QUT Law Review
Volume 18, General Issue 2 pp. 268–289

ISSN: Online–2201-7275
DOI: 10.5204/qutlr.v18i2.770

MANDATORY DATA BREACH NOTIFICATION AND HACKING THE SMART HOME: A LEGAL RESPONSE TO CYBERSECURITY?

THANAPHOL PATTANASRI*

This paper will investigate whether the Australian legal and regulatory framework sufficiently addresses cybersecurity concerns particular to the smart home. Specifically, the paper will analyse the extent to which the introduction of the data breach notification scheme in Australia will apply to smart home device manufacturers regulated by the federal Privacy Act 1988 (Cth) regarding device breaches. By examining Australian Privacy Principle 11 and the introduction of mandatory data breach notification, the paper aims to determine whether the Australian privacy model of Principles-Based Regulation is capable of providing a market-based solution to cybersecurity concerns in the smart home.

I INTRODUCTION

The law has traditionally recognised the home as a private and passive space, wherein there is a reasonable expectation of privacy.[1] Cory J in the Canadian case *R v Silveira* stated that 'there is no place on Earth where persons can have a greater expectation of privacy than within their dwelling house.'[2] The smart home marks a new frontier in the digital disruption caused by the emergence of the Internet of Things landscape. While the smart home promises users unparalleled freedom and flexibility, there is a risk that the devices converging to create the smart environment may have poor in-built security measures, making infiltration attractive to hackers.[3] The dangers are especially prevalent in a world where smart home devices are becoming progressively interconnected in the amount of data that is transferred and stored between them.[4] The smart home, therefore, presents a primary example of the challenges facing an increasingly digitised society. Given the steady increase in demand for smart home device products, and the relative concerns which have been raised as to their level of security and consumer privacy protection capabilities, the problems presented by the insecurity of data and its systems arise as significant concerns in the smart home environment.[5]

*LLB (Hons) Candidate, The University of Queensland. I would like to thank Dr Mark Burdon (Associate Professor, Queensland University of Technology) for his extensive guidance and support on this article. I am grateful for the comments provided by the two anonymous reviewers, and would also like to thank Ms Ellen Purcell for her comments and assistance. An earlier version of this article was submitted in partial fulfilment of the course requirements in LAWS4114 (Advanced Research) at The University of Queensland. All errors remain my own.

[1] *R v Spencer* (2014) SCC 43; 2 SCR 212; *Rowan v United States Post Office Department* 397 US 728, 737 (1970). See also *Semayne's Case* [1572] EngR 333; *Bostock v Saunders* (1773) 2 Wm Bl 912, 914, which were endorsed in *Monis v The Queen* [2013] HCA 4 [321] – [322].

[2] *R v Silveira* (1995) 2 SCR 297 [140]. See also *Giller v Procopets* [2008] VSCA 236 and *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. This was confirmed by the High Court of Australia in *Monis v The Queen* [2013] HCA 4 [321], where it was recognised as a 'continuing vitality' that the home is considered as one's 'castle', wherein there is an intricate and inherently personal nature to the interactions occurring.

[3] Vijay Sivaraman, Hassan Habibi Gharakheili and Professor Clinton Fernandes, 'Inside Job: Security and Privacy Threats for Smart-Home IoT Devices' (Research Paper, University of New South Wales, 2017) 3.

[4] Megan Richardson et al, 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives' (2017) 6(1) *Internet Policy Review* 1. Cybersecurity matters generally are gaining traction and its importance continues to arise.

[5] See generally Sivaraman et al, above n 3; Angela Daly, 'The Introduction of Data Breach Notification Legislation in Australia: A Comparative View' (2018) 34(3) *Computer Law and Security Review* 477, 478-479. Telstra Corporation Limited, 'Telstra Security Report 2018' (Media Release, April 2018) 45. Telstra notes that, in context of the ongoing trend toward multiple smart devices connections in consumer homes, many devices feature inadequate security measures.

This paper will investigate whether the Australian legal and regulatory framework sufficiently addresses cybersecurity concerns particular to the smart home. Specifically, the paper will analyse the extent to which the introduction of the data breach notification scheme in Australia will apply to smart home device manufacturers regulated by the federal *Privacy Act 1988* (Cth) regarding device breaches. By examining Australian Privacy Principle 11 and the introduction of mandatory data breach notification scheme, the paper aims to determine whether the Australian privacy model of Principles-Based Regulation is capable of providing a market-based solution to cybersecurity concerns in the smart home.

Part II of the paper provides a background to the concept of a smart home, and the cybersecurity threats particular to the smart home environment. In particular, it highlights three threats discussed in the Australian Cyber Security Centre 2017 Threat Report: *Data and Identity Theft, Device Hijacking and Ransomware* and discusses how these may translate to a hacker breaching a smart home network.[6]

Part III of the paper outlines the current legal and regulatory frameworks in place to address the cybersecurity risks identified within the smart home. Focus is placed on the theoretical underpinning of Australia's model of Principles-Based Regulation, and its application into Australian Privacy Principle 11 and the introduction of the mandatory data breach notification scheme.

Part IV of the paper analyses the frameworks introduced in Part III, and their potential application to smart home devices. It is stated that Australian Privacy Principle 11 is unlikely to apply in the smart home environment, and so the introduction of the mandatory data breach notification scheme is analysed to determine whether the scheme may be of potential relief for consumers of smart home devices. Further tensions within the data breach notification scheme and APP 11 are identified, and inconsistencies highlighted. It is argued that the increasing interconnectivity of data in smart home devices does not readily fit within the traditional conception of privacy law frameworks.

Part V concludes the paper by noting that the impact that mandatory notification laws will have on smart home devices remains unknown. Nevertheless, the application of smart home device data breaches to a Principles-Based Regulation approach does not provide a clear market-based solution to the joint rise in the smart home market and the increasing sharing of data between internet connected devices and platforms.

II CYBERSECURITY AND THE SMART HOME

A *Background*

The introduction of the smart phone offered users instantaneous access to information and 'all-in-one functionality', which slowly gained the trust and dependency of its consumers.[7] The smart home finds its natural evolution from this trust and dependency, enlivening the vision to entrench devices and the

These may include unsecured factory default settings and passwords, which can leave consumers vulnerable to hackers easily installing malware to gain access to entire home networks.

[6] Australian Cyber Security Centre, '2017 Threat Report' (Report, Australian Government Australian Cyber Security Centre, 2017).

[7] Kaman Tsoi and Mandy Milner, ''What Can I help You With?': Privacy and the Digital Assistant' (2016) 13(9) *Privacy Law Bulletin* 190. See generally the introduction of the DragonDictate released in 1997 and the release of the iPhone in 2007; See generally Sivaraman et al, above n 3.

'ultimate digital assistant' into the home.[8] The smart home forms part of the broader Internet of Things ('IoT') landscape. While there is a myriad of potential definitions of IoT,[9] in essence it refers to the:

> Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with cloud computing as the unifying framework.[10]

The smart home is concentrated on 'smart connectivity of objects with existing networks and context-aware computation using network resources.'[11] The smart home signals a shift in the increase of invisible infrastructure, where technology is no longer monolithic but now has a malleable duality, capable of constant change.[12] It is a point of intense contact between the user and the device.[13] Through the implementation of smart home devices, the ultimate vision is to create 'ambient computing' in the home where 'smart devices disappear into the background, consumers only [having] to consider the tasks they want performed, and no longer have to consider which device … will be capable of performing that task.'[14] In order to achieve this, various computational nodes ('smart home devices') are connected in the home. Hidden within these smart home devices are advanced technological processes of collection, storage and use.[15] For example, the smart television, with its abilities of content sharing and web browsing, is widely considered a major step towards the convergence of computing and entertainment.[16] Two issues arise in the context of the smart home: the collection, and the consolidation of, information.

