The introduction of data breach notification legislation in Australia: a comparative view

Angela Daly[i]

PRE-PRINT OF ARTICLE FORTHCOMING IN COMPUTER LAW & SECURITY REVIEW, 2018

Abstract

This article argues that Australia's recently-passed data breach notification legislation, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), and its coming into force in 2018, makes an internationally important, yet imperfect, contribution to data breach notification law. Against the backdrop of data breach legislation in the United States and European Union, a comparative analysis is undertaken between these jurisdictions and the Australian scheme to elucidate this argument. Firstly, some context to data breach notification provisions is offered, which are designed to address some of the problems data breaches cause for data privacy and information security. There have been various prominent data breaches affecting Australians over the last few years, which have led to discussion of what can be done to deal with their negative effects. The international context of data breach notification legislation will be discussed, with a focus on the United States and European Union jurisdictions which have already adopted similar laws. The background to the adoption of the Australia legislation will be examined, including the general context of data privacy and security protection in Australia. The reform itself will be then be considered, along with the extent to which this law is fit for purpose and some outstanding concerns about its application. While data breach notification requirements are likely to be a positive step for data security, further reform is probably necessary to ensure strong cybersecurity. However, such reform

should be cognisant of the international trends towards the adoption of data breach notification, but lack of alignment in standards, which may be burdensome for entities operating in the transnational data economy.

1. Introduction

The Australian Parliament finally passed legislation to implement mandatory data breach notification requirements in Australia in early 2017, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).[1] This legislation, which amends the *Privacy Act 1988* (Cth), establishes a notification scheme for certain kinds of data breaches, involving unauthorised access to, or disclosure of, personal information which is likely to lead to serious harm to the individuals whose personal information has been compromised. These measures can be conceptualised as pertaining to a larger body of law and policy in Australia concerning cybersecurity, which is emerging as a priority area for government and business with their growing reliance on digital technologies and data gathering.[2]

This article examines the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), and its context. Firstly, the phenomenon of data breaches will be explained, including some of the prominent recent breaches which have impacted Australian organisations and citizens. Then the concept of data breach notification laws will be introduced, with reference to existing measures in the United States (US) and European Union (EU). The focus will then turn to Australia, where existing privacy and information security laws relevant to breaches will be identified, before the new legislation is considered. The extent to which the new Australian law is fit for purpose and is in line with international best practice will be determined, before some concluding thoughts are offered.

---

1 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) ('*Notifiable Data Breaches Act*').

2 See, eg, Chris Brookes, 'Cyber Security: Time for an Integrated Whole-of-Nation Approach in Australia' (Indo Pacific Strategic Papers, Australian Defence College, March 2015) <http://www.defence.gov.au/ADC/Publications/IndoPac/150327%20Brookes%20IPS%20paper%20-%20cyber%20(PDF%20final).pdf>.

Overall, the data breach notification requirements contained in *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) are a welcome addition to the body of Australian legislation pertaining to data privacy and cybersecurity. However, this body of legislation cybersecurity requires a more comprehensive update to address privacy and cybersecurity threats, which data breach notification legislation alone is not able to achieve. Furthermore, the emergence of legislative data breach notification obligations in different globally prominent jurisdictions which are not harmonised may be burdensome from a compliance perspective for entities operating in the transnational digital economy.

2. Data Breaches: Defined and Detailed

In legislative data breach notification requirements, there are differing definitions of 'data breach' (especially from different jurisdictions or legislation pertaining to different industry sectors) but broadly speaking data breaches involve security breaches which lead to the disclosure, access or acquisition of information. Often data breach notification requirements pertain to information which is personal but this is not always the case. Such breaches can happen for a number of reasons, including malicious external hacks of stored data, insider threats in the form of information being accessed for an unauthorised purpose, and accidentally or as a result of human error or incompetence. Data breaches can also occur as a result of a physical media object such as a computer or hard drive containing sensitive unencrypted data being stolen or lost. Another scenario is the posting, whether deliberate or accidental, of sensitive data to a publicly-accessible website or on a computer accessible via the Internet. Verizon's global Data Breach Investigations Report from 2016 found that 95% of breaches were attributable to nine patterns - most prominently miscellaneous errors, and insider and privilege misuse, which mostly affected the public sector, healthcare, information and administrative sectors.[3]

Data breaches can involve information about identifiable individuals which falls within the definition of 'personal information' as per section 6(1) of the *Privacy Act 1988* (Cth) ('*Privacy*

[3] Verizon, '2016 Data Breach Investigations Report' (Report, 2016) 4–6.

Act') in Australia, but can also involve information not about identified individuals or individuals who are reasonably identifiable that may fall within trade secrets protection or intellectual property protection.[4] The amendments to the Australian federal *Privacy Act*, the '*Notifiable Data Breaches Act',* are concerned with data breaches involving personal information, which is thus the focus of this article.

Data breaches are imposing significant costs on Australian businesses: the average cost of a data breach for a company has been estimated at $2.64 million.[5] In 2016, 59% of Australian organisations detected a 'business interrupting security breach on at least a monthly basis'.[6] As mentioned above, there have been a number of recent cases of major data breaches involving Australia or Australians' personal information in some way. One example is the major Yahoo hack, which involved 1 billion victims globally whose information had been compromised by hacks in 2013 (but the fact of the breach was only revealed in 2016), and specifically in Australia reportedly affected 'thousands of Australian Government officials, including high-profile politicians and senior Defence officials'.[7] Another significant hacking event concerned the Ashley Madison website, a service for adults seeking extramarital relationships headquartered in Canada but operating globally, which culminated in a joint investigation by the Australian federal Privacy Commissioner and the Office of the Privacy Commissioner of Canada with each body finding infringements of its respective jurisdiction's data privacy laws.[8]

Other data breaches have involved Australian Government agencies directly. In 2014, the Department of Immigration and Border Protection inadvertently published the personal details

---

4 See, eg, Elizabeth Rowe, 'RATs, TRAPs, and Trade Secrets' (2016) 57 *Boston College Law Review* 381.

5 Ponemon Institute, '2016 Cost of Data Breach Survey: Australia' (Research Report, June 2016) 1 <https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094auen/SEL03094AUEN.PDF>.

6 Telstra, 'Telstra Cyber Security Report 2017' (Research Report, Telstra, 2017) 2 <https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/pdf/cyber-security-whitepaper.pdf>, quoted in Commonwealth, 'Australia's Cyber Security Strategy: First Annual Update 2017' (Strategy Paper, Department of the Prime Minister and Cabinet, 2017) 8 <https://cybersecuritystrategy.dpmc.gov.au/cyber-security-strategy-first-annual-update-2017.pdf>.

7 Benjamin Sveen, 'Yahoo Hack: Email accounts of Australian Politicians, Police and Judges Compromised in Massive Breach, Dataset Reveals', *ABC News* (online), 17 January 2017 <http://www.abc.net.au/news/2017-01-17/senior-australian-politician-among-victims-of-massive-yahoo-hack/8185162>.

8 Australian Government Office of the Australian Information Commissioner, *Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner* https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madisonf

of 9250 asylum seekers in a document online, which remained accessible for eight and a half days until it was discovered and removed.[9] The Australian Government has recognised the data privacy concerns raised by such breaches, and also acknowledged that most of these breaches 'were not due to network compromises, but the rest of complacency and failures in the delivery and management of ICT services and information'.[10]

Yet it is not only government agencies affected by data breaches. In 2016, what was described as 'Australia's largest security breach' involved the personal data of 550,000 blood donors held by NGO Australian Red Cross inadvertently being publishing to a public website by the employee of a third party contractor.[11] The federal Privacy Commissioner investigated the breach, and found breaches of the *Privacy Act*, specifically Australian Privacy Principle (APP) 11 protecting the security of information.[12] Due to the haste with which the Australian Red Cross responded to the breach and its actions to rectify the consequences of the breach, the Privacy Commissioner did not impose a fine and indeed identified the Red Cross's response as a 'model of good practice for other organisations'.[13] In addition, Australian businesses including Aussie Travel Cover, Kmart and David Jones have also been the targets of malicious external attackers accessing data they held.[14]

---

9 'Immigration Department Breached Privacy of 9,250 Asylum Seekers by Publishing Their Details Online', *ABC News* (online), 12 November 2014 <http://www.abc.net.au/news/2014-11-12/immigration-department-breached-privacy-of-9250-asylum-seekers/5885326>.

10 Commonwealth, above n 6, 9.

11 'Red Cross Blood Service Admits to Personal Data Breach Affecting Half a Million Donors', *ABC News* (online), 28 October 2016 <http://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036>.

12 Australian Government Office of the Australian Information Commissioner, *DonateBlood.com.au data breach (Australian Red Cross Blood Service)* Investigation Report (7 August 2017) < https://www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/donateblood-com-au-data-breach-australian-red-cross-blood-service.pdf>

13 Ibid, 2

14 Will Ockenden and Benjamin Sveen, 'Aussie Travel Cover has Hundreds of Thousands of Records Stolen in Hacking, Policy Holders Not Informed', *ABC News* (online), 20 January 2015 <http://www.abc.net.au/news/2015-01-19/aussie-travel-cover-hacked-customers-not-told/6025652>; Marc Moncrief, 'Kmart Online Customers' Information Hacked in Security Breach', *Sydney Morning Herald* (online), 1 October 2015 <http://www.smh.com.au/business/retail/kmart-online-customers-information-hacked-in-security-breach-20150930-gjyoxe.html>; Will Ockenden, 'David Jones Computer System Hacked and Customers' Private Details Stolen', *ABC News* (online), 2 October 2015 <http://www.abc.net.au/news/2015-10-02/david-jones-computer-system-hacked-customer-details-stolen/6824170>.

As can be seen from the above, data breaches are affecting organisations in the public, private and not-for-profit sectors in Australia and internationally. As more aspects of society become digitised, the problems presented by insecurely-held data and insecure systems also become more evident and potentially debilitating. This can be evidenced by the effects of cyberattacks such as the 'WannaCry' ransomware attack in May 2017, which infected tens of thousands of computers worldwide, including some belonging to the UK National Health Service which resulted in some of its health services being suspended during the attack.[15] The new Australian data breach notification requirements can be seen as one measure contributing to a large body of cybersecurity legislation and policy in Australia and internationally, as actions which attempt to address data security concerns.

3. Background to data breach notification laws

One measure to respond to such data breaches is laws implementing disclosure obligations incumbent on the organisation which has suffered a breach, to inform individuals whose data has been compromised, as has now been adopted in Australia via the '*Notifiable Data Breaches Act'*.

There has been a global trend towards enacting such laws in recent years.[16] The State of California was the first jurisdiction to implement data breach laws in 2003.[17] This was followed by the enactment of similar laws in other US states, and then in other globally important jurisdictions including the European Union.[18] More recently, China adopted a new

---

15 Tracy Marshall, Sheila Millar and Nathan Cardon, 'WannaCry: Are Your Security Tools Up to Date?' *National Law Review*, 22 May 2017, <https://www.natlawreview.com/article/wannacry-are-your-security-tools-to-date>.

