring LLC*').
[51] See *Orange v Ring LLC and Amazon.*com, n 50; *LeMay et al v Ring LLC*, n 50. It is acknowledged that two-factor authentication has been mandatory for Ring accounts since 2020.
[52] *Cahen v Toyota Motor Corporation*, 147 F Supp 3d 955, 958 (ND Cal 2015) ('*Cahen v Toyota Motor Corporation*').
[53] *Cahen v Toyota Motor Corporation*, n 52, 958.
[54] *Cahen v Toyota Motor Corporation*, n 52, 969.
[55] *Flynn v FCA US LLC* (SD Ill, Case No 3:15-cv-00855-SMY) ('*Flynn v FCA US LLC*') affirmed, as modified, in *Flynn v FCA US LLC*, 39 F 4th 946 (7th Cir. 2022).
[56] Greenberg, n 4.

diminished the value of their car.[57] The court held that the prospect of future damage was too speculative and that the plaintiffs had failed to establish a concrete injury-in-fact.[58]

Where does this leave consumers who have purchased insecure products, such as insecure security systems, and who now find themselves not only suffering emotional distress following an invasion of privacy, but also loss of data and risk of future harm, including potential theft, fraud or physical injury? While manufacturers may claim to have resolved the security defect through a software patch or other repair, consumers do not have sufficient information to assess whether the risk has been addressed. They are now the owners of a device they do not trust and may be unwilling to use. Who, in these circumstances, is best placed to bear the burden arising as a consequence of such a safety defect? Applying established consumer protection policy principles, the manufacturer should play this role. To address the risks posed by consumer IoT devices, product liability law under the ACL must therefore move beyond the limited scope of physical injury and damage to physical property and, instead, extend to non-physical harms, such as emotional distress or invasion of privacy, damage to intangible property (such as data) and the risk of future harm.

IV PRODUCT SAFETY UNDER THE AUSTRALIAN CONSUMER LAW

In addition to the product liability regime dealing with safety defects outlined above, the ACL includes specific provisions dealing with product safety. Part 3-3 of the ACL sets out a national product safety regime, including provisions dealing with product recalls, product bans, mandatory reporting, product standards and information standards. The product safety regime set out in pt 3-3 has the objective of identifying and removing unsafe products from the market and 'promoting consumer confidence in the market through eliminating risks that cannot be mitigated by market forces alone and, in doing so, to enhance demand'.[59] The most relevant aspects of the product safety regime, for the purposes of this article, are the product recall and mandatory information standard provisions. Reform of both areas has the potential to strengthen protection for consumers of IoT devices.

A Product Recalls to Recognise the Scope of Harm for IoT Consumers

Under the ACL, consumer goods may be recalled, either voluntarily or upon order of the Minister, on the following grounds:

- The consumer goods will or may cause injury to a person;
- A reasonably foreseeable use (including misuse) of the consumer goods will or may cause injury;
- Non-compliance with a relevant safety standard for the consumer goods; or
- A ban on the consumer good is in force.[60]

If a Minister initiates the recall, the Minister must be satisfied that 'one or more suppliers of such goods have not taken satisfactory action to prevent those goods causing injury to any person'.[61]

The ACCC, through Product Safety Australia, provides information on safety issues involving what they refer to as 'interconnected devices'. They observe that:

---

[57] *Flynn v FCA US LLC*, n 55.
[58] *Flynn v FCA US LLC*, n 55.
[59] Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No. 2) 2010 (Cth) [24.16]–[24.17] ('Trade Practices Amendment Explanatory Memorandum').
[60] ACL ss 122, 128.
[61] ACL s 122(1)(c).

