available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The mandatory notification of data breaches: Issues arising for Australian and EU legal developments

Mark Burdon [a], *Bill Lane* [a], *Paul von Nessen* [b]

[a] *Faculty of Law, Queensland University of Technology, Australia*
[b] *Business Law and Taxation, Monash University and Consultant, McCullough Robertson Lawyers, Australia*

Keywords:
Data breach notification
Data protection
Information privacy
Identity theft
Information security

ABSTRACT

Public and private sector organisations are now able to capture and utilise data on a vast scale, thus heightening the importance of adequate measures for protecting unauthorised disclosure of personal information. In this respect, data breach notification has emerged as an issue of increasing importance throughout the world. It has been the subject of law reform in the United States and in other jurisdictions. This article reviews US, Australian and EU legal developments regarding the mandatory notification of data breaches. The authors highlight areas of concern based on the extant US experience that require further consideration in Australia and in the EU.

1. Introduction

An estimated 341 million records containing personal or sensitive person information have been disclosed in the United States (US) without proper authorisation since 2005.[1] Unauthorised disclosure of personal information can take several forms.[2] For example, the theft of computer equipment or storage media,[3] computer hacking incidents that take advantage of ineffective information security measures,[4] the inadvertent publication of personal information,[5] the improper decommissioning of storage media or the misappropriation of personal information by employees.[6,7] The

[1] Privacy Rights Clearinghouse, *A Chronology of Data Breaches* (2009) http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP; at 18 December 2009.

[2] See e.g. United States Government Accountability Office, 'Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown' (GAO-07-737, 2007); C M Curtin and L T Ayres, *Using Science to Combat Data Loss: Analysing Breaches by Type and Industry* (2009) <http://web.interhack.com/publications/breach-taxonomy>; at 29 April 2009; F J Garcia, 'Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time' (2007) 17(3) *Fordham Intellectual Property, Media & Entertainment Law Journal* 693.

[3] See e.g. Department of Veterans Affairs Office of Inspector General, 'Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans' (Department of Veterans Affairs, 2006).

[4] See e.g. J Pereira, 'Breaking The Code: How Credit-Card Data Went Out Wireless Door – In Biggest Known Theft, Retailer's Weak Security Lost Millions of Numbers', *The Wall Street Journal* (New York), 4 May 2007, A1.

[5] Nj.com, *N.J. accidentally reveals personal data of 28K unemployed residents* (2009) <http://www.nj.com/news/index.ssf/2009/05/3k_unemployed_nj_residents_may.html>; at 9 June 2009.

[6] See e.g. Computer Security Institute and Federal Bureau of Investigation, 'Computer Crime and Security Survey' (2006) 12 <http://pdf.textfiles.com/security/fbi2006.pdf>; at 27 January 2010.

[7] See e.g. Treasury Inspector General for Tax Administration, 'The Internal Revenue Service is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices' (Treasury Inspector General for Tax Administration, 2007) <http://www.treas.gov/tigta/auditreports/2007reports/200720048fr.pdf>; at 27 January 2010.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2010.01.006

scale of the US problem is captured by a Harris Poll conducted in October 2006.[8] Researchers led by Professor Alan Westin, surveyed over 2000 US citizens and found that 22% of respondents claimed to have received notification from one or more organisations that their personal information had been lost, stolen or improperly disclosed between 2003 and 2006. It is possible, based on an extrapolation of these figures, that 49 million US citizens may have potentially received formal notification of a data breach of their personal information.[9]

The continuous, and seemingly never-ending, procession of high-profile US data breaches generated sufficient levels of public concern to warrant the involvement of US legislators, initially at state level and eventually in Washington. A new subset of law developed – mandatory data breach notification that incorporates elements of privacy regulation, consumer protection and corporate governance mechanisms regarding the security of personal information and information systems. The first of these laws, Californian Civil Code § 1798.29(a) was a direct response to the advent of large-scale identity theft crimes and has been widely used as a model by other US legislatures.[10]

Since their enactment, US data breach notification laws have highlighted the significance of the data breach problem, prompting legal developments in other jurisdictions[11] including Australia and the European Union (EU). Australian developments focus on amendments to the *Privacy Act (Cth) 1988* (hereafter ''Privacy Act'') and EU initiatives are centred on Directive 2002/58/EC (hereafter ''e-Privacy Directive'').