16 See World Law Group, 'Global Guide to Data Breach Notifications' (Report, Second Edition 2016) i.

17 Cal Civ Code §1729.98 (West 2010).

18 See, eg, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* [2002] OJ L 201/37 ('*ePrivacy Directive*') – discussed in more detail below.

Cybersecurity Law in mid-2017, comprising its first comprehensive national information privacy and security regulation, which includes data breach notification requirements.[19]

More detail will be given on the comparative picture for data breach notification legislation in the following section. Here, some background to why data breach notification laws have been adopted is offered, their theoretical basis and connection with other legal regimes.

3.1 Justifications for data breach notification laws

Overall, the theory behind data breach notification laws is that consumers have the right to know when their personal information has been compromised, and that these laws will provide incentives for organisations to take adequate steps to protect the personal information they hold.[20] There are various arguments in favour, and against, implementing data breach notification laws.

One argument in favour is that of transparency: that making information about breaches publicly known is important in itself, but it may also have the effect of altering internal organisational practices in the entity which has suffered the breach,[21] and may also have flow-on effects for all organisations' data security and protection practices.[22] Another argument in favour of such laws takes an individual-centric view, and rests on the right of individuals to know that their data has been compromised since this gives them the opportunity to take

---

19 Gabriella Kennedy and Xiaoyan Zhang, 'China Passes Cybersecurity Law' (2017) 29(3) *Intellectual Property & Technology Law Journal* 20; Graham Greenleaf and Scott Livingston, 'China's New Cybersecurity Law – Also a Data Privacy Law?' (2016) 144 *Privacy Laws & Business International Report* 1. A detailed account of the Chinese cybersecurity legislation and its impact is beyond the scope of this article, but is an important topic for further research.

20 Alana Maurushat, 'Data Breach Notification Law across the World from California to Australia' (2009) *Privacy Law and Business International* 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1412063##>.

21 Paul Schwartz and Edward Janger, 'Notification of data security breaches' (2007) 105(5) *Michigan Law Review*, 913, 955.

22 *Data Breach Laws Make Companies Serious About Security* (7 September 2009) Berkley Law, University of California <https://www.law.berkeley.edu/article/data-breach-laws-make-companies-serious-about-security/>.

mitigation measures to minimise harm to their personal information from the data breach e.g. preventing/mitigating identity theft[23] – which may have flow-on benefits to the organisation holding the information in terms of reducing their costs vis-à-vis the breach.

Arguments against the enactment of data breach notification laws include: the questionable effectiveness of such laws in achieving their purpose; the costs to organisations of notification; the stifling of innovation by discouraging firms to innovate by using their customers' personal data;[24] and the concern that individuals will not actually act on data breach notifications, particularly if they become too desensitised to such notifications by receiving too many notices.[25]

It is difficult to judge how accurate justifications for and against data breach notification requirements are in practice due to the limited empirical research conducted on their efficacy. The limited, extant research has mainly been conducted by a team from Carnegie Mellon University: Romanosky, Telang and Acquisti estimated the impact of data breach notification laws in the US on identity theft between 2002 and 2009, and found that adopting such laws reduced identity theft caused by data breaches by 6.1% on average.[26] This is consistent with further research in the form of an economic analysis of data breach notification laws conducted by Romanosky, Sharp and Acquisti, which found that while such schemes could increase costs to organisations, these organisations could also increase their investment in security measures which may lower social costs overall, and they also found that the disclosure of breaches could induce consumers to increase their own level of care as regards their personal information.[27]

---

23 Sasha Romanosky, Rahul Telang and Alessandro Acquisti, 'Do Data Breach Disclosure Laws Reduce Identity Theft? (Updated)' (2011) 30(2) *Journal of Policy Analysis and Management* 256, 257.

24 Thomas M Lenard and Paul H Rubin, 'Slow Down on Data Security Legislation' (Progress Snapshot No 1.9, Technology Policy Institute, August 2005) 3 <https://techpolicyinstitute.org/wpcontent/uploads/2005/08/slow-down-on-data-security-leg-2007064.pdf>; Thomas M Lenard and Paul H Rubin, 'Much Ado about Notification' (2006) 29(1) *Regulation* 44, 46.

25 Fred H Cate, 'Another notice isn't answer', *USA Today* (online), 27 February 2005 <http://usatoday30.usatoday.com/news/opinion/2005-02-27-consumer-protection-oppose_x.htm>.

26 Romanosky, Telang, and Acquisti, above n 23, 260.

27 Sasha Romanosky, Richard Sharp and Alessandro Acquisti, 'Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?' (Paper presented at the Ninth Workshop on the Economics of Information Security, Harvard University, 7 July 2010) 2.

This empirical research suggests that data breach notification laws may have an overall positive effect on encouraging better data security practices and preventing identity fraud. However, there is clearly a need for more systematic research to be conducted into the impacts, intended and unintended consequences of these laws, and in jurisdictions outside of the US which do have comprehensive data protection laws, such as the EU - and now Australia.

3.2 The relationship between personal data breach notification and data privacy laws

There are similarities between data breach notification laws concerning breaches of personal information and laws protecting data privacy since they usually both involve legislative provisions relating to the protection of personal information, seek to foster better security practices and provide individuals with information about how their data is stored and used.[28]

However, there are important conceptual differences between these laws, including their original rationales, the market-based nature of data breach laws which are 'cognizant of corporate compliance cost burdens' and (originally) designed to mitigate identity theft especially in the US, compared to the rights-based protections for individual interests encompassed by more comprehensive information privacy laws.[29] Burdon also notes that both kinds of laws also share certain common weaknesses because they focus unduly on the type of information regulated rather than the broader social contexts and relationships involved in the gathering and exchange of personal information.[30] This has entailed that both data breach notification laws and data privacy laws in jurisdictions such as the US and EU are based on chains of accountability comprising providers, collectors and re-users of personal information, a chain which is too simplistic for the complex reality of information gathering and exchange in the various contexts in which this occurs.[31]

---

28 Mark Burdon, 'Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws' (2011) 27(1) *Santa Clara Computer and High-Technology Law Journal* 63, 65.

29 Ibid 66, 86. Although Lynskey recognises the 'hybrid' nature of EU data protection law, as both a rights-based regime, and also as laws facilitating the economic trade of personal data within the European Single Market. See Orla Lynksey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015) 8–9.

30 Burdon, above n 28, 66.

31 Ibid 98.

In practice, as will be detailed in the next section, data breach notification legislation has been implemented in jurisdictions which both have existing comprehensive data protection laws (such as the EU, and, more recently, Australia) and also in jurisdictions where there are no comparable comprehensive laws (such as the US).

3.3 The relationship between data breach notification and consumer protection laws

Another connection can be made between data breach notification laws and consumer protection law. As will be seen in the following section, the US Federal Trade Commission (FTC) has adopted a strong role in regulating consumer privacy in its jurisdiction, using its broad authority to prohibit unfair or deceptive practices within which the FTC has included data breaches and notification.[32] The flexibility of consumer protection law provisions and lack of comprehensive federal data privacy law in the US may be factors contributing to the FTC's activities in this area.

A strong link has not been established in practice between data breach notifications and consumer protection law in other jurisdictions, which may be related to the generally diminished role consumer protection has played regarding data so far, a possible consequence of the presence of data privacy laws in these places. However, conceptually the link between data breaches and consumer protection is increasingly being recognised. In the EU, the tardiness of consumer law to consider the digital economy matters has been acknowledged,[33] as well as its potential to play a greater role in that jurisdiction as regards data privacy and security in the future.[34] In Australia, Corones and Davies noted that the general prohibitions in the Australian Consumer Law (*'ACL'*) regulating misleading conduct, unconscionable conduct

---

32 15 U.S.C. §§41-58. See: Daniel Solove and Woodrow Hartzog, 'The FTC and the new common law of privacy' (2014) 114 *Columbia Law Review* 583.

33 Natali Helberger, Marco Loos, Lucie Guibault, Chantal Mak and Lodewijk Pessers, 'Digital Content Contracts for Consumers' (2013) 36(1) Journal of Consumer Policy 37.

34 Angela Daly and Amanda Scardamaglia, 'Profiling the Australian Google Consumer: Implications of Search Engine Practices for Consumer Law and Policy' (2017) 40(3) Journal of Consumer Policy 299.

and false or misleading representations[35] had not, at the time of writing, formed the basis of proceedings against online privacy or data security breaches.[36] However, they consider that the *'ACL'* could 'serve as a useful instrument in the regulation and enforcement of online privacy and data security breaches' in appropriate circumstances,[37] especially given private enforcement actions in the form of litigation are possible under the ACL, in contrast to the '*Privacy Act'*.[38] A very recent update on this topic has occurred in the form of a class action on behalf of NSW Ambulance staff whose medical records were sold to solicitors, against NSW Ambulance for alleged 'breach of confidence, invasion of privacy, breach of contract and misleading and deceptive conduct' on the basis of NSW Ambulance inadequately protecting their records, in a test case which may also establish whether a tort of breach of privacy exists at common law in Australia.[39]

4. Data breach notification laws in the US and EU

Data breach notification laws have widely implemented in the US, where 47 states including Washington DC, Guam, Puerto Rico and the Virgin Islands have introduced such laws.[40] The EU also has data breach notification schemes at the EU level, which have then been implemented in Member States.[41] Jurisdictions in other parts of the world have also adopted data breach notification laws: for instance, Indonesia also has data breach notification requirements for both public and private sector and not-for-profit 'electronic systems operators'

---

35 *Competition and Consumer Act 2010* (Cth), Sch 2.

36 Stephen Corones and Juliet Davis, 'Protecting Consumer Privacy and Data Security: Regulatory Challenges and Potential Future Directions' (2017) 45 *Federal Law Review* 66, 67

37 Ibid, 69.

38 *ACL* ss 232, 236-237. Corones and Davis, above n 36, 91.

39 Harriet Alexander, 'Paramedics launch class action over the sale of their medical records to personal injury solicitors' Sydney Morning Herald 18 November 2017 http://www.smh.com.au/nsw/paramedics-launch-class-action-over-the-sale-of-their-medical-records-to-personal-injury-solicitors-20171118-gzo44u.html

40 National Conference of State Legislatures, *Security Breach Notification Laws* (12 April 2017) <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

41 For the implementation in eg Italy, see Alessandro Mantelero, 'Si Rafforza la Tutela Dei Dati Personali: Data Breach Notification e Limiti Alla Profilazione Mediante Cookies' (2012) 28 *Il Diritto dell'informazione e dell'Informatica* 781.

and to actions 'through electronic media'.[42] As mentioned above, China has also recently adopted a new Cybersecurity Law which includes data breach notification provisions.

