Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

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

Angela Daly [a,b,*]

[a] *Queensland University of Technology, Brisbane, Australia*

[b] *Tilburg Institute for Law, Technology and Society, University of Tilburg, Tilburg, Netherlands*

Keywords:
Data breach notification
Data protection
Data security
Australia
European Union
GDPR
US
FTC

A B S T R A C T

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 security measures including 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

* Faculty of Law, Queensland University of Technology, GPO Box 2434, Brisbane, QLD 4001, Australia; Tilburg Institute for Law, Technology, and Society (TILT), P.O. Box 90153, 5000 LE Tilburg, The Netherlands.
E-mail address: Angela.daly@qut.edu.au

https://doi.org/10.1016/j.clsr.2018.01.005
0267-3649/

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

Please cite this article in press as: Angela Daly, The introduction of data breach notification legislation in Australia: A comparative view, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.01.005

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.

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 cybersecurity legislation 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 that 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 because of human error or incompetence. Data breaches can also occur because 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* 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

[2] See, e.g., 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>.

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

[4] See, e.g., 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-madison.

Please cite this article in press as: Angela Daly, The introduction of data breach notification legislation in Australia: A comparative view, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.01.005