1 *Collection and Consolidation of Information*

Smart home devices can be generally categorised into four segments: safety, health, energy and entertainment orientated devices.[17] Manufacturers and software providers of smart home devices, provided they meet the annual turnover requirement of over three million Australian dollars per financial year,[18] may be regulated by the *Privacy Act 1988* (Cth) ('*Privacy Act*') in relation to obligations regarding online privacy and data protection.[19] The manner in which data is collected is

---

[8] Tsoi and Milner, above n 7, 191.
[9] Ibid.
[10] Biljana Risteska Stojkoska and Kire Trivodaliev, 'A Review of Internet of Things for Smart Home: Challenges and Solutions' (2017) 140 *Journal of Cleaner Production* 1454, 1455.
[11] Richardson et al above n 4; Jayavardhana Gubbi et al 'Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions' (2013) 29(7) *Future Generation Computer Systems* 1645.
[12] See Mark Andrejevic and Mark Burdon, 'Defining the Sensor Society' (2015) 16(1) *Television & New Media* 19; See generally David Barnard-Wills, Louis Marinos and Silvia Portesi, 'Threat Landscape and Good Practice Guide for Smart Home and Converged Media' (Research Paper, European Union Agency for Network and Information Security, 1 December 2014).
[13] Barnard-Wills et al, above n 12.
[14] John Davidson, 'Why Your Virtual Assistant Still Needs Some Assistance', *The Australian Financial Review* (online), 26 December 2017, 9.
[15] Andrejevic and Burdon, above n 12; Barnard-Wills et al, above n 12; Sivaraman et al, above n 3.
[16] A smart television can either be smart by design or 'made smart' by connection to a set-top box such as Apple TV.
[17] Rambus, 'Cyber Security in the Era of the Smart Home' (White paper, 2016) 3; Sivaraman et al, above n 3, 5.
[18] *Privacy Act 1988* (Cth) s 6D(1).
[19] Ibid. Stephen Corones and Juliet Davis, 'Protecting Consumer Privacy and Data Security: Regulatory Challenges and Potential Future Directions' (2017) 45 *Federal Law Review* 66-67; Angela Daly, above n 5, 481. A manufacturer will not necessarily be covered by the Act by virtue of the infrastructure constituting a smart home device, in contrast to the nature of application of the Australian Consumer Law (ACL) guarantees, as the scope of the *Privacy Act* is directed at the data such devices collect and share. There has therefore been recognised opportunity for interplay between the *Privacy Act* and consumer protection law through the ACL regime, though Corones and Davis note that a strong link between the two regimes has not been established in practice. It is still considered, though, that the ACL may potentially serve as a useful

generally unobtrusive, in furtherance of the ultimate vision of ambient computing, and consumers of these devices may not necessarily understand the breadth of data collection potentially occurring in a single smart home network.[20] Data is collected and consolidated through a multiplicity of devices to provide the user with 'familiarity', storing consumer preferences such as light brightness in a smart light bulb, or temperature settings in a smart thermostat.[21] Interconnectivity between smart home devices, such as a lightbulb and thermostat, facilitate the objective of ambient computing by creating a network of sensors that detect external elements such as light, temperature and motion.[22] The devices then collect, send and receive data autonomously between each other for ultimate control and monitoring by a smart home user.[23] A consequence of modern data flow is that the data collected and sent from a smart home device will invariably be stored and received through a multitude of international servers. Though beyond the scope of exploration in this paper, considerable difficulties are presented by the regulation of such transnational data transfer, collection and storage.[24] These challenges are many and varied and are of particular prevalence from the perspective of international organisations in consideration of the varying standards for compliance across numerous jurisdictions of operation in which data may be shared.[25]

The unique and varying nature of data collected thus increases an individual's digital trail, and goes 'much closer to knowing and understanding the unique complexities and individual features of human beings' than may be expected.[26] For instance, the Google Home 'may combine personal information from one service with information, including personal information, from other Google services.'[27] The device may combine user data from various sources such as Gmail, Google Drive and the user's web history.[28] The device also offers third party application integration, allowing aggregation of data from platforms such as Uber, Spotify and FitBit.[29]

In order for a smart home to provide ever-present assistance and functionality to users, connected devices must establish a presence in the home alongside other internet connected devices and facilitate the transfer of data between them to perform tasks.[30] A smart home device 'communicates' with other

instrument in the regulation of online privacy and data breaches through public enforcement mechanisms, to supplement the private enforcement mechanisms provided under the *Privacy Act* and administered by OAIC.

[20] Edith Ramirez, 'Privacy and the IoT: Navigating Policy Issues' (Speech delivered at the International Consumer Electronics Show, Las Vegas, Nevada, 6 January 2015) 3 <https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf>; Richardson et al, above n 4, 3.

[21] Scott R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 *Texas Law Review* 85, 108-9.

[22] Office of the Privacy Commissioner of Canada, 'The Internet of Things: An Introduction to Privacy Issues with a Focus on the Retail and Home Environments' (Research Paper, Policy and Research Group of the Office of the Privacy Commissioner of Canada, February 2016) 12.

[23] Ibid; Peter Karcher, 'The Internet of Things: Considerations for IoT Technology Licence Agreements' (2016) 7 *Internet Law Bulletin* 350, 351; See generally Nest Legal Privacy Policy, *Nest Privacy Policy* (17 April 2017) < https://nest.com/au/legal/privacy-policy-for-nest-web-sites/>.

[24] See Angela Daly, above n 5, 477-478; Graham Greenleaf, 'Data Protection in a Globalised Network' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar Publishing, 2013) 221, 244. Daly notes that there is currently a lack of alignment in legal standards across jurisdictions, and to ensure strong international cybersecurity, reform should be cognisant of international trends and harmonious application should be sought. Though an important issue, the transnational aspects of data processing in the smart home are beyond the scope of this paper which focuses predominantly on the Australian position. Detailed separate legal analysis is required of the regulations and trends existing across international jurisdictions to explore these issues in sufficient depth.

[25] Angela Daly, above n 5, 478.

[26] Tsoi and Milner, above n 7, 191.

[27] Ibid; Google, *Privacy Policy* (August 2016) <www.google.com.au/intl/en/policies/privacy/>.

[28] Tsoi and Milner above n 7, 192.

[29] Google, above n 27.

[30] Barnard-Wills et al, above n 12, 5.

devices in a smart home network by relaying data through 'transmissions' which are secured through 'protocols', typically through Wi-Fi in a home gateway router.[31] However, where information is stored and data is capable of being accessed through multiple and potentially unlimited numbers of devices, invariably issues of mixed ownership arise due to the diversity of entities dealing with data on multiple devices and managing the increasing interconnectivity between them. Richard Mason, an information management scholar, foreshadowed in the 1980s that eventually the 'increased collection, handling and distribution of information will pose serious threats to the privacy, accuracy and accessibility of personal information.'[32] The handling of such data stored in a smart home thus raises questions in relation to legal responses to potential hacks, and obligations on entities to provide cybersecurity protocols.[33]

B *Cybersecurity Threats to the Smart Home*

There are three cybersecurity threats which are of particular relevance to the smart home. These are data and identity theft, device hijacking, and ransomware. The Australia Cyber Security Centre ('ACSC') 2017 Threat Report ('the Report') discusses the prevalence of these risks to cybersecurity more generally.[34] The Report emphasises the increasing sophistication in attacks by cyber criminals, but notes that many networks are compromised using 'publicly known vulnerabilities' which have known mitigations.[35] In the context of the smart home, the infrastructure of the devices comprising the home environment may expose the network to shared vulnerabilities.[36] This may arise either from poor cybersecurity protocols in a particular device, or result from outdated software nearing the end of its product life-cycle.[37] Nevertheless, hackers may target these vulnerabilities and infiltrate a smart home network through physical proximity to the home, or remote activation and access of the sensors in the smart devices.[38]

1 *Data and Identity Theft*

The potential for identity theft and crime in internet connected devices is not necessarily particular to the smart home.[39] Data and identity crimes have an estimated annual economic impact of over two billion dollars in Australia; four to five per cent of Australians are victims of identity crime resulting in financial loss annually.[40]

Studies have shown, however, that there is a link between the increase in the amount of personal information stored in a network and the incentive for hackers to breach that network and commit data

---

[31] Sivaraman et al, above n 3, 11.
[32] Richard Mason, 'Four Ethical Issues of the Information Age' (1986) 10(1) *Management Information Systems Quarterly* 5, 6.
[33] Miloslava Plachkinova, Au Vo and Ala Alluhaidan, 'Emerging Trends in Smart Home Security, Privacy, and Digital Forensics' (Paper presented at Twenty-second Americas Conference on Information Systems, San Diego, 2016).
[34] Australian Cyber Security Centre, above n 6.
[35] Ibid 2.
[36] Risteska, Stojkoska and Trivodaliev, above n 10, 1455.
[37] Ibid; Sivaraman et al, above n 3, 23-4; Megan Richardson et al, above n 4.
[38] Barnard-Wills et al, above n 12, 28.
[39] Attorney-General's Department, *Identity Crime and Misuse in Australia 2013-14* (2015) 4 < https://www.homeaffairs.gov.au/criminal-justice/files/identity-crime-misuse-australia-2013-14.pdf>.
[40] Ibid; Explanatory Memorandum, *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) [72], [94]. Telstra Corporation Limited, above n 5, 4**.** Though this figure is widely accepted, it must be noted that the statistic includes a large number of instances of misuse of authority by close intimates, such as the 'borrowing' of a credit card, as opposed to describing instances of cyber-crime by strangers. Worldwide, cybercrime damages have been estimated by Telstra to reach USD $6 trillion dollars annually by 2021.

and identity theft crimes.[41] Although these cyber-attacks can be widespread, smart homes present a more susceptible and attractive target for hackers due to their complex interconnected nature. This is because the sheer volume of data stored in even a small number of connected smart home devices provides more opportunity and incentive for hackers to extract personal information than would be possible from 'less rich data sets'.[42] Where multiple devices are connected on a single smart home network, the network becomes increasingly vulnerable to hacking due to a larger 'attack surface'.[43] Access to one device may provide a hacker with a gateway into all of the smart home devices connected on that network and the data that they store.[44]