[S]afety issues can occur in an interconnected device when:

- a connection to the internet or another product is lost
- a software download corrupts the operating system
- a software update contains a coding error
- a software update designed to fix a safety issue is not received or installed
- the supplier no longer provides software support
- a cyber security breach leads to a third party installing malicious software or remotely controlling a device, or
- a consumer alters the product by installing third party software.[62]

These scenarios can present a real risk of physical injury or harm as well as the potential for other non-physical injuries, such as loss or damage to data, loss of privacy and emotional distress. However, similar to the product liability provisions discussed above, the focus of the rules dealing with recalls is on products that will or may cause physical injury to a person. Since October 2017, 27 smart devices have been recalled.[63] These include products such as smart watches and fitness trackers, location trackers, medical devices, such as connected insulin pumps, and assisting living devices. Most of the recalls have been due to risks of physical harm or failure to function. This may be due to batteries overheating, causing burns or risk of fires, improperly secured button batteries that may pose a risk of choking or serious injury if ingested, or failure of the device to function in the event of network failure. In relation to medical IoT devices, which raise their own specific legal and policy issues, safety issues can interfere with the proper operation of the device, including incorrect administration of medication resulting in potentially serious consequences.

Consider the Ring example presented above, where hackers obtained unauthorised access to internet-connected video doorbells and security cameras. In those cases, the harm did not involve physical injury. Instead, the complainants alleged that, in addition to no longer being able to use the products as intended, they had suffered emotional distress and exposure to increased risk of theft or fraud due to the data breach. This suggests that the recall provisions under pt 3-3 of the ACL should be expanded to encompass situations where consumer goods may cause non-physical loss or damage, such as data loss. While there may be questions about determining the quantum of loss in relation to non-physical harms, this reform is needed to ensure that product safety laws under the ACL are responsive to the full scope of harm that consumer IoT devices may pose.

B Expansion of Information Standards to Address Information Asymmetry

As discussed above, information asymmetries between manufacturers and consumers mean that consumers are often unaware of the security and privacy risks posed by consumer IoT devices. These information asymmetries may be mitigated by using information standards to better inform consumers of the dangers. Under pt 3-3 of the ACL, the product safety regime creates a national information standards scheme that allows the Minister to publish an information standard applicable to goods or services of a particular kind.[64] Information standards concerning a specific product or service may set out the types of information that should be provided to consumers, including the manner and form of such information.[65] It is prohibited to supply goods or services that do not comply with a relevant information standard.[66] There are currently several information

[62] ACCC Product Safety Australia, *Interconnected Devices* (Web Page) <https://www.productsafety.gov.au/products/electronics-technology/interconnected-devices>.
[63] ACCC Product Safety Australia, *Browse All Recalls – Smart Devices* (Web Page, last updated 23 December 2022) <https://www.productsafety.gov.au/recalls/browse-all-recalls?f%5B0%5D=field_psa_product_category%3A4803>.
[64] ACL s 134(1).
[65] ACL s 134(2).
[66] ACL ss 136–137.

standards designated under the ACL, including information standards dealing with the labelling of free-range eggs,[67] warnings on button batteries,[68] labelling of cosmetic ingredients[69] and tobacco labelling.[70]

The objective of the information standards regime, as set out in the Explanatory Memorandum to the Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010, is as follows:

> Information standards are an example of regulatory intervention to address market failure associated with information asymmetry. Lack of information on which to base purchasing decisions can lead consumers to make decisions which are not in their best interests … Information standards … are proactive, requiring a positive standard of information disclosure that the market, on its own, has not provided.[71]

Given the information asymmetry that exists in relation to consumer IoT devices, there may be utility in implementing a mandatory information standard governing the type of information that must be provided to consumers. This could include information relating to the security of such devices, the availability of software updates, and the measures consumers may implement to secure their devices, such as changing default passwords and implementing two-factor authentication. Such an approach could provide consumers with the information to make more informed decisions regarding the potential risks posed by insecure consumer IoT devices.