In order to provide a point of comparison for the new Australian legislation a brief overview given of existing data breach notification laws in the US and EU will be provided here. They are the two major Western jurisdictions to have adopted data breach legislation, which they have possessed for some time, relatively speaking, with the US in particular being an early adopter of these provisions. Furthermore, they each represent a different Western model of (data) privacy protection identified by Lindsay - the European 'rights-based' approach and the American 'market-based' approach - which Australia can consider for the development of its own laws on this topic.[43]

4.1 US

The US does not have comprehensive data breach notification laws at the federal level. Instead, there are some sector-specific breach requirements in federal legislation, and most states have such laws in their own jurisdictions, whose provisions vary. It is important to note that data breach notification laws in the US have mainly been introduced with an objective of dealing with cybercrime, by giving individuals affected the opportunity to mitigate any harm they may suffer from the breach, and giving organisations incentives to adopt better data security practices lest they suffer from reputation damage. This can also be evidenced by the many instances of data breach litigation in the US, and the debates concerning whether it is necessary to demonstrate harm or injury beyond a 'mere' unauthorised accessing of data.

---

42 Graham Greenleaf and Sinta Dewi Rosadi, 'Indonesia's Data Protection Regulation 2012: A Brief Code with Data Breach Notification' (2013) 122 *Privacy Laws and Business International Report* 24, 24.

43 David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29(1) *Melbourne University Law Review* 131. However, as mentioned above Lynskey notes that European data protection law has a 'hybrid' nature as a rights-based and economics-driven legal regime. See Lynskey, above n 29.

4.1.1 Federal level statutes

While the US does not have comprehensive data privacy laws at the federal level, there are some sector-specific data privacy laws, which have data breach provisions. The most prominent legislation includes:

- the Federal Trade Commission Act (FTC Act),[44] which has been used by the FTC to prohibit unfair or deceptive practices as regards consumer privacy and security policies;[45]
- the Financial Services Modernization Act (Gramm-Leach-Bliley Act) regulating the collection, use and disclosure of financial information;[46]
- the Health Insurance Portability and Accountability Act (HIPAA) regulating medical information,[47] as revised by the HIPAA 'Omnibus Rule' in 2013.

In addition to these requirements for segments of the private sector, there are also obligations incumbent on state and federal government agencies to notify of breaches of data in their possession or databases.[48]

Regarding the enforcement of these provisions, Rabin has observed that there are two main forms for regulatory action at the federal level as regards data breaches: federal agencies' use of enforcement actions or rulemaking 'to influence the data security practices of corporations within the federal agency's mandate'; and the imposition of criminal penalties for data breaches and data misuse.[49]

---

44 15 U.S.C. §§41-58

45 The FTC also enforces other legislation such as the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506) applying to the online collection of information from children.

46 15 U.S.C. §§6801-6827

47 42 U.S.C. §1301 et seq.

48 World Law Group, above n 16, 59. The federal-level data breach notification regimes were due to be supplemented by the 'FCC Privacy Rule' for broadband Internet Service Providers adopted by the Federal Communications Commission at the end of the Obama administration. The FCC Privacy Rule included data security and data breach notification requirements would have come into force during 2017. However, in April 2017, President Donald Trump signed into law a bill passed by the US Congress that repealed the FCC Privacy Rule before it came into force. See: Paul Gaus, 'Only the Good Regulations Die Young: Recognizing the Consumer Benefits of the FCC's Now-Defunct Privacy Regulations' (2017) 18(2) *Minnesota Journal of Law, Science and Technology* 713.

49 Robert Rabin, 'Perspectives on Privacy, Data Security and Tort Law' (2017) 66(2) DePaul Law Review 313, 319.

Some features of the three most prominent federal data breach regimes are outlined below.

4.1.1.1 The FTC Act

The FTC has taken a prominent role in addressing data security breaches in the US, especially as regards organisations which are not covered under one of the sector-specific federal schemes such as HIPAA,[50] and has done so on the basis of section 5 of the FTC Act which prohibits 'unfair or deceptive acts or practices in or affecting commerce'.[51] The FTC has made deceptive practices claims in circumstances when an organisation has a data breach after having published statements that it secured data, with unfair practices claims regarding data security being made less frequently.[52] Since 2002, the FTC has brought more than 60 cases against companies whose practices have placed consumers' data 'at unreasonable risk', and in one case from 2016 the FTC ordered the company in breach (LabMD) to notify customers whose personal information was exposed.[53]

The FTC's activities in this area have been criticised from a due process perspective for not offering sufficient clarity and publicity as to what data security practices it considers to be 'fair', especially when the agency can levy large fines for organisations in violation.[54] However, there are some exceptions, such as the FTC's Health Breach Notification Rule, which sets out notification instructions for companies with websites that collect consumer health data or applications for personal health records (and are not covered by HIPAA) which have experienced a data security breach.[55]

---

50 Gerard Stegmaier and Wendell Bartnick, 'Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements' (2013) 20(3) *George Mason Law Review* 673, 674.

51 15 U.S.C. § 45(a)(1) (2006)

52 Stegmaier and Bartnick, above n 50, 674-675.

53 Federal Trade Commission, *Privacy and Security Update* (2016) <https://www.ftc.gov/reports/privacy-data-security-update-2016#data>.

54 Stegmaier and Bartnick, above n 50.

55 Federal Trade Commission, *Health Breach Notification Rule* (August 2009) <https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule>.

4.1.1.2 HIPAA

Other data breach notification requirements are found in federal sector-specific legislation. Prominent among them is the data breach notification requirement in the HIPAA Breach Notification Rule which requires HIPAA-covered entities to provide a notification following a breach of unsecured protected health information.[56] A breach is defined as an impermissible use or disclosure that compromises the privacy or security of the protected health information.

There is an exception for circumstances where the organisation which has suffered the breach can demonstrate that there is a low probability that the information has been compromised based on a risk assessment of:

- the nature and extent of the health information involved, including the types of identifiers and likelihood of re-identification;
- the unauthorised person who used the information or to whom the information was disclosed;
- whether the information was actually acquired or viewed; and
- whether and to what extent the risk to the information was mitigated.

There are exceptions in cases: where a breach by an employee or contractor was unintentional and made in good faith and within the scope of authority; where a breach was an inadvertent disclosure by one employee or contractor to another (both of whom being authorised to access the information); and where the organisation has a good faith belief that the unauthorised person to whom the impermissible disclosure of information was made would not have been able to retain the information.

Most notifications must be provided within 60 days of the discovery of a breach, with an exception for breaches affecting less than 500 individuals which can be submitted annually to the US federal Department of Health and Human Services. Notifications need only be provided

---

56 45 CFR §§ 164.400-414.

for information which is 'unsecured' i.e. information that has not been rendered unusable, unreadable or indecipherable to unauthorised individuals. Guidance is issued by the Department Secretary as to what technologies and methods can be used to render information secure, which currently includes forms of encryption for electronic data.[57]

4.1.1.3 Financial data breaches

Data breach notification requirements for personal information held by financial organisations are contained in the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, an interpretation of section 501(b) of the Gramm-Leach Bliley Act.[58] This Guidance contains an obligation for an organisation to notify its customers and regulator when there is an incident of unauthorised access to 'sensitive consumer information' (including name, address, telephone number in conjunction with the customer's Social Security number, driver's licence number, account number, credit card number, or account username and password). Customers should be notified when the financial organisation discovers unauthorised access to customer information and has concluded that misuse of the information has occurred or that this is a reasonable possibility. This notification should happen as soon as possible, except in circumstances where an appropriate law enforcement agency determines that notification will interfere with a criminal investigation. Notably there is no exception for the use of measures such as encryption as in other data breach notification laws.

---

57 United States Department of Health & Human Services, *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (26 July 2013) <https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>.

58 United States Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation, *Final Guidance on Response Programs Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice FIL-27-2005* <https://www.fdic.gov/news/news/financial/2005/fil2705.pdf>. See: Sean Honeywill, 'Data Security and Data Breach Notification for Financial Institutions' (2006) 10(1) *North Carolina Banking Institute* 269.

4.1.2 State level statutes

The State of California was the first American state (and the international leader) to implement a data breach notification law.[59] This law entails that anyone who conducts business in California involving computerised personal data must notify Californian residents of an existing or potential breach that includes the unauthorised acquisition of unencrypted digital personal information, without reasonable delay. The notification can be made via communication directly to individuals, through a notice posted on the organisation's website, or via state media sources if the data breach involved more than 500,000 individuals or would exceed US$250,000. There are various exemptions to the notification requirement, including if the breach related to a good faith acquisition of personal information by an employee or agent of the organisation in breach, or if the personal information at issue is encrypted. The law also limits the definition of personal information to an individual's name in combination with other identifying information such as a social security number, drivers licence, bank account details, etc – which can be explained by the fact that the law was introduced as a measure to address identity fraud.[60]

Since this law was introduced in California, almost every other US State (and the District of Columbia, Puerto Rico and Guam) has implemented data breach notification laws of their own, with at least 23 of these laws based on the Californian one.[61] Some of these laws diverge from the Californian model by requiring a threshold of harm (e.g. reasonable likelihood of harm or material harm) to be suffered arising from the breach before a notification is mandated by law.[62] Some states also require an organisation suffering from a breach to conduct an investigation soon after a breach to determine whether there is the need to notify individuals or law enforcement agencies.[63] Other variances with the Californian model include: the need to notify certain law enforcement or consumer credit agencies of the breach; broader definitions of what

---

59 California Civil Code §1798.82.

60 Mark Burdon, Bill Lane and Paul von Nessen, 'The mandatory notification of data breaches: Issues arising for Australian and EU legal developments' (2010) 26 *Computer Law and Security Report* 115, 116.

61 Paul M Schwartz and Edward J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913, 924. At the time of writing, 48 states have enacted data breach notification legislation. See National Conference of State Legislatures, above n 40.

62 See, eg, Alaska, Arkansas, Connecticut, Florida, Iowa, Louisiana, North Carolina and Oregon.

63 See, eg, Arizona, Colorado, Delaware, Idaho, Kansas, Maine, Maryland, Nebraska, New Hampshire and Utah.

constitutes personal information; the inclusion of personal information held in non-electronic formats; and the imposition of fines or civil penalties for non-compliance.[64]

4.1.3 Data breach litigation

In addition to enforcement action regarding data breaches taken by the FTC and other regulatory bodies, the US has also experienced a comparatively significant amount of litigation concerning data breaches, including class actions, notwithstanding challenges plaintiffs have faced in proving standing and injury in accordance with Article III of the US Constitution.[65]

Based on a review of case-law, Cease notes that such class actions 'are often state law claims for negligence and breach of implied contract',[66] and often involve three types or categories of alleged injury: when a third party has stolen an individual's personal or financial information and the third party has used that information to make purchases using the individual's money (a class of cases which tend to satisfy standing issues concerning the need for plaintiffs to suffer an injury in fact); when individuals' information has been accessed and used in other ways producing harm such as incurring costs for credit-monitoring services, paying to cancel and receive new bank cards and suffering stress and anxiety (it is less clear whether plaintiffs in these cases have met the standing requirement); and when a plaintiff brings a case on the belief that their information is not being sufficiently protected and it could potentially be accessed by a third party in the future (this category is the least likely to meet the standing requirement).[67]

Some further empirical analysis has been conducted by Romanosky, Hoffman, and Acquisti regarding data breach notification litigation in the US between 2005 and 2010. The main notable findings were: that data breaches were more likely to be litigated when individuals had suffered financial loss; that they were also more likely to be litigated when the breach was

64 Burdon, Lane, and von Nessen, above n 60, 117.

65 The seminal case on standing in the US is *Lujan v Defenders of Wildlife* (504 U.S. 555 (1992)) in which the Supreme Court recognised standing for injuries that were either actual or imminent.