The most common method of data and identity theft in the smart home is through credential-harvesting malware, where hackers bypass security protocols through social engineering and 'credential phishing'.[45] The granular data collected in the smart home through a multiplicity of devices compiles to form a unique digital profile of the user. The digital profile is capable of detailing both the consumer's behaviour, such as viewing habits on a smart television or energy consumption on a smart meter,[46] and providing essential information which may be used for document forgery, such as in passports or drivers' licences.[47] Hackers may either use stolen data personally or sell it on dark web marketplaces for use in financial crime or identity theft.[48] The nature of this personal information also appeals to stalkers, who by accessing the data may gain knowledge of a potential target's home and their lifestyle patterns, and may make inferences based on physical proximity.[49]

2 *Device Hijacking*

The purpose of smart home devices is to automate processes and simplify tasks.[50] The hyper-connectivity of devices in a smart home environment necessarily entails high levels of communication and data transfer between different smart devices over a range of protocols and technologies.[51] These protocols contain differing levels of security, and could thus allow a 'weak link' to be identified by a hacker for targeting, allowing them to gain access to the whole smart home network.[52] For example, the Philips Hue lightbulb has been criticised for its poor security, as the bulb does not encrypt data before it is transferred to another device.[53] This may allow a hacker to send commands to override and infiltrate the second device merely by gaining access to the lightbulb.[54] A similar situation may also arise for smart devices with outdated software, which increases the device's susceptibility to a security breach.[55] Studies have shown that many smart home devices are configured with identical or

[41] Attorney-General's Department, above n 39, 23; Ibid [75].
[42] i.e. in smaller networks which collect less data. See generally Ramirez, above n 20.
[43] Sivaraman et al, above n 3, 11.
[44] Ibid 10; Office of the Privacy Commissioner of Canada, above n 22, 21.
[45] Australian Cyber Security Centre, above n 6, 33-4.
[46] Peppet, above n 21, 108-9; Office of the Privacy Commissioner of Canada, above n 22, 13.
[47] Entertainment and lifestyle smart home devices generally have fewer security vulnerabilities. See Sivaraman et al, above n 3, 21; Australian Cyber Security Centre, above n 6, 34.
[48] Australian Cyber Security Centre, above n 6, 34.
[49] Ibid 7.
[50] Davidson, above n 14.
[51] Such as Wi-Fi, Bluetooth and ZigBee. Barnard-Wills et al, above n 12, 20.
[52] Office of the Privacy Commissioner of Canada, above n 22, 21.
[53] Sivaraman et al, above n 3, 18-9.
[54] Ibid.
[55] Hayley Upton, Scott Sloan and Kelli Stallard, 'The 'Internet of Things' Phenomenon and What it Means For Product Liability' (2016) 5 *Australian Product Liability Reporter* 146; Office of the Privacy Commissioner of Canada, above n 22, 21.

substantially similar software and firmware, which increases the potential for a hacker to exploit common vulnerabilities in a range of devices connected on a single smart home network.[56]

Prima facie, individual data from a single smart device such as a lightbulb may not necessarily provide access to a wide range of data on consumer behaviour.[57] However, preferences stored in devices like smart lightbulbs may indicate whether or not a consumer is presently at the home by sending a 'current status' update.[58] This would provide the hijacker with 'a source of close, granular and intimate data on the activities and behaviour' of the smart home's inhabitants.'[59] Further, once a device is hijacked, a 'man-in-the-middle' attack can be made between smart home devices as a result of the 'weak link' in the smart home environment.[60] 'Man-in-the-middle' attacks involve the hijacker making independent connections with various devices and relaying communications between them.[61]

Similarly to cases of data and identity theft, unique data from multiple devices can be obtained via device hijacking, which allows hijackers to gain contextual knowledge about the individuals and inhabitants of a smart home.[62] Pieced together, the inferences made based on learned behaviour have the potential to 'paint a near complete and accurate digital portrait of users.'[63] From utilising this method, a hacker in physical proximity to an infiltrated smart home may remotely access the compromised devices and use this to create a physical attack on the inhabitants. Smart thermostats may be used to increase heating system temperatures and cause pipes to burst by altering user inputs,[64] or surveillance cameras may be remotely turned on to view activities of inhabitants inside the home.[65]

3 *Ransomware*

Ransomware is a method used by financially-motivated hackers to extort funds from victims by blocking access to, or controlling, user data.[66] The method is a persistent and prevalent threat both in Australia and worldwide, with an 'increasing frequency and variation of campaigns' being reported.[67] When this method is applied to a smart home environment, manipulation of data in the devices may be pushed to extremes in the pursuit of revenue generation.[68] For example, distributed denial-of-service ('DDoS') attacks may be made to shut down a home network or tamper with devices.[69] Hackers may then demand a ransom through an internet connected printer to restore access.[70] Alternatively, a hacker who has gained control of a smart home network may orchestrate a physical attack through a smart device and deny inhabitants access to security devices like smart locks or garage openers.[71] Smart televisions are also vulnerable to malicious malware. Malware 'Revoyem' redirects users on smart

[56] Rambus, above n 17, 7.
[57] Barnard-Wills et al, above n 12, 21.
[58] Sivaraman et al, above n 3, 7.
[59] Barnard-Wills et al, above n 12, 55.
[60] Ibid 22.
[61] Ibid.
[62] Ibid 21.
[63] Tsoi and Milner, above n 7, 191-192.
[64] Sivaraman et al, above n 3, 8.
[65] Ibid 9; Office of the Privacy Commissioner of Canada, above n 22, 21.
[66] Australian Cyber Security Centre, above n 6, 26.
[67] Ibid.
[68] Ibid.
[69] Sivaraman et al, above n 3, 9; Barnard-Wills et al, above n 12, 24.
[70] Printers are particularly susceptible to poor cybersecurity protocols. See Sivaraman et al, above n 3, 21.
[71] Office of the Privacy Commissioner of Canada, above n 22, 13.

televisions, through its web browsing facilities, to child-pornographic-themed pages, and demands payment to 'clean' the system.[72]

III LEGAL RESPONSES TO THE SMART HOME

Cybersecurity in Australia is not directly regulated by a single governing piece of legislation. Rather, there exists a patchwork of different laws, regulations and guidelines which regulate conduct and place obligations on 'entities' subject to the *Privacy Act*.[73] Non-compliance with those obligations render an entity liable to punishment and enforcement under the civil penalty framework imposed by the *Privacy Act*.[74] This part of the paper will examine and discuss the current privacy law framework in Australia in relation to potential forms of relief that may be sought by an affected smart home device user following a hack. Specific emphasis will be placed on the rationale of Australia's Principles-Based Regulation framework, reasonable steps to protect personal information under Australian Privacy Principle 11, and the introduction of the mandatory data breach notification scheme.

A *Principles-Based Regulation*

The privacy regime adopted in the Australian model is based on the 1980 Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ('OECD Guidelines').[75] The OECD Guidelines, and hence Australia's regulatory framework of legal obligations in information security, are modelled on Principles-Based Regulation ('PBR'). Australia's adoption of PBR is widely accepted.[76] Of particular interest to this paper is the OECD Guidelines' advancement of the 'security safeguards principle', which states that 'personal data should be protected by reasonable security safeguards.'[77]

PBR distinguishes the regulator from the regulated. In Australia, these most commonly amount to the Office of the Australian Information Commissioner ('OAIC') and the entities subject to the authority of the *Privacy Act.*[78] Julia Black, a leading scholar in PBR, has explained the theory as effectively involving a shift in responsibility from the regulator to the regulatee.[79] The delegation of regulatory function is described as a conscious and deliberate intention by the regulator to influence the regulatee's internal systems of management and control.[80] The delegation of control inherent in this

---

[72] Iain Sutherland, Huw Read and Konstantinos Xynos, 'Forensic Analysis of Smart TV: A Current Issue and Call to Arms' (2014) 11(1) *Digital Investigation Review* 175, 176.

[73] *Privacy Act 1988* (Cth) ss 6C-6D; Jeremy Douglas-Stewart, *Presidian Legal Publications Australian Privacy Law Handbook* (at 25 September 2017) [1.40]; Mark Burdon, Jodie Siganto and Lizzie Coles-Kemp, 'The Regulatory Challenges of Australian Information Security Practice' (2016) 32(4) *Computer Law and Security Review* 623, 626-629.

[74] See *Privacy Act 1988* (Cth) Pt VIB. See also Michael Morris, 'Chapter 5: Australia' in Alan Charles Raul (ed), *The Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, 4th ed, 2017) 49. Maximum penalties of $420,000 Australian dollars for individuals and $2.1 million Australian dollars for corporations can be imposed for 'serious' or 'repeated' offences.

[75] Organisation for Economic Co-operation and Development ('OECD'), 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (OECD, 1980).

[76] Commonwealth, Parliamentary Debates, House of Representatives, 8 November 2000, 22370 (D Williams, Attorney-General); OAIC, 'Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act 1988*' (2005) < https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-reports-archive/getting-in-on-the-act-the-review-of-the-private-sector-provisions-of-the-privacy-act-1988>; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (2008) Chapter 4.