Similarly, labelling consumer IoT devices has been much debated, with voluntary security labelling schemes adopted in Singapore and Finland. As discussed above in relation to security standards, the Department of Home Affairs is engaging in consultation on cyber security regulations. This consultation also includes whether labelling for smart devices should be introduced, either as a voluntary scheme or a mandatory requirement. As observed by the Department of Home Affairs in their discussion paper *Strengthening Australia's Cyber Security Regulations and Incentives*:

> Labelling schemes can be effective in changing consumer behaviour … and are widely used in Australia for nutritional information and energy, water and fuel efficiency. There is evidence that consumers think that cybersecurity is an important buying consideration and worth paying for. For these reasons, we think that a cyber security labelling scheme could be successful in Australia.[72]

Creating a mandatory consumer IoT device information standard under the ACL may help address the information asymmetries identified above and could support other labelling initiatives, such as those currently under consideration by the Department of Home Affairs.

V CONCLUSION

Consumer IoT devices are complex products that pose challenges for security, privacy and consumer protection law. Market forces alone have been insufficient to ensure that manufacturers implement appropriate security features. The information asymmetry between manufacturers and consumers means that consumers generally do not understand how IoT devices function or the security and privacy risks associated with them. Existing regulation fails to adequately protect consumers from the risk posed by insecure devices or address the resulting harm in the event of a security breach. Reform is necessary to ensure that the ACL is responsive to disruptive

[67] Australian Consumer Law (Free Range Egg Labelling) Information Standard 2017.
[68] Consumer Goods (Button/Coin Batteries) Information Standard 2020; Consumer Goods (Products Containing Button/Coin Batteries) Information Standard 2020.
[69] Consumer Goods (Cosmetics) Information Standard 2020.
[70] Competition and Consumer (Tobacco) Information Standard 2011.
[71] Trade Practices Amendment Explanatory Memorandum, n 59, [23.180]–[23.181].
[72] Department of Home Affairs (Cth), n 8, 36.

technologies, such as consumer IoT devices, and continues to meet the objectives of effective product liability and product safety law, as discussed in this article.

Product liability regimes provide important protections for consumers who purchase unsafe products. Yet there is uncertainty as to how the current product liability regime under the ACL applies to consumer IoT devices, and whether a security vulnerability may constitute a 'safety defect' for the purpose of s 9. In particular, the nature of the reasonable expectation of the public when assessing a safety defect in an insecure consumer IoT device is unclear. Guidance is necessary to provide certainty to consumers and manufacturers, and the ACCC, as the applicable regulator, should be involved in providing consumer guidance and commencing test cases where appropriate. Further, the current product liability regime fails to recognise the full scope of loss or damage that consumers may suffer when an insecure consumer IoT device is hacked. The current product liability regime focuses on physical injury and loss or damage to tangible goods or property. The loss or damage a consumer may suffer as a consequence of an insecure consumer IoT device is likely to include loss or damage to intangible property, such as loss of data, and potential future harm, such as the risk of theft or fraud. Manufacturers and suppliers are best placed to bear the risk of such harm, and reforms are necessary to ensure that manufacturers and suppliers bear the risk of loss caused by their goods, consistent with the principles of good product liability law as outlined by the Law Reform Commission.[73]

Product recalls and mandatory information standards are two mechanisms within the product safety regime established under the ACL that could be better deployed to protect consumers of IoT devices. The product recall provisions set out in pt 3-3 of the ACL should be amended to allow unsafe devices to be removed from the market where they cause physical or non-physical loss or damage, such as data loss. Such an approach would ensure that product safety laws are responsive to the risks posed by new technologies and the full scope of the potential loss suffered by consumers. Furthermore, a mandatory information standard for consumer IoT devices under the existing information standards provisions of the ACL would support consumers in making informed decisions regarding the potential risks posed by insecure consumer IoT devices, and address the significant information asymmetries between manufacturers and consumers. Together, these changes address some of the risks posed by these devices and make the Internet of Things a safer place for Australian consumers.

[73] Law Reform Commission, n 10, 22.