66 Caroline Cease, 'Giving out Your Number: A Look at the Current State of Data Breach Litigation' (2014) 66 Alabama Law Review 395, 397.

67 Ibid at 397-404.

unauthorised disclosure or disposal of consumer information rather than breaches caused by lost or stolen data or cyberattacks; and when the information concerned was financial information.[68] They also found that breaches involving medical data, and those caused by cyberattacks were more likely to result in the case being settled.[69] However, overall only 4% of breaches resulted in federal litigation, and the authors warned that litigation could only be effective 'to the extent that a plaintiff can identify the cause of a breach and subsequent harm', with scenarios involving data brokers being more conceptually problematic because of the lack of direct relationship between these actors and the individuals whose data they handle.[70] The constituent requirements of standing, including injury, proximity and causation, can be seen here to mount obstacles for plaintiffs in US data breach litigation.

On the issue of standing in data breach litigation, the Seventh Circuit court issued its opinion in *Remijas v Neiman Marcus*,[71] a 2015 case 'widely recognized as having opened the door to standing in the subset of information privacy cases that involve data breaches'.[72] The Seventh Circuit court recognised standing in certain situations where there was a risk with an 'objectively reasonably likelihood' to occur.[73] Given the circumstances at hand, 'plaintiffs in data breach litigation have standing when hackers or thieves access financial of potentially injurious information, and some members of this exposed group suffer fraudulent charges'.[74] However, in proceedings subsequent to the *Remijas* decision, many courts have distinguished the decision on legal and factual bases, especially where there is no injury among any members of the class, with only a few courts following it, where the circumstances were very similar to those in *Remijas*.[75] There has been a subsequent Supreme Court ruling in the 2016 *Spokeo v Robins* judgement concerning standing issues,[76] although from the perspective of data breach litigation, Rotenberg and Thomson have argued that the decision does not provide much clarity

---

68 Sasha Romanosky, David Hoffman and Alessandro Acquisti, 'Empirical Analysis of Data Breach Litigation' (2014) 11(1) *Journal of Empirical Legal Studies* 74, 76–7.

69 Ibid 98.

70 Ibid 101–102.

71 *Remijas v. Neiman Marcus Grp*., 794 F.3d 688 (7th Cir. 2015).

72 Julie Cohen, 'Information Privacy Litigation as Bellwether for Institutional Change' (2017) 66(2) DePaul Law Review 535, 547.

73 *Remijas*, above n71, 693.

74 Jordan Dillon, 'Standing on the Wrong Foot: The Seventh Circuit's Eccentric Attempt to Rescue Risk-Based Standing in Data Breach Litigation [*Remijas v. Neiman Marcus Grp.*, 794 F.3d 688 (7th Cir. 2015)' (2017) *Washburn Law Journal* 123, at 140

75 Ibid at 145-148

76 *Spokeo, Inc v Robins*, 136 Supreme Court 1540 (2016).

to the standing issue.[77] Thus standing is likely to pose an ongoing obstacles to some claims in the context of data breach litigation.

A more general critique of this kind of litigation has been advanced by Cohen, who has criticised the jurisprudential isolation of data breaches from cases of more general data profiling, despite profiling's negative effects for personal data protection and security: by emphasising the purported exceptional nature of data breaches, she has argued that 'courts … ignore the extent to which background norms and design practices favoring virtually unconstrained data collection, processing and exchange harm the subjects of those practices', harm which may not be imminent or immediate, and has not properly been addressed by American courts to date.[78]

4.1.4 Summary of US situation

As can be seen from the above, the overall situation in the US is a patchwork of unharmonised data breach notification legislation: unharmonised both across different states and federal jurisdictions, and also unharmonised across different industry sectors at the federal level. This leads to a situation where a company which has experienced a breach must look to the different state-level laws of where the individuals whose data has been breached reside in order to determine whether and how the individual should be notified of the breach, and may also have to look to the federal sector-specific laws too – all of which impose differing standards. Peters has argued that this situation of legislative disharmony 'compounds the problems and costs associated with these breaches'.[79]

To improve this situation, some commentators have called for a general data breach notification requirements at the federal level in order to remedy the lack of consistencies and ensure

---

77 Marc Rotenberg and Aimee Thomson, 'US Supreme Court Fails to Clarify 'Standing' Doctrine in Consumer Privacy Case' (2016) 3 *European Data Protection Law Review* 428.

78 Cohen, above n 72, 548.

79 Rachael Peters, 'So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Laws' (2014) 56 (4) *Arizona Law Review* 1171, 1174.

residents of any state will be notified about data breaches involving their personal information.[80] Bills have been put before Congress, but at the time of writing none has passed into law.

While data breach litigation, especially class actions, has been used as a tool by individuals affected by data breaches to address the negative consequences of such events, the aftermath of the Seventh Circuit court decision in *Remijas* may still pose obstacles for plaintiffs who cannot show harms such as identity fraud themselves or among some members of their class. A data breach which compromises their privacy and information security per se probably cannot occasion a successful claim alone.

Overall, given this picture, Rabin has argued that the current US approach to data breaches has three outstanding main problems: '(1) uncompensated victims; (2) inadequate incentives for companies and governments to invest in data security; and (3) uncertainty for corporations with respect to their regulatory burdens and litigation risk'.[81] He asserts that the failures of the existing US data breach regime to prevent data breaches occurring in practice can be attributed to the absence of a comprehensive federal regime on the topic, the lack of clear rules and standards issued through administrative agencies' individual enforcement actions, and the limited mandates these administrative agencies actually have to address data breaches.[82]

4.2 European Union

80 See: Jonathan Darrow and Stephen D Lichtenstein, 'Do You Really Need My Social Security Number? Data Collection Practices in the Digital Age' (2008) 10(1) *North Carolina Journal of Law and Technology* 1, 53; Samuel Lee, 'Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs' (2006) 1(1) *Entrepreneurial Business Law Journal* 125, 136.

81 Rabin, above n49.

82 Ibid, 323-324.

In contrast to the US, the EU has comprehensive data protection laws, firstly in the form of the 1995 Data Protection Directive ('DRD'),[83] which is currently being superseded by the General Data Protection Regulation ('GDPR').[84] This differs from the US approach to data privacy, which has generally been sector-based as mentioned above, and provides an overall weaker level of substantive protection than in the EU.[85] In this sense, Australia resembles the EU more closely, with the '*Privacy Act'* as its own comprehensive federal-level data privacy regime.

However, data breach notification requirements are not just found in the EU's main data privacy legislation: instead there are various requirements contained in different EU laws. Indeed, the initial notification obligation can be found in the ePrivacy Directive, which despite its name is not the EU's main data protection law (which is the aforementioned DRD, to be superseded by the GDPR). This obligation has been supplemented by others in the GDPR and also in the EU's first cybersecurity Directive. In July 2014, the EU also adopted its Regulation on electronic identification and trust services (eIDAS Regulation) which introduced breach notification for 'trust service providers', a category which could encompass telecoms providers and financial institutions.[86]

Similarly to the aforementioned criticisms of the US situation, Esayas has argued that this 'array of breach notification requirements within the EU means that an organization might be required to notify for different aspects of the same breach under different notification requirement, creating significant administrative and financial burden for multinational companies'.[87] However, with the transition of legal instrument from Directives to Regulations containing most of the EU's data breach notification obligations, there should be a higher

---

83 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)* [1995] OJ L 281.

84 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*GDPR*').

85 See: *Maximillian Schrems v Data Protection Commissioner* (C-362/14) [2015] ECR 650, where the CJEU invalidated the US-EU Safe Harbor agreement for the transfer of personal data.

86 *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC* [2014] OJ L 257/73, art 19(2).

87 Samson Esayas, 'Breach Notification Requirements under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance' (2014) 31(3) *John Marshall Journal of Information Technology and Privacy Law* 317, 321.

degree of harmonised implementation of these obligations in Member States,[88] and so a less fragmented approach to notification obligations should be achieved in the Single Market, at least compared to the US. Yet the EU's new cybersecurity legislation is in the form of a Directive, not a Regulation, and there are still differing standards in the different sectoral laws, as will be seen below.

4.2.1. ePrivacy Directive

Until the GDPR, the ePrivacy Directive has, since its 2009 revision, included the main data breach notification obligation in the EU, directed at the 'electronic communications sector' rather than more generally at all organisations.[89] Organisations falling within the scope of these obligations are telecommunications companies and Internet Service Providers (ISPs), a narrow focus that has been contentious.[90]

A 'personal data breach' is defined in Article 2 of the Directive, as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications services in the Community'. The data breach notification obligations itself is contained in Art 4(2), and provides that providers of publicly available electronic communications services must inform subscribers of a particular risk of a breach to the network's security. When the risk lies outside 'the scope of the measures to be taken by the service provider', the provider must inform subscribers of 'any possible remedies,

---

88 The text of EU Regulations has binding legal force in every Member State and enters into force on the same day in all Member States, while Directives lay out certain goals which must be achieved but leave each Member State free to decide how to devise domestic legislation to transpose these goals into national law.

89 *ePrivacy Directive* amended by *Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* [2006] OJ L 105/54; *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws* [2009] OJ L 337/11.

90 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 Review* 296, 298.

including an indication of the likely costs involved'. Providers are also under an obligation in Art 4(3) to notify the competent national authority of any personal data breach. They must also inform any individual (who does not necessarily have to be a 'subscriber') if their privacy or personal data is likely to be adversely affected by the personal data breach, without undue delay.

There are exemptions from this notification requirement if the provider demonstrates to the satisfaction of the competent authority that it implemented appropriate technological protection measures (such as encryption) and applied these to the data affected by the security breach that would 'render the data unintelligible to any person who is not authorised to access it'. In 2014, the Article 29 Working Party provided non-binding guidance to data controllers to assist them in determining whether to notify individuals affected of a personal data breach, with illustrative (but non-exhaustive) examples of situations in which notifications to individuals would be appropriate.[91]

Subsequent to the ePrivacy Directive's 2009 reform, the EU adopted Regulation 611/2013 with the objective of harmonising the ePrivacy Directive's data breach notification requirements among Member States. The Regulation concerns the notification of personal data breaches by providers of publicly available electronic communications services. There is an obligation to notify the competent national authority within 24 hours of any (regardless of severity) personal data breach being detected.[92] Individuals whose personal data or privacy is likely to be adversely affected in a personal data breach should also be notified,[93] although this is not required if the provider implemented appropriate technological protection measures to the data concerned which render the data unintelligible to unauthorised persons accessing it, as described above.[94]

---

91 Article 29 Data Protection Working Party, 'Opinion 03/2014 on Personal Data Breach Notification, 693/14/EN' (Opinion No 693/14/EN WP 213, 25 March 2014).

92 *Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications* [2013] OJ L 173/2, art 2(2) ('*Regulation on notification of data breaches*').

93 *Regulation on notification of data breaches*, art 3.