[77] OECD, above n 75.

[78] *Privacy Act 1988* (Cth) ss 6C and 6D.

[79] Ibid.

[80] Julia Black, 'The Rise, Fall and Fate of Principles Based Regulation' (LSE Legal Studies Working Paper No 17/2010) 6.

theory is consistent with 'meta-regulation'.[81] PBR requires and assumes a high level of trust and co-operation on the part of the regulatee to be competent and responsible, maintaining 'regulatory conversation' with the regulator.[82] It reinforces the notion of the 'self-observing, responsible organisation.'[83]

To prevent the market being dis-incentivised, the regulatee, assumedly understanding its own environmental context, self-regulates. It is assumed that these entities, through corporate culture, will maintain a level of corporate social responsibility to consumers, particularly in the form of cybersecurity.[84] The Australian model has been referred to as 'light touch regulation' by its national government, as maximum flexibility is maintained in allowing entities freedom to meet principle-based statutory outcomes by developing innovative forms of compliance.[85] PBR can be contrasted to a hierarchical rule-based regime, where 'bright line' and specific rules are adopted.[86] PBR is argued to provide an advantage over the hierarchical approach by identifying broad principles which encourage compliance with the spirit rather than the letter of the law.[87] The model attempts to prevent the stifling of progress, particularly at the design level, by not burdening entities with obligations to incorporate specific security features to strengthen the protection and integrity of a particular device.[88]

However, the PBR regime has been criticised for allowing regulators to act retrospectively, increasing the level of uncertainty of consumers and regulatees as to their standing regarding current conduct and measures, and reducing predictability of regulatory responses to future disputes. It is argued that PBR provides inadequate protection to consumers by creating a corporate culture of adhering to the very 'minimum level' of compliance, hence failing to afford certainty and predictability to consumers.[89] Key to the successful implementation of PBR, therefore, is the manner in which it is implemented and the institutional context which surrounds it. Without this context, PBR's 'light touch' regulation may lead to a market consensus of risk-taking in the pursuit of profit over product safety,[90] and the use of ineffective compliance systems based on internal organisational control.[91]

B *Australian Privacy Principle 11*

The Australian Privacy Principles (APP) were introduced to the *Privacy Act* under the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*,[92] and commenced operation in 2014.[93] The APPs replaced the now-repealed National Privacy Principles and Information Privacy Principles.[94]

---

[81] Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press, 2nd ed, 2012) 303.
[82] Julia Black, 'Forms and Paradoxes of Principles-Based Regulation' (2008) 3(4) *Capital Markets Law Journal* 425, 432-439.
[83] Ibid 432; Baldwin, Cave and Lodge, above n 81, 303.
[84] Baldwin, Cave and Lodge, above n 81, 303.
[85] Ibid; Australian Law Reform Commission, above n 76 [18.28].
[86] Robert Baldwin and Julia Black, 'Really Responsive Regulation' (2008) 71(1) *Modern Law Review* 59-74.
[87] Australian Law Reform Commission, above n 76 [18.28]; Burdon, Siganto and Coles-Kemp, above n 73, 627.
[88] Rambus, above n 17, 6.
[89] Black, above n 82, 426; Julia Black, Martyn Hopper and Christa Band, 'Making a Success of Principles-Based Regulation' (2007) 1(3) *Law and Financial Markets Review* 191; Cary Coglianese and David Lazer, 'Management-Based Regulation: Prescribing Private Management to Achieve Public Goals' (2003) 37(4) *Law and Society Review* 691. While PBR can facilitate co-operation and an educative approach between the regulator and regulatee, compliance-based principles are also open to abuse and more flexible interpretation by regulatees.
[90] Upton, Sloan and Stallard, above n 55, 146.
[91] Baldwin, Cave and Lodge, above n 81, 305; Black, above n 82, 453.
[92] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
[93] Commenced operation on the 14 March 2014.
[94] Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (Federation Press, 2005) 99.

They are designed as a broad 'technology-neutral approach' for application to current and future technologies, and reflect PBR by acting as 'high-level principles' to guide data management practices of entities regulated under *Privacy Act*.[95] APP 11 does not mandate specific security obligations on entities.[96] Each entity ultimately takes the onus and responsibility of determining how to comply with the APPs in the context of their specific circumstances and the data management practices in which they employ.[97]

In the context of obligations for cybersecurity in the smart home, APP 11 is of most relevance as it relates to security of personal information.[98] APP 11.1 states that if an APP entity 'holds personal information' it must take 'such steps as are reasonable in the circumstances' to protect the information from: 'misuse, interference and loss', as well as 'unauthorised access, modification or disclosure.'[99] 'Personal information' is defined under section 6(1) of the *Privacy Act* as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable.'[100] An entity 'holds' personal information if the information complies with the definition of 'personal information' under section 6(1) and the entity 'has [physical or electronic] possession or control of a record that contains the personal information.'[101]

1 *Such Steps as are Reasonable in the Circumstances*

The Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 states that 'reasonable steps in the circumstances' is an objective assessment, but that 'objectively reasonable steps' depend on the 'specific circumstances of each case.'[102] It is dependent on the relevant risks within an entity and their particular devices.[103] For example, it would be unreasonable to implement high cybersecurity protocols in a device that has low privacy risks where the costs of taking such steps are high.[104] This reflects the underlying reasoning of PBR as the regulated entity is best placed to identify its own risks in its internal environment, and has delegated authority to implement cybersecurity protocols proportionate in cost to these conceived risks.[105]

The *Joint Investigation of Ashley Madison* in 2016 highlights that cybersecurity governance frameworks are assessed with consideration of possible risks faced in the circumstance, and security measures in view of the amount of sensitive personal information held.[106] Failure to take reasonable

[95] Morris, above n 74, 54. See also Mark Burdon, Bill Lane and Paul von Nessen, 'The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU legal developments' (2010) 26(2) *Computer Law and Security Review* 115, 120.
[96] Morris above n 74, 53. The OAIC has released non-binding guidance. See Office of the Australian Information Commissioner, *Guide to Securing Personal Information* (January 2015) <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.
[97] Ibid; *Privacy Act 1988* (Cth) Sch 1 APP 11.1; Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) 86.
[98] *Privacy Act 1988* (Cth) Sch 1 APP 11.1.
[99] Ibid. An 'APP Entity' refers to an entity characterised as falling within the scope of the *Privacy Act* under s 6C.
[100] *Privacy Act 1988* (Cth) s 6(1).
[101] Ibid.
[102] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) 73.
[103] Office of the Australian Information Commissioner, *Vodafone Hutchinson Australia: Own Motion Investigation Report* (16 February 2011) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/vodafone-hutchison-australia>.
[104] *Explanatory* Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) 73.
[105] Baldwin, Cave and Lodge, above n 81, 302-303.
[106] Office of the Australian Information Commissioner and Office of the Privacy Commissioner of Canada, *Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner* (2016) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison#overview-of-investigation>.

steps may also include having a lack of basic security measures in place which could reasonably have been implemented, such as encryption of passwords.[107] Further, the hack of the Sony PlayStation Network in 2011 emphasises that if appropriate security safeguards are in place, an entity may still comply with its data security obligations under APP 11.1 despite a security breach occurring.[108]

2 *'Misuse, Interference and Loss' and 'Unauthorised Access, Modification or Disclosure'*

A 'misuse' occurs where personal information is used for a purpose not permitted by the *Privacy Act*.[109] 'Interference' with personal information arises where the integrity and security of the personal information is compromised, but does not necessarily require modification of its content.[110] This would have application where smart home devices are hijacked but the hacker does not change the basic functionality of the device.[111] The same scenario could also be applied to establish an 'unauthorised access'.[112] A 'loss' is established in this context where there is either a physical or electronic loss of personal information.[113]

3 *Destroy or De-Identify Information*

Under APP 11.2, where personal information is no longer needed by the entity 'for any purpose for which the information may be used or disclosed' the entity must take reasonable steps to 'destroy the information or to ensure that the information is de-identified.'[114] De-identification requires removal of personal identifiers and removing or altering information which may allow an individual to be identified.[115] The costs involved in this process are generally high, so entities may opt rather to destroy information through secure methods, but must avoid unauthorised disclosure during the destruction process.[116]

C *Mandatory Data Breach Notification Scheme*

The Australian privacy model previously operated on a voluntary notification scheme, whereby there was no requirement under the *Privacy Act* to notify affected individuals or the Information Commissioner when a data security breach occurred.[117] This voluntary notification scheme was criticised for underreporting instances of serious data breaches and for excessive delays in notification.[118] The introduction of mandatory data breach notification scheme, which took effect from 22 February 2018, is the result of numerous recommendations by the Australian Law Reform

[107] *Adobe Systems Software Ireland: Own Motion Investigation Report* [2015] AICmrCN 1.
[108] Office of the Australian Information Commissioner, *Sony PlayStation Network/Qriocity: Own Motion Investigation Report* (29 September 2011) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity>.
[109] Douglas-Stewart, above n 73 [7.5090]; Office of the Australian Information Commissioner, above n 96.
[110] OAIC, above n 96.
[111] Rambus, above n 17, 5.
[112] OAIC, above n 96.
[113] Ibid.
[114] *Privacy Act 1988* (Cth) Sch 1 APP 11.2.
[115] Douglas-Stewart, above n 73 [205.105].
[116] Ibid.
[117] Office of the Australian Information Commissioner, *Data breach notification — A guide to handling personal information security breaches* (August 2014) <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>.
[118] Explanatory Memorandum, *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) 69.