This article examines the development and application of mandatory data breach notification laws and the authors highlight key concerns based on the US literature that should inform Australian and EU developments. Section 2 details the development of data breach notification laws from their genesis in the US. Section 3 explains what is known about Australian data breaches and outlines recent legislative proposals for an Australian data breach notification scheme. Section 4 highlights recent EU developments. Section 5 then highlights issues to be resolved regarding Australian and EU developments and concluding observations are set forth in Section 6.

2. US data breach notification laws

The first mandatory data breach notification law was enacted by the Californian legislature in 2003. The Californian Civil Code § 1798.29(a) requires:

> *'[a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, [to] disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.'*

Accordingly, any Californian business that suffered a data breach of unencrypted and computerised personal information, which entails an unauthorised acquisition by another person, is required to notify Californian residents about the incident. Organisations are to notify individuals within a timeframe that is expedient and without reasonable delay. However, law enforcement agencies can request a delay if notification would impede a criminal investigation. The actual form of organisational notification can be made by letter, electronically in conformance with federal regulations or by a form of substitute notice, entailing email, or ''conspicuous posting'' on the organisation's website or via state media sources. The latter option is only available if the data breach involved more than half a million individuals or would exceed a cost of over $250,000.

In accordance with the Code, not all data breaches need to be notified as the law contains a range of exemptions. For example, a data breach does not need to be notified if it relates to a good faith acquisition of personal information by an employee or agent of the breaching organisation or if the personal information acquired without authorisation is encrypted. Additionally, the Californian law only covers data breaches of computerised information and thus provides a detailed and limiting definition of personal information. Essentially, this means an individual's name in combination with one or more other identifying items – such as a social security number, state driver licence or ID number, financial account number details, medical or health insurance details.

The definition of personal information signifies a key underlying rationale of the Californian data breach notification law – that organisational notification provides individuals with a means to protect themselves from adverse consequences of unauthorised acquisition of their personal information, specifically in the form of identity theft or identity fraud related crimes.[12] The cogency of this rationale appeared to have been borne out almost immediately, post implementation of the Californian law, after notification by Choicepoint, one of the largest data brokerage firms in the US, of a major data breach incident.[13] In February 2005, criminals posing as a small business were able to gain access to Choicepoint's data as a legitimate subscriber of their services. The criminals acquired personal information of 163,000 persons, which culminated over 800 incidents of identity theft.[14]

[8] Harris Interactive, *Many U.S. Adults Claim to Have Been Notified that Personal Information Has Been Improperly Disclosed* (2006) <http://www.harrisinteractive.com/harris_poll/index.asp?PID=708> at June 9 2009.

[9] Harris Interactive, *Many U.S. Adults Claim to Have Been Notified that Personal Information Has Been Improperly Disclosed* (2006) <http://www.harrisinteractive.com/harris_poll/index.asp?PID=708> at June 9 2009.

[10] K E Picanso, 'Protecting Information Security Under a Uniform Data Breach Notification Law' (2006) 75(1) *Fordham Law Review* 355, 369.

[11] E Preston and P Turner, 'The Global Rise of a Duty to Disclose Information Security Breaches' (2004) 22 *John Marshall Journal of Computer & Information Law* 457.

[12] California Office of Privacy Protection, 'Recommended Practices on Notice of Security Breach Involving Personal Information (California Office of Privacy Protection, 2008): 6.

[13] P N Otto, A I Anton and D L Baumer, 'The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information' (2007) 5(5) *IEEE Security & Privacy* 15.

[14] P N Otto, A I Anton and D L Baumer, 'The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information' (2007) 5(5) *IEEE Security & Privacy* 15.