94 *Regulation on notification of data breaches*, art 4.

The ePrivacy regime is currently under review in the EU, with a proposal for a new ePrivacy Regulation being discussed at the time of writing.[95] There is no explicit data breach notification requirement in the proposals, perhaps due to the implementation of data breach notification requirements in the GDPR and NIS Directive, detailed below. However, Article 17 of the proposed ePrivacy Regulation includes an obligation for electronic communications service providers to inform end-users of any risks that may compromise the network and service security, as well as inform them of any possible remedies that they should implement if the risk 'lies outside the scope of the measures to be taken by the service provider'.[96]

4.2.2 GDPR

In 2016, the EU adopted its update to data protection laws, the GDPR, whose provisions are scheduled to come into force in May 2018. The GDPR strengthens existing EU data protection standards, and introduces certain new elements, including an increased extra-territorial scope,[97] a right to data portability,[98] and the principle of data protection by design and by default.[99]

The GDPR also includes data breach notification obligations. The GDPR's data breach notification obligations cover a broader range of situations than those covered by the ePrivacy Directive, given that they are incumbent on data controllers in any sector, while the ePrivacy Directive is confined to the telecommunications sector. Also, the level of fines under the GDPR for non-compliance with its provisions are high: up to 2% of global turnover.[100]

The GDPR defines a 'personal data breach' in almost identical language to the revised ePrivacy Directive, with the exception that the relevant breach is defined more generically, rather than just those related to the electronic communications sector. It also contains two sets of obligations. One is for data controllers to notify a personal data breach to the competent supervisory authority within 72 hours, unless the breach is 'unlikely to result in a risk to the

---

95 *Proposal for a Regulation of the European Parliament and Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)* COM (2017) 10 final ('*ePrivacy Regulation*).

96 *ePrivacy Regulation*, art 17.

97 *GDPR* art 3.

98 *GDPR* art 20.

99 *GDPR* art 25.

100 *GDPR* art 83(4).

rights and freedoms of natural persons'.[101] The other data breach notification obligation concerns the communication of a personal data breach by the data controller to the data subject, which must happen 'without undue delay' when the breach 'is likely to result in a high risk to the rights and freedoms of natural persons'.[102] However, data controllers are exempt from this obligation in certain circumstances: when the controller has implemented and applied technical and organisational measures to the affected personal data in ways which render it unintelligible to unauthorised persons (such as encryption); the controller has taken mitigation measures which ensure that the high risk to data subjects' rights and freedoms is no longer likely to materialise; and when it would involve 'disproportionate effort', in which case a public communication or similar measure would suffice.[103]

4.2.3 NIS Directive

In addition to the GDPR, breach notification obligations are also included in the new Directive on security of network and information systems (NIS Directive), the first EU-level legislation on cybersecurity, which entered into force in August 2016. Concerns have been raised about the risk of unnecessary costs due to a lack of harmonisation across Member States in implementing the NIS Directive incident reporting, and the overlapping scope of the data breach notification requirements between the NIS Directive and the GDPR.[104]

The NIS Directive places on operators of 'essential services'[105] and 'digital service providers''[106] notification requirements. Operators of essential services must notify, without

---

101 *GDPR* art 33(1).

102 *GDPR* art 34(1).

103 *GDPR* art 34(3).

104 Esayas, above n 87, 355-356.

105 It is up to Member States to define entities which meet the criteria of 'essential services' in their territory, but a list of 'essential services' is provided in Annex II to the NIS Directive and includes providers of energy, transport, banking, financial market infrastructure, health, water and digital infrastructure providers. See *Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* [2016] OJ L 194/1, recital 19, arts 4(4), 5(2) ('*NIS Directive*').

106 See *NIS Directive.* Article 4(5) and (6) define 'digital service providers' as a provider of a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, which is of a type listed in Annex III of the NIS Directive. These types in Annex III comprise three categories: online marketplace, online search engine and cloud computing service. Esayas has pointed about the problems in including cloud providers which may be unaware of the service or data being used over its infrastructure. See Esayas, above n 87, 364–365.

undue delay, the competent authority or computer security incident response teams (CSIRTs)[107] of incidents having a significant impact on the continuity of the essential services they provide.[108] Various factors are given in order to determine the significance of an incident's impact: the number of users affected, the incident's duration; and the geographical area affected by the incident.[109] The competent authority or CSIRT may inform the general public about security incidents in circumstances 'where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident'.[110]

In order to implement and enforce these obligations, Member States' competent authorities should have the powers to require essential services operators to provide the necessary information to assess their network and information systems' security, and evidence of the effective implementation of security policies.[111] The competent authority also has an obligation to work closely with data protection authorities when addressing incidents resulting in personal data breaches.[112]

There is also a separate incident notification obligation for digital service providers, which is very similar in substance to the obligation on essential service providers.[113] In addition, there is an obligation to notify if an essential service relies on a third-party digital service provider, and if there is a 'significant impact on the continuity of the essential services due to an incident affecting the digital service provider'.[114] Furthermore, there is provision for the general public to be notified, but in slightly different circumstances to the essential service providers' obligation above: where public awareness is necessary in order to prevent an incident, deal with an ongoing incident or where disclosure is otherwise in the public interest.[115]

In addition to these mandatory requirements on essential services providers and digital service providers, other operators may notify on a voluntary basis of any incident having a significant

---

107 The establishment of CSIRTs is a requirement of the Directive for Member States, in order to ensure that they have effective technical and organisational capabilities to deal with incidents and risks, and ensure cooperation at the EU level. See *NIS Directive*, recital 34, art 9.

108 *NIS Directive*, art 14(3).

109 *NIS Directive*, art 14(4).

110 *NIS Directive*, art 14(6).

111 *NIS Directive*, art 15(1)–(2).

112 *NIS Directive*, art 15(4).

113 *NIS Directive*, art 16(3).

114 *NIS Directive*, art 16(5).

115 *NIS Directive*, art 16(7).

impact on the continuity of their services, and this voluntary notification will not result in any new obligations being placed on the operator.[116]

4.2.4 Summary of EU situation

The above discussion shows some parallels between the US and EU data breach notification requirement frameworks, such as fragmentation through a lack of harmonisation of different data breach notification requirements in different legislation aimed at different sectors. The GDPR's data breach notification obligations incumbent on data controllers in any sector should result in some level of harmonisation across different industry sectors, although the endurance of pre-existing obligations in the ePrivacy Directive (for the time being), and the introduction of new ones in the NIS Directive, will still have the effect of exposing operators in certain industries to additional breach notification requirements.

The use of Regulations as a legal instrument to introduce new data breach notification obligations in the eIDAS Regulation and then the GDPR may mitigate a lack of harmonised approach to the implementation of EU laws in this area at the Member State level, however this lack of harmonisation may still ensue from the NIS Directive's implementation.

It may be merely rhetorical, but the wording of the GDPR's data breach notification obligations does point to the (partial) 'rights-based' nature of European data privacy law, with mention made of 'the rights and freedoms of natural persons' in the context of data breaches. While this may be laudable, there is little empirical evidence as regards the extent to which the EU's data breach notification requirements actually are effective in upholding the fundamental rights, or, for that matter, economic interests, of European citizens. Such empirical evidence on this point should be a topic of further research in order to assess the efficacy of notification requirement in the EU and to guide future legislative and policy reform in this area.

---

116 *NIS Directive*, art 20.

A further point of divergence between the EU and US has been on the issue of data breach litigation. Litigation, especially in the form of class actions, has played a much more marginal role in addressing data breaches in the EU than the US. Indeed, in some jurisdictions such as the UK, it is only at the time of writing that the first class action proceedings regarding a data breach have been initiated as a test case.[117] It remains to be seen whether there will be any growth in litigation in the coming years, particularly with the implementation of the GDPR obligations concerning data breaches and data breach notification.

5. Existing Australian situation

Before turning to examine the new data breach notification legislation in Australia, the legal scenario preceding the introduction of these measures is outlined here. The aforementioned '*Privacy Act'* is the main piece of legislation governing data privacy and security in Australia, and there are also specific state and territory-level laws governing aspects of this topic. A brief description of these laws is given.

5.1 Commonwealth legislation

The '*Privacy Act'* regulates the handling of personal information about individuals (natural persons) that includes the collection, use, storage and disclosure of this information, as well as access to and correction of personal information. Organisations bound by the '*Privacy Act'* are Commonwealth agencies (with exemptions), private companies with an annual turnover of more than $3 million and private health service providers (regardless of size).[118]

---

117 See: Jane Croft, 'UK companies keep close eye of Morrisons data leak case' Financial Times, 8 October 2017 https://www.ft.com/content/42423624-a466-11e7-9e4f-7f5e6a7c98a2. In December 2017, the High Court found that the defendant was vicariously liable for the acts of a rogue employee who posted payroll data relating to other employees on the dark web. See: Kate Macmillan, 'High Court confirms data breach litigation risk' PWC 1 December 2017 <http://pwc.blogs.com/data_protection/2017/12/high-court-confirms-data-breach-litigation-risk-1.html>

118 *Privacy Act*, s 6.

The '*Privacy Act'* contains the Australian Privacy Principles (APPs), which comprise obligations as regards personal information that bind Commonwealth agencies and large private companies. The most relevant APP to the topic of unauthorised access to and disclosure of information that may otherwise constitute a data breach is APP 6 on the use or disclosure of personal information, which states that if an APP entity holds personal information about an individual, it must not be used or disclosed for a purpose other than for the primary purpose for which it was collected, unless the individual has consented, or unless the individual would reasonably expect the APP entity to use or disclose the information for that secondary purpose.[119] In addition to these requirements, the '*Privacy Act'* also contains provisions relating to the proper use or disclosure of credit reporting information,[120] including the use and disclosure of information by mortgage insurers, credit managers, advisers and related bodies corporate.[121]

As regards information security, APP 11 is of utmost importance: it provides that organisations must take 'such steps that are reasonable in the circumstances' to protect personal information it holds from 'misuse, interference and loss' and from 'unauthorised access, modification or disclosure'. Broadly speaking, APP 11 provides that organisations bound by the APPs must take reasonable steps to prevent data breaches, whether inadvertent, deliberate or from external malicious sources. APP 11 also provides that organisations should destroy personal information they hold which is no longer necessary to keep or ensure this information is de-identified. However, until the new mandatory data breach notification legislation, there was no obligation incumbent on organisations bound by the APPs to inform individuals if their information was misused, lost or subject to unauthorised access.

If an APP has been breached in the form of an interference with an individual's privacy, then the individual must first make complaints to the organisation allegedly in breach of the APPs, and if the organisation does not address the complaint satisfactorily, the individual can escalate

---

119 *Privacy Act* s 14, sch 1. See Australian Privacy Principle 6.1–6.2(a) (*'APP'*) – use or disclosure of personal information. There are a number of exceptions to this, contained in APP 6.2 – if required by law, if a permitted general situation exists (including to lessen or prevent a serious threat to the life, health or safety of an individual or the public), if a permitted health situation exists (including collection of information to provide a health service or conduct research, or disclosure of genetic information), or if use or disclosure is reasonably necessary for enforcement related activities conducted by or on behalf of an enforcement body.