Commission ('ALRC') and the OAIC to provide increased transparency to consumers.[119] Mandatory Data Breach Notification ('DBN') emanates principally from California in the United States of America,[120] but has been adopted worldwide from Canada to the European Union and New Zealand.[121] Angela Daly highlights the comparative regimes in the US, which operate in sectors as a 'patchwork of unharmonised data breach notification legislation', to that of the European Union, where, similar to Australia, data breach notification laws operate alongside existing comprehensive data protection laws.[122] It is predicted that notification rates should double in Australia with the introduction of the new scheme for mandatory notification.[123]

The rationale of DBN in Australia is twofold. First, it is so individuals may personally take remedial steps if personal information is compromised, such as by changing passwords to mitigate the potential for identity theft.[124] Second, it encourages entities to be proactive in taking steps to address data breaches and have readily available data breach response plans.[125] DBN recognises that the absence of notification to individuals of data breaches which involve personal information 'does not align with the almost universal agreement from the Australian public that an organisation should inform them if their personal information is lost [or breached].'[126] Australia's new mandatory DBN scheme is enacted under the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.[127] The amendments insert a new Part IIIC into the *Privacy Act*.[128] This was done deliberately in an attempt to streamline the regulatory process.[129] The DBN scheme places an obligation on entities subject to the *Privacy Act* to notify the OAIC and 'affected individuals' as soon as practicable when an entity has reasonable grounds to 'believe' that an 'eligible data breach' has occurred.[130] An 'eligible data breach' occurs where there is a 'data breach', the 'data breach' is likely to result in 'serious harm' to one or more individuals from the perspective of a 'reasonable person', and an exception to the requirement for notification cannot be established.[131] As the relevant entity ultimately determines whether or not an 'eligible data breach' occurs and mandatory notification is required, the DBN scheme is based on the PBR notion of delegated authority.[132] It relies on entities acting responsibly through a detailed 'risk-based analysis' and maintaining regulatory conversation with the OAIC.[133]

---

[119] Australian Law Reform Commission above n 76 [18.28] – [18.55]; Office of the Australian Information Commissioner, *Discussion Paper: Australian Privacy Breach Notification* (November 2012) <https://www.oaic.gov.au/engage-with-us/submissions/discussion-paper-australian-privacy-breach-notification>.

[120] Introduced as 'Senate Bill 1386' in 2003.

[121] See Explanatory Memorandum, *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) [39] and [40].

[122] See Angela Daly, above n 5, 484. See also Mark Burdon, Bill Lane and Paul von Nessen, 'Data Breach Notification Law in the EU and Australia – Where to Now?' (2012) 28(3) *Computer Law and Security Law Review* 296, 297, 302.

[123] Ibid 69. Daly, above n 5, 478. Telstra reported that in 2016, 59 per cent of Australians detected a 'business interrupting security breach' at least monthly.

[124] Ibid [47], [62] and [74]. Burdon, Lane and von Nessen, above n 95, 125 – 126.

[125] Ibid [99]. See also Mark Burdon, Bill Lane and Paul von Nessen, above n 122, 297. Data breach notification laws in general are viewed as addressing the 'multifaceted problems of personal information, inadequate corporate information security measures and the rapid increase of identity theft crimes.'

[126] Ibid [68]; OAIC, 'Community Attitudes to Privacy Survey' (Research Report, 2013) <https://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf> 5.

[127] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).

[128] Ibid.

[129] OAIC, above n 117.

[130] *Privacy Act 1988* (Cth) s 6C; Explanatory Memorandum, *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) [14].

[131] See *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) generally.

[132] Baldwin, Cave and Lodge, above n 81, 308.

[133]Julia Black 'The Emergence of Risk-Based Regulation and the New Public Risk Management in the UK' (2005) *Public Law Journal* 512.

1 *Data Breach*

A 'data breach' occurs under section 26WE(2) of the *Privacy Act* where there is 'unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information.'[134] These terms are not defined in the current *Privacy Act* or new provisions, but are to be given their ordinary meanings.[135] 'Unauthorised access' has been described to occur where personal information is accessed by someone who is not permitted access to that information.[136] This definition is generally intended for external interferences with an individual's personal information stored by an entity. [137] The *Data Breach Guide* refers to unauthorised access as 'databases containing personal information being "hacked" into or otherwise illegally accessed by individuals outside of the agency or organisation.'[138] The terms 'unauthorised disclosure' and 'loss' are generally intended for internal interferences with personal information, and may arise from inadvertence on the part of the entity.[139] Where the entity does not have reasonable grounds to believe an eligible data breach has occurred but 'suspects' one may have, the entity must, within thirty days of developing the suspicion, perform a 'reasonable and expeditious assessment' of the suspected breach under section 26WH.[140] Wilful ignorance will not circumvent an entity's obligations or liability under the new provisions.[141]

2 *Serious Harm*

In order to balance individual and corporate interests, the compliance burden in DBN is reduced to eligible data breaches likely to cause 'serious harm'.[142] The legislative intention for this requirement is to minimise the risk of 'notification fatigue' on the part of individuals and the administrative burden this may place on entities.[143] 'Serious harm' is not defined in the *Privacy Act* but is considered a high threshold.[144] The Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) notes that serious harm may include 'serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation as well as other forms of serious harm'.[145] 'Serious harm' is measured from the perspective of a 'reasonable person in the entity's position' and what they would 'identify as a possible outcome of the data breach.'[146] Section 26WG of the *Privacy Act* identifies a non-exhaustive list of matters relevant in assessing the likelihood of serious harm, including the kind and sensitivity of the information.[147] In determining whether an unauthorised access or disclosure will cause serious harm, the phrase 'likely to occur' is interpreted as

---

[134] Privacy Amendment (Notifiable Data Breaches) Bill 2017 (Cth) 5-7.
[135] OAIC, 'Identifying Eligible Data Breaches' (Government Resource, December 2017) <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches.pdf >.
[136] Ibid.
[137] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 60.
[138] Ibid; OAIC, above n 117.
[139] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 60.
[140] Privacy Amendment (Notifiable Data Breaches) Bill 2017 (Cth) 3-18.
[141] Ibid.
[142] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 36.
[143] OAIC, above n 96.
[144] Australian Law Reform Commission above n 76, [51.14] – [51.40].
[145] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 9.
[146] Ibid.
[147] Privacy Amendment (Notifiable Data Breaches) Bill 2017 (Cth) 10. Relevant matters include, inter alia, the kind of information; the sensitivity of the information; whether the information is protected by one or more security measures; and the nature of the harm.

having to be 'more probable than not'. Overall, whether the data breach is likely to result in serious harm still remains an objective assessment.[148]

3 *Exceptions*

Even if it can be established that an eligible data breach has occurred and serious harm is likely, the data breach may still not be notifiable if the entity can establish an exception to notification such as 'remedial action'.[149] This exception may apply under section 26WF of the *Privacy Act* where an entity takes remedial action prior to notification such that the data breach is no longer perceived likely to result in serious harm to the affected individuals.[150] Whether a data breach is no longer likely to result in serious harm is assessed from the perspective of a reasonable person in the entity's position.[151] If this can be established, the entity is no longer required to notify OAIC or the affected individuals.[152]

4 *'Jointly and Simultaneously' Held Information*

In recognition of the increasing interconnected nature of data transferred and stored between entities and devices, the DBN scheme also includes the concept of 'jointly-held information'.[153] Where more than one entity 'jointly and simultaneously' 'holds' personal information, within the meaning of the term under section 6(1) of the *Privacy Act*, an 'eligible data breach' of one entity also becomes an eligible data breach of the other entities which concurrently hold the information.[154] While 'jointly and simultaneously' remains undefined in the *Privacy Act*, the legislative intention of the phrase is stated to 'potentially arise in cases involving outsourcing, joint ventures or shared service arrangements … for example, if one entity stores personal information in an online platform provided by another entity.'[155] Under general principles of statutory interpretation, the class rule states that general words derive their meaning and colour from the specific words used in the overall expression.[156] When the phrase is read together as a class of words, it is possible that the inclusion of the term 'online platform', while not directly falling within the meaning of outsourcing, joint venture or shared service arrangement, may still be covered under the concept of 'jointly-held information'.