120 *Privacy Act* pt IIIA div 2.

121 *Privacy Act* pt IIIA div 4 sub-div B.

the complaint to the federal Privacy Commissioner.[122] The federal Privacy Commissioner can then investigate the complaint depending on its merits and is also empowered to instigate own-initiative investigations without there being a complaint.[123] Organisations found to have engaged in conduct constituting an interference with an individual's privacy can be subject to fines and other measures.[124]

There are a number of recent determinations by the federal Privacy Commissioner regarding entities' inadequate data security practices in breach of the APPs (and their predecessors: the Information Privacy Principles which applied to federal agencies, and the National Privacy Principles which applied to private companies).[125] One such determination occurred following a data breach by private company TeleChoice, where an individual whose personal information was compromised was awarded AUS$3,500 for non-economic loss in the form of the individual and her family suffering stress and anxiety caused by the interference with her privacy, with the implication that the complainant would have received a greater sum had she suffered more serious kinds of harm.[126] The federal Privacy Commissioner has also undertaken a number of Commissioner-initiated investigations in recent years concerning prominent data breaches.[127] Despite the investigations often concluding that there had been infringements of the *Privacy Act*, usually the Commissioner has not levied a fine on the parties at fault - as can be seen in the aforementioned instances involving the Department of Immigration and Border

---

122 *Privacy Act*, s 36. Representative complaints are also possible under *Privacy Act*, s 38.

123 *Privacy Act*, s 40.

124 See Office of the Australian Information Commissioner, 'Guide to Privacy Regulatory Action' (Regulatory Guide, Australian Government, June 2015) 51 <https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/guide-to-oaic-s-privacy-regulatory-action/oaic-regulatory-action-guide.pdf>. A data breach involving the Department of Defence resulted in a $5000 fine from the Privacy Commissioner. See: Paris Cowan, 'Defence Fined $5000 for Privacy Breach', *IT News* (online), 8 September 2014 <https://www.itnews.com.au/news/defence-fined-5000-for-privacy-breach-391792>.

125 See: Australian Government Office of the Australian Information Commissioner, *Privacy Law Determinations* <https://www.oaic.gov.au/privacy-law/determinations/>

126 'IY' and Business Service Brokers Pty Ltd t/a TeleChoice [2016] AICmr 44 (30 June 2016)

127 Office of the Australian Information Commissioner, 'Commissioner initiated investigation reports' <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/>

Protection,[128] the joint investigation of the Ashley Madison breach,[129] and the Australian Red Cross Blood Service breach.[130]

Yet over the last few years there have been serious concerns about the Office of the Australian Information Commissioner (OAIC), which includes the federal Privacy Commissioner, receiving insufficient funding and resourcing from the government to carry out its functions effectively.[131] Since individuals cannot bring a case to the courts themselves, they must rely on an organisation which may be unable, due to resource constraints, to pursue their complaint. While Australian consumer protection law may have a greater role to play in the legal sphere of data privacy and security, and may bring with it the possibility of private actions and the regulatory power of the Australian Competition and Consumer Commission (ACCC) as mentioned above, no public or private enforcement activity from the perspective of consumer protection law on this topic is known to have yet occurred in Australia, with the exception of the NSW Ambulance staff class action currently pending.[132]

5.2 State and territory information privacy laws

In addition to Commonwealth legislation, most, but not all, states and territories in Australia have information privacy laws regulating state-level public authorities' use of personal information, which contain offences for the unauthorised use and/or disclosure of personal information.[133] While some states and territories do not have data privacy legislation that applies to personal information generally, all have data protection laws specific to the proper

---

128 Office of the Australian Information Commissioner, 'Department of Immigration and Border Protection: Own motion investigation report' (CII report, November 2014) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/dibp-omi>

129 Office of the Australian Information Commissioner, 'Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner' (CII report) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison>

130 Office of the Australian Information Commissioner, 'DonateBlood.com.au data breach (Australian Red Cross Blood Service)' (CII report, 7 August 2017) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/donateblood-com-au-data-breach-australian-red-cross-blood-service>

131 See Allie Coyne, 'Starved of Funding, Resources, OAIC is left to shrivel', *IT News* (online), 17 July 2015 <http://www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273>; Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *UNSW Law Journal* 121, 138-139.

132 Corones and Davis, above n 36.

133 See, eg, *Privacy and Personal Information Protection Act* 1998 (NSW) ss 62–63; *Information Privacy Act 2009* (Qld) s 185; *Information Act* (NT) ss 146(5), 148(3).

management of the personal health information of individuals which contain similar offences for the unauthorised disclosure and/or use of personal information.[134]

5.3 Pre-existing data breach notification requirements

In the field of health, prior to the introduction of data breach notification legislation, there is one example of a statutory sector-specific data breach notification requirement. The *My Health Records Act 2012* (Cth) governs the Australian government's digital health records system. Under the *My Health Records Act 2012* (Cth) s 75, an entity that is a registered healthcare provider organisation, a registered repository operator, a registered portal operator, or a registered contract service provider, is required to notify the state or territory System Operator or the Information Commissioner if they become aware of unauthorised collection, use or disclosure of health information,[135] or if an event or set of circumstances has occurred (or may occur) that compromises (or may compromise) the security or integrity of the My Health Records system.[136] Failure to comply with this notification requirement is a civil penalty provision.[137]

Additionally, as soon as practicable after becoming aware that a situation may occur, the entity is obliged to take steps to contain the potential breach, evaluate the risks, and if there is a reasonable likelihood that the breach and its effects might be serious for at least one healthcare recipient, to ask the System Operator to notify all healthcare recipients affected (or if they are a System Operator, to carry out that notification).[138] If an entity becomes aware that a breach has already occurred, they are also obliged to take reasonable steps to contain the breach, evaluate the risks, and if they are a System Operator, to notify all healthcare recipients, or to ask the System Operator to do so.[139] If a significant number of healthcare recipients are affected, the general public must also be notified.[140] Failure to comply with these sections will

---

134 *Health Records (Privacy And Access) Act* 1997 (ACT) ss21–2; *Health Records and Information Privacy Act* 2002 (NSW) ss 68–69; *Public and Environmental Health Act* (NT) s 112(1); *Public Health Act* 2005 (Qld) ss 274–275, 291; *South Australian Public Health Act* 2011 (SA) s 100; *Health Records Act* 2011 (Vic) ss 81–82; *Health Services Act 2016* (WA) s 219.

135 *My Health Records Act 2012* (Cth) ss 75(1)(b)(i), 75(2) ('*My Health Records Act*').

136 *My Health Records Act* ss 75(1)(b)(ii)–(iii), 75(2).

137 *My Health Records Act* s 75(2).

138 *My Health Records Act* s 75(5).

139 *My Health Records Act* s 75(6).

140 *My Health Records Act* s 75(6)(c)–(d).

not accrue civil penalties, however the legislation notes that failure to comply may have other consequences, for example, cancellation of registration.[141]

Australian government agencies also have an obligation to report cyber security incidents to the Australian Signals Directorate, which include various data breach scenarios: any compromise or corruption of information; unauthorised access or intrusion into an ICT system; data spills; theft or loss of electronic devices that have processed or stored Australian government information).[142]

6. *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)

Until recently Australia had no generic legislation governing the notification of data breaches. However, that situation has been remedied by the passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) which amends the '*Privacy Act'* by establishing a scheme for notification of data breaches. The scheme will commence 12 months after Royal Assent, namely 22 February 2018, giving affected entities one year to prepare.

6.1 Background to new legislation

The possibility of data breach notification requirements in Australian law is not a novel idea. Cautious support in Australia for such measures has been expressed in the past from commentators,[143] with more mixed views from stakeholder groups.[144] The implementation of

---

141 *My Health Records Act* s 75(5)–(6).

142 Australian Government Department of Defence, *Report a Cyber Incident*, Australian Signals Directorate <https://www.asd.gov.au/infosec/reportincident.htm>. See also Australian Government Department of Defence, *ISM - Information Security Manual*, Australian Signals Directorate <https://www.asd.gov.au/infosec/ism/>.

143 See, eg, Sara Smyth, 'Does Australia Really Need Mandatory Data Breach Notification Laws – And If So, What Kind?' (2013) 22(2) *Journal of Law, Information and Science* 159, 178-9.

144 See, eg, Bill Lane, Mark Burdon, Evonne Miller and Paul von Nessen, 'Stakeholder perspectives regarding the mandatory notification of Australian data breaches' (2010) 15 *Media and Arts Law* Review 149.

notification requirements is happening ten years after their first prominent appearance in Australian legal debate.

Indeed, the first major recommendations for the introduction of data breach notification requirements can be found in the Australian Law Reform Commission's (ALRC) 2008 report *For Your Information: Australian Privacy Law and Practice*, a recommendation which received 'strong support' from stakeholders.[145] The ALRC proposed a notification requirement to the federal Privacy Commissioner and affected individuals in circumstances in which 'specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person, and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual'. The agency or organisation would have been able to investigate the data breach and make an assessment as to whether it would give rise to serious harm to an individual, which would not have been confined to identify theft or fraud but also could have included discrimination.[146]

This scheme would have entrusted the agency or organisation with the task of deciding whether the triggering event had occurred, while providing oversight by the federal Privacy Commissioner, with a preference for consultation between the Privacy Commissioner and the agency or organisation in the decision-to-notify process, comprising a co-regulatory model.[147] The ALRC also recommended various exceptions to notification in circumstances: where adequate encryption had been used; where good-faith acquisition had occurred by an employee or agent acting within the *Privacy Act* if the information was not subjected to further unauthorised disclosure; and would also have given the Privacy Commissioner a broad discretion to waive the notification requirement where it was not in the public interest to notify.[148] The ALRC recommended a minimum content requirement for breach notices which would include: a description of the breach; a list of the types of personal information disclosed; and contact information for affected individuals to obtain more information and assistance.[149]

---

145 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), at 51.50. See also Kayleen Manwaring, 'Data Breach Notifications: An Australian Perspective' (2009) *Privacy and Data Security Law Journal* 848.

146 Australian Law Reform Commission, ibid, 51.84

147 Ibid, 51.86-88. On co-regulation, see: Ann Wardrop, 'Co-regulation, responsive regulation and the reform of Australia's retail electronic payment systems' (2014) 30(1) *Law in Context* 197.

148 Australian Law Reform Commission, ibid, 51.91-51.94.

149 Ibid, 51.100.

Finally, the ALRC recommended that a failure to notify the Privacy Commissioner of such a qualifying data breach be subjected to a civil penalty, in appropriate circumstances, such as where 'there was an apparent blatant disregard of the law; the agency or organisation has a history of previous contraventions of the law; or there was a significant public detriment arising from the breach'.[150]

However, the ALRC's Recommendations were not adopted. An attempt to introduce data breach notification legislation by a previous Labor government in 2013 failed.[151] Despite the measures having bipartisan support, the legislation was not passed before the 2013 federal election and so lapsed.[152]

Prior to the new data breach notification legislation, the OAIC issued non-binding guidance for organisations on how to handle personal data breaches, which included recommendations to inform individuals affected and the OAIC where there was a risk of serious harm.[153] Before the introduction of the legislative obligations, the OAIC has operated a voluntary breach notification scheme whereby organisations having suffered a breach could notify the OAIC of that fact.