To avoid a double notification requirement, only one entity must inform the OAIC and affected individuals of the data breach.[157] Under section 26WJ, the other entities are not required to also assess the data breach. However, if no assessment is conducted and notification is not complied with, then each entity 'holding' the information will be assumed to have breached the notification requirements under section 26WL(2).[158] Although the scheme does not place the duty of notification on a particular entity, the Commissioner has stated that it is likely the entity which has the most direct relationship with the individual and their personal information will be in the best position to notify the relevant

[148] OAIC, above n 126.
[149] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 19.
[150] Privacy Amendment (Notifiable Data Breaches) Bill 2017 (Cth) 7.
[151] *Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) 9.
[152] Ibid.
[153] Ibid 12-13. See generally OAIC, *Data Breaches Involving More Than One Organisation* (December 2017) <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/data-breaches-involving-more-than-one-organisation>.
[154] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 12-13.
[155] Ibid.
[156] See generally *Quazi v Quazi* [1980] AC 744.
[157] Ibid.
[158] Privacy Amendment (Notifiable Data Breaches) Bill 2017 (Cth)

parties.[159] Once an entity has complied with the obligation, the other entities are relieved of that same duty.

5 *Existing Criticisms of Mandatory DBN: Enforcement and Compliance*

The mandatory data breach notification model has been criticised for its focus on reputational sanctions as its principal regulatory mechanism and has been described as failing to adequately address the aftermath of a data breach in a practical manner.[160] Greenleaf and Clarke have identified a near-universal failure internationally of compliance authorities, including the OAIC, in documenting and publishing statements of data breach complaints as a major contributing factor to issues of transparency in the enforcement and compliance process of such models. [161] Though organisations are required under the scheme to publish notifications of data breaches with respect to affected individuals and the OAIC, it has been argued this alone is insufficient to make details of data breaches available for public attention.[162] Further supplementation of notification under the scheme has been advised in the form of publication on the OAIC website, as part of a permanent, browsable and searchable database, to allow recurrent aspects of breach notification to be identified by interested parties.[163] Such a searchable data base is promoted as likely to exhibit more of a deterrent effect on organisations and more effectively induce improvement of data security measures than is currently observed in compliance activities of regulated parties.[164] Without a public forum in which OAIC can publish statements by affected entities, the 'light touch regulation' envisioned by the PBR may be imbalanced given the lack of 'feedback loops' available to allow consumers to become aware of data breaches, encourage organisational compliance and complaints, and discourage data security breaches.[165]

IV Analysis of Legal Responses

This part of the paper will analyse the legal responses identified in Part III and determine whether those responses are capable of sufficiently addressing cybersecurity concerns in the smart home.

A *Does Data in a Smart Home Device Constitute 'Personal Information'?*

In order for cybersecurity breaches to be regulated under APP 11 or the DBN scheme, the data collected by the relevant smart home device must constitute 'personal information' within the meaning of section 6(1).[166] If the information is not capable of identifying or reasonably identifying an individual, it is outside the ambit of the *Privacy Act.*[167] This question can only be answered on a case-

[159] Ibid.
[160] Burdon, Lane and von Nessen, above n 122, 304. Daly, above n 5, 492.
[161] Graham Greenleaf, 'Australia's Data Breach Notification Bill: Transparency Deficits' (2016) 139 *Privacy Laws and Business International Report* 18, 19; Roger Clarke, Submission to the Commonwealth Attorney-General's Department, November 2012, 3; See Daly, above n 5, 489. There have been concerns, however, that OAIC has received 'insufficient funding and resourcing from the [Australian] government to carry out its functions effectively.'
[162] Greenleaf, above n 161. Greenleaf notes that the MDBN Bill does not require the OAIC to publish and retain all statements about serious data breaches on its website. Greenleaf suggests that unless this published collection of statements comes into existence, the Commissioner's statements will never come to the attention of the public unless published by individuals receiving them.
[163] Roger Clarke, Supplementary Policy on Data Breach Notification Legislation, 4 May 2013, 5.
[164] Greenleaf, above n 161; Clarke, above n 161. Greenleaf states that '[t]he absence of a body of privacy jurisprudence and of examples of significant penalties for non-compliance has made it very difficult for privacy officers and others with an interest in strong privacy compliance to sell the need for compliance measures as a priority even within regulatory/compliance teams, let alone as a wider governance and risk management issue.'
[165] Greenleaf, above n 24, 245.
[166] *Privacy Act 1988* (Cth) s 6(1).
[167] Australian Law Reform Commission, above n 76 [28.104].

by-case analysis. Clearly, the Google Home, which synthesises a user's web history and emails, and is further capable of integrating with third party applications, will constitute 'information … about an identified individual' within the meaning of section 6(1). Even if the information did not explicitly name the individual,[168] the context and sheer volume of information stored about the user would make that individual 'reasonably identifiable'.[169] Additionally, information relayed from a FitBit to the Google Home exposes the device to 'health information' within the meaning of 'sensitive information' under section 6(1).[170] In contrast, the information collected on a smart lightbulb may only store preferences for remote-control lighting, which makes identifying or reasonably identifying an individual challenging. Thus, data stored by some smart home devices such as a smart lightbulb may not necessarily, alone, constitute 'personal information' under the *Privacy Act*. This is particularly so given the Federal Court's recent consideration of the definition and what constitutes information 'about' an individual for this purpose in *Privacy Commissioner v Telstra Corporation Limited*,[171] where, according to some commentators, the qualification may have been narrowed.[172]

The situation of a breached smart lightbulb may change regarding the interpretation of the kind of data involved, however, where a hacker infiltrates a smart bulb and patches through a 'current status' update.[173] The individual would then be reasonably identifiable, as the presence of their physical location can be determined by the hacker. The situation changes again where a hacker uses a breached lightbulb to access other devices in the smart home network, where the other devices carry similar firmware with shared vulnerabilities to the smart bulb. The hacker would then theoretically be able to access a user's home control inputs and devices and commit further attack.[174]

Mark Burdon highlights that while the ALRC's 2008 Report recommended a limited definition of 'personal information', it recognised the purpose of DBN in Australia, alike that in the EU, is more extensive in application than in mitigation of identity theft, the principal approach of the US.[175] As such, Burdon argues that, to achieve this more comprehensive application, the Australian DBN approach must seek to incorporate rather than negate circumstances which are context-dependent.[176] Under this approach, circumstances of breach constituting personal information triggering an obligation to notify may change when a device, which is interconnected with other devices in a smart home network, is breached. This may be so even where the obligation would not exist for breach of the device alone had it not been interconnected.

Therefore, as more smart home devices are connected within a home, the potential for the data stored inside of those devices to constitute personal information increases. Where there are multiple devices,

---

[168] Such as if the consumer used the device under a false name.
[169] *Privacy Act 1988* (Cth) s 6(1).
[170] Ibid. See also generally *My Health Records Act 2012* (Cth) s 75.
[171] [2017] FCAFC 4.
[172] See generally Joshua Yuvaraj, 'How About Me? The Scope of Personal Information under the Australian Privacy Act 1988' (2018) 34(1) *Computer Law and Security Review* 47, 63; ALRC, above n 73, Chapter 6; Pinsent Masons, *'Internet of Things' Data Should be 'Treated as Personal Data', say Privacy Watchdogs* (21 October 2014) <https://www.out-law.com/en/articles/2014/october/internet-of-things-data-should-be-treated-as-personal-data-say-privacy-watchdogs/>. It should be noted, however, that the ALRC stated a broad definition of personal information was not within the scope of the *Privacy Act.* This can be contrasted to the position in the European Union, where data protection authorities generally consider most of the data which is collected by IoT devices to constitute 'personal data' given the enhanced ability to draw inferences about an individual's personal characteristics within a network.
[173] Sivaraman et al, above n 3, 7.
[174] Rambus, above n 17, 5.
[175] See generally Burdon, Lane and von Nessen, above n 122, 303; ALRC, above n 76. See also Flora J Garcia, 'Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time' (2007) *Fordham Intellectual Property, Media and Entertainment Law Journal* 693, 701.
[176] Ibid.

the volume of information stored in the smart home network almost guarantees that the information constitutes personal information under section 6(1) as it is readily identifiable to an individual. Telstra has estimated that the average Australian household contains thirteen internet-connected devices.[177] This figure is set to increase to over thirty devices by 2021.[178] Given the rise of the smart home market in Australia, it is increasingly likely that the data stored in an individual smart device will either constitute 'personal information' alone, or, if not, it will fall within the definition as part of the smart network, due to the greater context provided by additional information from an increased number of devices.[179]

B *Do the Legal Responses Address Cybersecurity Threats to the Smart Home?*

1 *Australian Privacy Principle 11*

(a) APP 11.1

Compliance with APP 11 is ultimately delegated to the regulated entity to interpret and implement protocols in a smart home device.[180] Assuming that smart home device data constitutes 'personal information' within the meaning of section 6(1), an entity may be liable for failure to take 'such steps as are reasonable in the circumstances' in relation to a cybersecurity breach of a device.[181]