The current legislation was introduced subsequent to the passage of controversial data retention laws in 2015,[154] as a part of a political compromise between the Government and the Opposition,[155] on the basis of a recommendation from the Parliamentary Joint Committee on Intelligence and Security.[156] The Attorney-General's Department released an exposure draft of

---

150 Ibid, 51.107-51.109

151 Privacy Amendment (Privacy Alerts) Bill 2013 (Cth). See: Alice Coyne, 'Labor Resurrects Data Breach Notification Bill', *IT News* (online), 21 March 2014 <https://www.itnews.com.au/news/labor-resurrects-data-breach-notification-bill-375804>.

152 Nick Abrahams and Jamie Griffin, 'The End of a Long Road: Mandatory Data Breach Notification Legislation Becomes Law' (2017) 32 *LSJ – Law Society of NSW* Journal 76.

153 Office of the Australian Information Commissioner, 'Data Breach Notification Guide — A Guide to Handling Personal Information Security Breaches' (Regulatory Guide, Australian Government, August 2014) <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>.

154 *Telecommunications (Interception and Access Amendment (Data Retention) Act 2015 (Cth)*.

155 Commonwealth, *Parliamentary Debates*, House of Representatives, 19 October 2016, 2430 (Michael Keenan).

156 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access Amendment (Data Retention) Bill 2014* (2015).

the Bill for comment in December 2015,[157] a modified version of the Bill was introduced into the Senate in October 2016,[158] and passed in February 2017.[159]

6.2 Content of legislation

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) amends the *Privacy Act*, and the new breach notification scheme commences on 22 February 2018, as mentioned above.

The legislation introduces a new notification obligation that the federal Privacy Commissioner and any affected individuals be notified when an 'eligible data breach' has occurred. An entity must give a notification either if it has reasonable grounds to believe an eligible data breach has occurred or if it has been directed to give a notification by the Commissioner.[160] If an entity believes there are reasonable grounds to suspect that it may have suffered an eligible data breach, it must carry out a 'reasonable and expeditious assessment' within 30 days of when it first became aware of whether the circumstances actually amount to an eligible data breach.[161]

An 'eligible data breach' will happen if there is unauthorised access to, or unauthorised disclosure of information, and a reasonable person would conclude that the access or disclosure would be likely to result in 'serious harm' to any of the individuals to whom the information relates.[162] An eligible data breach will also occur when information is lost in circumstances where unauthorised access to, or unauthorised disclosure of information is likely to occur, and assuming that the access or disclosure were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in 'serious harm' to any of the individuals to whom the information relates.[163] Whether a disclosure might be likely to result in 'serious harm' is to be determined by reference to: the kind of information affected; the sensitivity of information; whether the information is protected by security measures (and whether they could be overcome); the kinds of persons who might have obtained the information; the

157 Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth).
158 Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth)
159 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).
160 *Notifiable Data Breaches Act* s 26WA.
161 *Notifiable Data Breaches Act* s 26WH.
162 *Notifiable Data Breaches Act* s 26WE(2)(a).
163 *Notifiable Data Breaches Act* s 26WE(2)(b).

possibility that those persons could circumvent a security technology or methodology used to protect the information (e.g. use an encryption key); and the nature of the harm.[164]

The obligation is binding on APP entities (federal government agencies and businesses with an annual turnover greater than AUS$3 million),[165] as well as credit reporting bodies, credit providers, and tax file number recipients.[166] ISPs are also subject to the notification obligations even if they would not otherwise be APP entities. If one of these entities become aware that there are reasonable grounds to believe a eligible data breach has occurred, 'as soon as practicable' it must inform the federal Privacy Commissioner of the breach and take reasonable steps to notify each individual whose information has been affected by the breach.[167] If informing individuals individually is not practicable, the organisation can publish a statement on its website and take reasonable steps to publicise the statement.[168] The statement of notification should include the identity and contact details of the entity, a description of the suspected eligible data breach, the kinds of information concerned, and recommendations for affected individuals.[169]

However, these entities may not be obligated to inform about data breaches if they take action in relation to the unauthorised access or disclosure, or loss of information, before this results in serious harm to any of the individuals to whom the information relates, and if a reasonable person would conclude that the access, disclosure or loss would not be likely to result in serious harm to any of those individuals. Such circumstances are not considered to be an eligible data breach, and the entity is not required to notify the individual of the circumstances.[170] The Privacy Commissioner can also give an entity an exemption from its obligations to inform the individuals whose information is at risk if the Commissioner considers it in the public interest to do so (but it seems that the Commissioner is not obliged to make this exemption publicly known).[171]

---

164 *Notifiable Data Breaches Act* s 26WG.
165 *Privacy Act* ss 6, 6C.
166 *Notifiable Data Breaches Act* s 26WE(1).
167 *Notifiable Data Breaches Act* s 26WK(2).
168 *Notifiable Data Breaches Act* s 26WL(2).
169 *Notifiable Data Breaches Act* s 26WK(3).
170 *Notifiable Data Breaches Act* s 26WF.
171 *Notifiable Data Breaches Act* s 26WQ.

The relevant information is information protected by the *Privacy Act* and 'all retained telecommunications data' which ISPs are obligated to retain under the aforementioned data retention requirements. 'Harm' for the purposes of this section means physical, psychological, emotional, reputational, economic and financial harm, and whether that harm is 'serious' is to be considered against various factors, including the subject matter of the information at issue, its sensitivity, intelligibility, protective measures, likely recipients, nature of likely harm and mitigation of damage undertaken.[172]

The Privacy Commissioner will have powers to investigate, make determinations, and provide remedies in relation to non-compliance.[173] The Privacy Commissioner has a new power to require an entity, which it has reasonable grounds to believe has suffered a data breach, to make a notification.[174] The Privacy Commissioner also has the power to declare that an entity does not have to comply with the notification obligation, and can extend the time that an entity has to comply with the notification obligations.[175]

The failure to report an eligible data breach will be viewed as an act that is an 'interference with the privacy of an individual'[176] for the purposes of the *Privacy Act*, and such a failure could be the subject of a complaint to the Privacy Commissioner.[177] Remedies include compensation orders, enforceable undertakings, civil penalty orders (of up to $360,000 for individuals and up to $1.8 million for corporations), or other any orders the Court considers appropriate to compensate an individual for loss or damage, or to prevent or reduce the loss or damage that is being or is likely to be suffered by the individual to whom the information relates.[178]

7. Analysis

172 *Notifiable Data Breaches Act* s 26WG.
173 Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth).
174 *Notifiable Data Breaches Act* s 26WR(1).
175 *Notifiable Data Breaches Act* s 26WQ.
176 *Notifiable Data Breaches Act* s 2.
177 Abrahams and Griffin, above n 152, 77.
178 *Privacy Act 1988* (Cth) ss 25–25A, 80W–80X.

7.1 Domestic perspectives

The notification obligations can be welcomed as an attempt to bring Australian data security practices as regards data breach notification in line with the emerging practice internationally, and as a contribution to the task of improving cybersecurity of Australian public and private sector organisations as threats to this cybersecurity appear to be increasing.

The data breach notification obligations broadly replicate the ALRC's suggestions in 2008, such as the trigger of 'serious harm', the circumstances in which notification may not be necessary (e.g. the use of security measures), the ability for the Privacy Commissioner to waive the notification requirement if not in the public interest, and the kinds of information that a notification ought to contain.

While the introduction of data breach notification seems to have been generally met with cautious approval, there has also been some domestic criticism. Greenleaf identified two major deficiencies: the 'unjustifiable' exemption of organisations from data breach notification requirements which also enjoy *Privacy Act* exemptions such as small businesses, employers, media organisations and political parties (although law enforcement and security agencies would probably require 'special consideration'); and the lack of requirement for the Privacy Commissioner to publish the notices it receives from organisations about data breaches on its website and retain them there, in one location, for future reference and research purposes.[179] Greenleaf also considers that the Privacy Commissioner should publish information about the fact of (possibly anonymised) applications for exemptions from data breach notification requirements and the results of these applications in order to ensure procedural transparency.[180]

Furthermore, the introduction of data breach notification obligations at the federal level in Australia has not yet been accompanied by similar notification obligations at the state level. While state level data privacy legislation is broadly similar to the federal *Privacy Act*, they are

---

179 Graham Greenleaf, 'Australia's Data Breach Notification Bill: Transparency Deficits' (2016) 139 *Privacy Laws and Business International Report* 18, 18–19.

180 Ibid.

not completely consistent as it stands,[181] and can now be viewed as diverging even more in their requirements as regards data breach notification.

Moreover, as regards data security, data breach notification requirements are insufficient alone to protect against data security breaches and the problems they cause.[182] They are an *ex post* response to a breach, and while they may indirectly have a preventative effect, this is not guaranteed. A requirement for more stringent *ex ante* data security measures would address this problem directly, and may be more likely to prevent data breaches from occurring in the first place.

At the time of writing, the Australian Government has been considering additional measures as regards data security, in the form of the criminalisation of the re-identification of de-identified information released by federal government agencies.[183] While data re-identification poses privacy risks, commentators including advocacy group the Australian Privacy Foundation has been concerned that this legislative proposal may inhibit legitimate data security research and does not provide incentives for Australian Government agencies to increase their levels of internal data security.[184]

Strengthened data privacy and security laws in Australia are a necessary complement to this data breach notification legislation. Better enforcement mechanisms, including the right for individuals to bring actions themselves, including in the form of class actions, possibly via a tort of invasion of privacy, may be one mechanism by which this could be achieved. Despite such a cause of action being recommended by law reform bodies,[185] the government does not at this time support the introduction of such a tort,[186] so unless a more 'suitable' case with more

---

181 See, eg, the recent discussion as to whether Queensland should reform its *Information Privacy Act 2009* (Qld) *inter alia* in a way which would make it consistent with the federal Privacy Act. Queensland Government Department of Justice and Attorney-General, *2016 Consultation on the Review of the Right to Information Act 2009 and Information Privacy Act 2009* Consultation Paper (December 2016).

182 Smyth, above n 122, at 180.

183 Privacy Amendment (Re-identification Offence) Bill 2016 (Cth).

184 Australian Privacy Foundation, Submission to Senate Legal and Constitutional Affairs Committee, Privacy Amendment (Re-Identification Offence) Bill 2016, 16 December 2016 <https://www.privacy.org.au/Papers/SLCA-DeId-161216.pdf>.

185 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014); Standing Committee on Law and Justice, New South Wales Legislative Council, *Remedies for the Serious Invasion of Privacy in New South Wales* (2016).

186 See Law, Crime and Community Safety Council, *October 2016 Communique* (21 October 2016) Australian Government, Attorney-General's Department <https://www.ag.gov.au/About/Committees

'suitable' factual scenario than *Lenah Game Meats* reaches the High Court,[187] a tort of invasion of privacy remain a more academic than pragmatic solution. However, the use of the '*Australian Consumer Law'*, with its possibilities for private actions, to address data privacy and security breaches may be a (partial) solution to this issue.[188] Furthermore, the aforementioned pending NSW Ambulance class action may well be the 'more suitable case' to establish a tort of invasion of privacy in Australian common law.

Finally, by restricting its scope to 'personal information', the notification scheme may not be sufficiently forward-looking to developments such as the Internet of Things (IoT). There are ambiguities over whether data collected by IoT devices will constitute 'personal information' for the purposes of the *Privacy Act*. While in the EU, data protection authorities seem to consider that most data collected by IoT devices would be attributable to individuals and thus 'personal data',[189] the situation in Australia after the recent Federal Court decision in *Privacy Commissioner v Telstra* casts doubt on whether that would also be the case here.[190] Since the notification requirement only applies to 'personal information', this may well entail that only part of the proliferation of data gathered by IoT devices would be subject to this requirement. The legislation also does not address data breaches which involve the exposure of commercially sensitive information protected by trade secrets and other proprietary data regimes.[191]

7.2 International comparisons

andCouncils/Law-Crime-and-Community-Safety-Council/Pages/default.aspx>; Gabrielle Upton, 'NSW Government response to the Legislative Council Standing Committee on Law and Justice's report into *Remedies for the serious invasion of privacy in New South Wales*' (Response to Recommendations, New South Wales Government, 5 September 2016).

187 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63.

188 Corones and Davis, above n 36.

189 Pinsent Masons, *'Internet of Things' Data Should be 'Treated as Personal Data', Say Privacy Watchdogs* (21 October 2014) Out-Law.com <https://www.out-law.com/en/articles/2014/october/internet-of-things-data-should-be-treated-as-personal-data-say-privacy-watchdogs/>.

190 *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4. See Anna Johnston, 'Data, Metadata & Personal Information: A Landmark Ruling From The Federal Court' (2017) 31 *Law Society of NSW Journal* 82, 82–3.

191 On this point see, eg, Peter Yu, 'Trade Secret Hacking, Online Data Breaches, and China's Cyberthreats' (2015) *Cardozo Law Review De Novo* 130.

There are a number of points of comparative analysis for the new Australian requirements and overall situation as compared to those in the US and EU detailed above. Firstly, certain substantive features of the schemes are compared, namely the data covered and the trigger for notification. Then, the overall models presented by the different jurisdictions' schemes.

7.2.1 Substantive Provisions

Through the various schemes detailed in this article in Australia, the United States and European Union, two substantive points of comparison can be identified: the kind of data which is covered by the data breach notification scheme, and the triggering event for notification.

Regarding the data covered by the data breach notification schemes above, even schemes which cover data about individuals vary somewhat in what precisely this data comprises. The Australian scheme covers certain breaches of 'personal information' ('information or an opinion about an identified individual, or an individual who is reasonably identifiable'),[192] while the EU GDPR notification requirements concern 'personal data' ('any information relating to an identified or identifiable natural person').[193] While these terms and their definitions may seem largely similar, the aforementioned Federal Court decision in *Privacy Commissioner v Telstra* casts doubt over whether 'personal information' covers as expansive a range of data as 'personal data' in the EU. The issue of what data or information is covered by data breach notification schemes becomes more complex in the US, where 'personally identifiable information', a central concept in information privacy laws there, does not have a uniform definition across the different state and federal laws.[194] This can be seen in the kinds of data or information which are specifically listed, and thus covered by data breach notification provisions, in some of the statues discussed above in Section 4.1. These lists of specific types of data usually result in a more restricted amount of relevant data types in US laws compared to the EU and Australia's definitions of personal data and personal information respectively. However, the advantage of the approach of some US statutes to listing specific types of information is that there is some clarity as to what information is covered; the challenge of the

[192] *Privacy Act*, s 6.
[193] *GDPR*, Art 4 (1).
[194] See: Paul Schwartz and Daniel Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *New York University Law Review* 1814.

broader EU and Australian approaches lies in their application to contemporary data practices, and the fact that it is possible to re-identify de-identified information, thus rendering potentially large and contextual the pool of 'personal information' or 'personal data'.

The trigger for notification of a data breach can also be compared across the different jurisdictions. The Australian data breach notification requirements may actually position Australia as a leading jurisdiction on the topic of strong data security measures on a literal reading of the legislation, since an entity may be obliged to inform of a breach if it 'believes' one to have taken place, and not just after it discovers such a breach has taken place.[195] (Although part of the trigger for notification in the Australian legislation is that a reasonable person would conclude that the unauthorised access or disclosure of information would be likely to result in 'serious harm' to individuals.) This can be contrasted with the EU GDPR scenario, where individuals whose personal data or privacy would be 'adversely affected' must be informed of a breach. Thus it seems that a higher threshold of harm must be suffered for the Australian notification requirement to be triggered. Then, Australian entities need only take 'reasonable steps' to inform individuals of such breaches, whereas the obligation to inform individuals in the EU legislation is less qualified. Here, the wording of the Australian legislation may be conceptualised as closer to the 'risk-based' approach taken by US data breach notification requirements, where the possible consequences of the breach, or the risk that adverse consequences may occur, can be a factor in triggering notification. The EU's GDPR data breach notification requirements on its face seems less qualified, although how breached data being 'adversely affected' is conceptualised may also involve an assessment of risk in practice.

The extent to which these legislative divergences actually translate into practice in Australia, the EU and the American jurisdictions remains to be seen. It may well be that these differences are academic, and in practice the different jurisdictions deal very similarly with similar data breach scenarios. However, these legislative differences may still matter, given the GDPR's extra-territorial reach: its provisions purport to apply to data processors and controller located

---

195 Leonard Kleinman, 'Hidden challenges emerge as data breach notification laws finally hit Australia' *Australian Financial Review*, 28 November 2016 <http://www.afr.com/technology/web/security/hidden-challenges-emerge-as-data-breach-notification-laws-finally-hit-australia-20161125-gsxnri>.

outside of the EU which process the data of EU citizens.[196] This has sparked debate in Australia about Australian businesses' compliance with the GDPR if they process EU citizens' data, including as regards data breach notification given the different formal standards in these two jurisdictions.[197] An Australian entity which suffers a data breach may in theory have to comply with both the new data notification obligation in Australia, and the notification obligation under the GDPR if it is processing EU citizens' data. Yet a scenario is conceivable, for instance, in which the GDPR notification is triggered by a breach but those same circumstances do not trigger the Australian legislative notification obligation.

7.2.2 Models

As an amendment to the '*Privacy Act'*, the Australian legislative introduction of data breach notification may be conceptualised as being closer to the European than American model in its form, with data breach notification requirements included in its own data privacy laws (firstly the ePrivacy Directive, and then the GDPR). The fact that the Australian legislation is also limited in application to data breaches involving personal information is also similar to the European approach in its data privacy legislation. One divergence is that Australia does not have mandatory data breach notification laws for non-personal information-related data breaches, unlike the NIS Directive and eIDAS Regulation in the EU.

Furthermore, the federal legislation in Australia and harmonised law at the regional level in the EU are closer models than the fragmented state-by-state approach to mandatory data breach notification legislation in the US – although it is important to note, as mentioned above, that the state- and territory-level information privacy regimes in Australia do not currently include their own respective data breach notification obligations.

---

196 *GDPR* art 3(2). See: Shakila Bu-Pasha, 'Cross-border issues under EU data protection law with regards to personal data protection' (2017) *Information & Communications Technology Law* (forthcoming).

197 See Lora Shaw, *The Impact of the New European General Data Protection Regulation in Australia* (22 December 2015) Keypoint Law <http://www.keypointlaw.com.au/keynotes/impact-new-european-general-data-protection-regulation-australia>.

Yet the sector-specific approach to data breach notification, prominent in the US, is not entirely absent in the EU, as discussed above, with data breach notification requirements found in other pieces of legislation beyond the core data privacy instruments. In Australia, the only other main legislative data breach notification requirement is found in the '*My Health Records Act'*. It would be prudent for Australia, in considering any future data breach notification requirements, to ensure sector-specific fragmentation is avoided, as well as fragmentation as regards state-level obligations.

The US model of data breach notification legislation and its more general approach to data breaches, including the role of litigation, may, at a more conceptual level, be viewed as more clearly instrumentalist to the aim of avoiding or mitigating cybercrime - rather than the protection of personal data or information for its own sake, an approach which may be reflected more in the rights-based EU model. Nevertheless, it may well be that the EU GDPR's data breach notification provisions are enforced in a more instrumentalist fashion, where there are high risks to personal data security such as cybercrime. It may also the case that this is what will happen too in Australia. Given the novelty of both the GDPR and the Australian provisions, the extent to which a risk-based instrumentalist approach is taken, or not, can only be assessed once their practical implementation has taken place.

8. Conclusion

This article has examined the new data breach notification requirements in Australian federal law against a backdrop of cybersecurity concerns more generally, the unique domestic conditions of data privacy legislation in Australia, and similar laws in other jurisdictions, namely the US and EU. Overall, the introduction of data breach notification requirements is to be welcomed from a data privacy and security perspective, with some evidence of positive impact, although the legislation has various deficiencies.

The introduction of data breach notification obligations in Australia is consistent with international trends for these obligations. However, from the perspective of transnational businesses and other entities, compliance with these obligations in different jurisdictions may prove complicated and burdensome given the lack of international alignment of these measures, and even a lack of harmonisation within jurisdictions, as can be seen from the discussion in this article.

While this article has provided a comparative context for Australian data breach notification requirements with analogous requirements in the two major Western jurisdictions of the US and EU, the adoption of cybersecurity legislation in China including data breach notification requirements, is a significant development in the Asia Pacific region and may further complicate compliance for businesses operating transnationally. However the current regional free trade agreement negotiations for the Regional Comprehensive Economic Partnership (RCEP), including *inter alia* Australia and China, and the likelihood this agreement will include digital economy matters, may result in some harmonised standards on this topic at least in the Asia Pacific region.[198]

As cybersecurity matters become more prominent on political and business agenda in Australia and internationally, data security is likely to increase in importance, and may be subject to further legislative reform in Australia and other jurisdictions. Further research would be illuminating on the implementation, impact and efficacy of data breach notification requirements in Australia, and the extent to which differing standards in different jurisdictions impose burdens on entities operating transnationally, in order to guide future legislators and policymakers.

[i] Vice-Chancellor's Research Fellow, Faculty of Law, Queensland University of Technology, Research Associate, Tilburg Institute for Law, Technology and Society, University of Tilburg. The author would like to thank Lisa Kruck and Rebecca Morrison for their research assistance for this article, and Monique Mann, Amanda Scardamaglia and John Selby for their comments on earlier drafts. This research has been funded by QUT

198 See Deborah Elms, 'Evolving Digital and E-Commerce Trade Rules for Northeast Asia' *KIEP Research Paper Studies in Comprehensive Regional Strategies* 16-09.

Australian Centre for Health Law Research/Institute of Health and Biomedical Innovation Research Collaboration Grant ‘Handle with Care: Digitally Managing Health Information Infrastructure’.