The expansion of the smart home market has raised concerns that some manufacturers of smart home devices are prioritising profitability over product development at the expense of product safety in the commercial drive for an increased profit margin.[182] A study which interviewed IoT designers and developers in Australia regarding their perspectives on the growth of the market identified that there are entities in Australia that focus purely on 'innovation' rather than 'privacy in the design of IoT devices.'[183] It was found that these entities aimed for 'quick innovation and pushing new products'; the legal framework 'a lagging indicator into what innovation offers.'[184]

If this reasoning resulted in a market consensus or trend of implementing poor cybersecurity protocols in smart home devices at the design phase in favour of innovation,[185] and that device was breached by a hacker, 'reasonable steps' would be construed in relation to the steps, or lack of steps, the entity had taken to prevent the breach. The focus of the terminology in APP 11.1 is not on the design infrastructure of a breached device, but rather on analysing the security measures at the point of the breach.[186] The use of the terms 'misuse, interference and loss' as well as 'unauthorised access, modification or disclosure' concentrate the analysis on reasonable steps taken at the point of breach, such as incorporating mutual authentication or secure communication.[187]

While the OAIC may determine that an entity did not adequately secure personal information, such as in failing to encrypt data as it is transmitted and transferred to other smart home devices, this does not materially prevent the breach of the device from occurring in the first place. The effectiveness of APP

[177] Sivaraman et al, above n 3, 3. Figure accurate as at 2017.
[178] Ibid.
[179] Upton, Sloan and Stallard, above n 55, 146; Barnard-Wills et al, above n 12.
[180] Burdon, Siganto and Coles-Kemp, above n 73, 626.
[181] *Privacy Act 1988* (Cth) Sch 1, APP 11.1.
[182] Upton, Sloan and Stallard, above n 55, 4-5.
[183] Richardson et al, above n 4, 7.
[184] Ibid.
[185] See Rambus, above n 17, 6.
[186] *Privacy Act 1988* (Cth) Sch 1, APP 11.1.
[187] Ibid; Rambus, above n 17, 8.

11.1 is hence based on the type of security failure which occurs. For example, a DDoS attack which arises from a failure to patch a smart home device's security infrastructure is unlikely to be covered by APP 11.1 as it does not relate to the point of the breach but rather its design infrastructure. The problem of a breach by a hacker is addressed by APP 11.1, not problems of poor design and cybersecurity infrastructure.

The design infrastructure of smart home devices is a significantly important factor because of the interconnected nature of the smart home; poor design infrastructure in a smart lightbulb may provide a gateway for multiple breaches to other devices on the smart home network.[188] Where cybersecurity is ignored at the design level, 'a wide-open door for malicious actors to exploit smart home products' is provided.[189] Thus, in the smart home context, design infrastructure is equally as important as mitigating a breach at the point of its occurrence.

If there are poor cybersecurity protocols in the fundamental design of the smart home device, the only steps an entity would be able to take following release would be steps to mitigate the hacker's threat to the individual.[190] The entity's obligations in these circumstances are reduced as 'reasonable steps' is only interpreted at the point of the breach. APP 11 thus offers individuals a weak remedy when relied on alone in situations of poor cybersecurity design of a smart home device. It rather addresses regulation from the process of 'containment' of a problem than the problem itself. The assumption of a responsible organisation essential to PBR would fail.

(b) APP 11.2

The obligation under APP 11.2 to reasonably destroy or de-identify information 'no longer needed' for 'any purpose for which the information may be used or disclosed by the entity' is unlikely to apply to smart home devices. For a smart home device to provide 'familiarity', a high level of historical data must be collected, consolidated and stored.[191] Generally, the entity will obtain consent for this data storage, express or implied, so that the information is readily accessible by the entity.[192] APP 11.2 is said to be interpreted 'flexibly', only in effect to impose an obligation on entities to 'justify their retention of personal information.'[193] The justification here on the part of smart home device manufacturers would be that historical retention of data is required to effectively compute the functions and activities of the device, particularly in a heterogeneous smart home network.[194]

2 *The DBN Scheme*

(a) Serious Harm

The DBN scheme may operate as a remedy where APP 11 does not apply, or may operate in tandem with the Principle. There are tangible incentives for an entity to avoid notification upon realisation of a potential eligible data breach. The Australian government estimated in the *Draft Early Assessment Regulatory Impact Statement* the total cost of a data breach under the voluntary scheme to amount to nearly three million dollars; around $144 for each stolen or lost record.[195] The cost of mandatory

[188] See generally Sivaraman et al, above n 3.
[189] Ibid 2.
[190] Ibid.
[191] Tsoi and Milner, above n 7, 191.
[192] See *Gao v Victoria Legal Aid (Health and Privacy)* [2012] VCAT 523; *I v Retail Company* [2006] PrivCmrA 8.
[193] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth).
[194] Risteska, Stojkoska and Trivodaliev, above n 10, 1455.
[195] Douglas-Stewart, above n 73 [205.970]; Ponemon Institute, '2016: Cost of Data Breach Study Australia' (Ponemon Report, 2016); Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 93.

notification obligations has been calculated to be a much higher amount overseas.[196] Under PBR reasoning, the obligation of mandatory notification incentivises entities to further invest in data security measures in their devices. This is to prevent cybersecurity breaches from occurring and the need for notification ever arising, as this could cause significant reputational damage on top of the surface and hidden costs that would result from a notifiable breach.[197] The PBR reasoning underpinning DBN does not always align smoothly in the context of smart home devices as establishing the requirement for notification is not always clear.

By focusing on 'data' breaches, an entity may comply with the 'letter of the law' in not reporting 'data' breaches even if a smart home device has been hacked. Two concepts can be distinguished: a hack of a device and a hack of data. A clear hack of data, such as widespread ransomware or physical attack on numerous smart homes, would likely trigger the obligations of the scheme. On the contrary, a hack of a single smart home device is not strictly notifiable as it may not fulfil the requirements of an 'eligible data breach'.[198] While the first limb in establishing a data breach is likely fulfilled given that 'unauthorised access' is interpreted liberally, proving 'serious harm' is considered a high threshold.[199] A hacker may obtain 'unauthorised access' to a smart device, but where they do not modify the content of the device and merely observe the use of information by the inhabitants, it may be difficult to establish 'serious harm'. This sort of breach would have to be established as either 'psychological', 'emotional' or, a more probable than not threat of 'physical' harm to the affected individuals.[200]

Where a hacker obtains unauthorised access to surveillance cameras, 'serious harm' may be established as the private nature of the home and the reasonable expectation of privacy within it is compromised, and the inhabitants are at greater risk of serious physical or psychological harm.[201] Thus, whether breaches of smart home devices that do not necessarily modify 'data' will be notifiable is inherently contextual. The content has to be 'defined by individuals themselves according to context' and not delegated upon an entity to determine from the standard of a 'reasonable person in the entity's position'.[202] The entity may obfuscate its obligation under the DBN scheme in these situations by either remedially acting to shut down the hacker, or avoiding notification to comply strictly with the letter of 'serious harm', but not the spirit of the term.[203] Depending on the method used to infiltrate a smart home or a particular device, these situations would allow hackers who breach smart home devices for stalking purposes to continue without the risk of being compromised. Neither of these situations result in the potentially affected individuals from being able to take remedial steps to protect themselves or increase transparency. This is counter to the intention and purpose of the scheme.[204]

Further, there are issues with quantifying an 'eligible data breach'. The use of the words 'one or more individuals' implies that an 'eligible data breach' may apply to a small household which establishes a smart home network.[205] At the same time, the provisions also militate against the risk of 'notification fatigue' from entities and the corresponding lack of utility for individuals in constant notification.[206] This would suggest the scale of the breach and number of individuals affected remains the primary

[196] Ibid.
[197] Rambus above n 17, 8.
[198] See Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) generally.
[199] ALRC, above n 73 [51.14] and [51.30].
[200] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 9.
[201] See *R v Silveira* [1995] 2 SCR 297, (1995) CanLII 89 [140]. See also *Giller v Procopets* [2008] VSCA 236.
[202] Colin J Bennett and Charles D Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2nd ed, 2006) 9; Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 9.
[203] See Burdon, Siganto and Coles-Kemp, above n 73, 627.
[204] The intention and purpose being to mitigate the threat of data and identity theft and to also increase transparency.
[205] See Douglas-Stewart, above n 73 generally.
[206] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 11.

indicator of whether the eligible data breach is notifiable in the circumstances. Paradoxically, the increase in the scale of a data breach may decrease or diminish the chance of 'serious harm' to each particular individual,[207] and thereby fail the requirement for notification on the second limb of the criterion. Hence, 'eligible data breach' potentially may be inapplicable to both breaches of small smart home networks and large-scale breaches, such as of cloud service providers in the smart home.[208]

(b) 'Jointly and Simultaneously' Held Information

The concept of jointly-held information may have application to interconnected devices in the smart home and the requirement for notification provided the devices 'hold' personal information within its meaning under section 6(1).[209] The application of 'jointly-held information' will inevitably depend on the individual devices in a smart home network and whether the data transfer between these devices constitute outsourcing, joint ventures, shared service arrangements or potentially an 'online platform'.[210] The concept may apply where data is held jointly and simultaneously on a smart home network and a hacker uses a single smart home device to breach the entire network.[211] 'Man-in-the middle' attacks could also trigger notification requirements in these scenarios.[212] For example, 'a data breach involving an individual's name may [increase the risk of serious harm] if the entity's name links the individual with a particular form of physical or mental health care.'[213] The interconnected nature of smart home data places tensions on the conceptions of 'serious harm' and 'personal information', as when information is combined and concurrently accessible through various smart home devices through 'communication' via protocols, the sensitivity of the information increases the risk of 'serious harm'.

C *Are Smart Home Devices Conceptually and Practically Compatible with Australia's Existing Legal Framework?*

The DBN scheme attempts a balancing act between individual and corporate interests.[214] The scheme asserts that individuals have a 'right to know' about unauthorised access to devices storing their information to facilitate mitigation of identity theft and other kinds of access likely to give rise to 'serious harm'. It is designed to protect those adversely affected by security breaches,[215] by letting 'individuals know that their data has slipped into unauthorised hands.'[216] The auxiliary aim is for mandatory DBN to act as a public information disclosure mechanism which improves organisational security control by encouraging sound informational and cybersecurity management as an organisational priority. The regulatory tool is framed with the consequence of reputational sanction.[217]

---

[207] OAIC, above n 135.
[208] OAIC, above n 153.
[209] *Privacy Act 1988* (Cth) s 6(1).
[210] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 12-13.
[211] See generally Sivaraman et al, above n 3.
[212] Barnard-Wills et al, above n 12, 22.
[213] cf OAIC, above n 135.
[214] Sara A Needles, 'The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law' (2009) 88 *North Carolina Law Review* 267, 281; Paul M Schwartz and Edward J Janger, 'Notification of Data Security Breaches' (2007) 105 *Michigan Law Review* 913, 918.
[215] Thomas Smedinghoff, 'Trends in the Law of Information Security' (2005) 17 *Intellectual Property and Technology Law Journal* 1, 4.
[216] Needles, above n 214, 281.
[217] Ibid 78-80.

In applying these aims, the contextual environment and its 'social application' is crucial.[218] Consumers of smart home devices have a reasonable expectation of end-to-end secure connectivity.[219] In a smart home network, a hacker may infiltrate a home automation system and manipulate appliances to cause physical and emotional attack. As more devices are connected to a smart home network, the accumulation of risks increases, and the interconnectivity between these devices is capable of causing problems such as uncoordinated administrators and differences in administrator preferences.[220] Information stored on these devices is also potentially accessible to an unlimited number of devices.[221] This raises tensions as to whether the consumer expectation that a single smart home device will not 'create a backdoor to other devices in their home' remains achievable.[222]

V CONCLUSION

Since the enactment of mandatory DBN in February 2018, there have been 550 notifications reported as at the June to September 2018 Quarter.[223] Of this total, 57 per cent were from malicious or criminal attacks, with the largest sources subject to notification being health service providers and the finance sector.[224] To date, there have been no specific reported instances of notification in relation to smart home devices and as such security standards are yet to be enforced by the Commissioner.

It still remains to be seen how the DBN scheme and the introduction of the concept of 'jointly-held' information will be applied to breaches of smart home devices in Australia. Entities may no longer conceal cybersecurity breaches that have compromised their networks where an eligible data breach can be established and no relevant exceptions apply.[225] In this regard, mandatory DBN may provide greater potential relief to affected consumers of smart home devices by creating a trend of increased transparency. Despite early criticisms of its practicality and enforceability, the scheme is therefore a welcome contribution to Australia's data breach notification regime.[226] The benefits would be increasingly realised if, as recommended by various commentators, the OAIC were to implement a searchable public database recording notifiable data breaches to encourage organisational compliance to the scheme.[227]

Mandatory DBN attempts to advance overarching objectives of deterrence, mitigation, transparency through information and public confidence.[228] There are clear advantages and disadvantages of the merging of the DBN scheme with the current legal and regulatory privacy framework, and these are brought to the forefront in the context of smart home device breaches. The merge highlights 'vertical tensions' and 'shared horizontal weaknesses' between the current privacy law framework and the

---

[218] Bennett and Raab, above n 202, 9.
[219] Rambus, above n 17, 8.
[220] Upton, Sloan and Stallard, above n 55, 6.
[221] Barnard-Wills et al, above n 12.
[222] Sivaraman et al, above n 3, 23.
[223] OAIC, *Notifiable Data Breaches Quarterly Statistics Report: 1 July – 30 September 2018* (30 October 2018) <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/notifiable-data-breaches-quarterly-statistics-report-1-july-30-september-2018.pdf>; OAIC, *Notifiable Data Breaches Quarterly Statistics Report: 1 April – 30 June 2018* (31 July 2018) <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018.pdf>; OAIC, *Notifiable Data Breaches Quarterly Statistics Report: January 2018 – March 2018* (April 2018) <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/Notifiable_Data_Breaches_Quarterly_Statistics_Report_January_2018__March_.pdf>.
[224] Ibid
[225] See Privacy Amendment (Notifiable Data Breaches) Bill 2017 (Cth) 7.
[226] Daly, above n 5, 495.
[227] Clarke, above n 163; Greenleaf, above n 161; Clarke, above n 161.
[228] OAIC, above n 117.

introduction of the DBN scheme.[229] Vertically, there are inconsistencies in application of the DBN scheme, as an increase in the number of affected individuals may decrease the risk of 'serious harm' to each individual. The risk of 'serious harm' increases, however, in situations where information is 'jointly-held' and each individual is deemed to be more at risk. Horizontally, the adherence to PBR and 'light touch regulation' allows entities subject to the *Privacy Act* to dictate the terms in which smart home devices are designed and administered potentially without regard to cybersecurity protocols. While mandatory data breach notification may help to foster organisation culture and corporate social responsibility centred around privacy and security,[230] it may simultaneously encourage increased risk-taking, poor design level security protocols and 'creative compliance'.[231]

The extent to which the DBN scheme may apply to smart home device breaches is uncertain, but it is also unlikely to have much, if any, impact for breaches of small smart home networks. This is because the introduction of the scheme, whilst enforcing notification for serious breaches of some devices, may not prevent individual data breaches for other devices in a smart home network from becoming notifiable. There are issues with the conceptualisation of the definition of 'personal information' under the *Privacy Act*.[232] The data collected by a smart home device, in its retention of personal preferences for automation of certain functions of the home, does not neatly fit under 'personal information' or 'sensitive information' within the meaning of section 6(1).[233] The focus of the DBN scheme on 'data' may also allow an entity to obfuscate its obligations of mandatory notification by complying with the 'letter' of the scheme rather than its spirit. The most viable use for the scheme in relation to the smart home is its application to the concept of 'jointly-held information', which lacks historical legal basis. The interconnectivity of devices highlights unchartered territory in cybersecurity and an attempt to achieve legal certainty in an inherently uncertain area.[234] Questions surrounding obligation and liability will inevitably arise as the concept of 'jointly-held information' gains traction and smart home devices become outdated and extend beyond their intended product life-cycle.[235]

This paper has argued that, while attempting to balance conflicting interests between individuals and entities,[236] the DBN scheme raises questions over the continuing viability of PBR in the wake of digital disruption. Gartner Consulting predicts that the smart home market is between five to ten years away from maturity.[237] The global smart home market is projected to be worth around forty billion dollars by 2020.[238] It is possible that a principle-based approach which allows overwhelming flexibility to the regulated entity is no longer feasible, as there may be no market-based solution to the issue of poor cybersecurity.[239] A more prescriptive approach which specifies mandatory minimums and is less focused on ensuring flexibility for entities, or an approach which focuses on cybersecurity more generally rather than an emphasis on 'data', may be more tenable alternatives to traditional PBR in the rise of the smart home.[240]

---

[229] Mark Burdon, 'Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws' (2010) 27(1) *Santa Clara High Technology Law Journal* 63, 66 and 128-129.
[230] OAIC, above n 117.
[231] Baldwin, Cave and Lodge, above n 81, 303-309; Burdon, Siganto and Coles-Kemp, above n 73, 625-627.
[232] *Privacy Act 1988* (Cth) s 6(1).
[233] Ibid.
[234] Sivaraman et al, above n 3, 23; Barnard-Wills et al, above n 12.
[235] Sivaraman et al, above n 3, 23.
[236] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth); Needles, above n 214, 279-281; Schwartz and Janger, above n 214, 918.
[237] Davidson, above n 14.
[238] Rambus, above n 17, 2.
[239] Sivaraman et al, above n 3, 23.
[240] Richardson et al, above n 4, 8-9; Burdon, Siganto and Coles-Kemp, above n 73, 627. See generally New York State Department of Financial Services, *23 NYCRR 500: Cybersecurity Requirements for Financial Service Companies* (28 August 2017) <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf>.