University of New South Wales
University of New South Wales Faculty of Law Research Series
2009

Year 2009 *Paper* 11

Data Breach Notification Law Across the World from California to Australia

Alana Maurushat*

*University of New South Wales

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

http://law.bepress.com/unswwps-flrps09/art11

Copyright ©2009 by the author.

Data Breach Notification Law Across the World from California to Australia

Alana Maurushat

Abstract

Data breach notification and disclosure laws are emerging around the globe. The following article and table examine the specifics of data breach notification frameworks in multiple jurisdictions. Over the year of 2008, Alana Maurushat of the Cyberspace Law and Policy Centre, with research assistance from David Vaile and student interns Renee Watts, Nathalie Pala, Michael Whitbread, Eugenie Kyung-Eun Hwang and David Chau, compiled the data. The table represents a detailed survey of data breach disclosure requirements in 25 countries, conducted by surveying those current or proposed statutory or similar instruments setting out the nature and conditions of such requirements to give notice. The Centre hopes that the table will be useful to compare and contrast elements of data breach notification schemes. The researchers at the CLPC will research the effectiveness of such schemes in future projects.

Data Breach Notification Law across the World from California to Australia

Alana Maurushat*

Originally published in Privacy Law and Business International (February, 2009)

Data breach notification and disclosure laws are emerging around the globe. In essence, data breach notification legally requires corporations and organisations to notify individuals when a breach of security leads to the disclosure of personal information.[1] Two related phrases aptly describe the impetus behind such laws: *"Sunlight as disinfectant"* and the *"Right to Know"*.[2] Data breach notification is promulgated under the theory that the consumer has the right to know when *their* personal information has been stolen or compromised. Equally, it is hoped that data breach notification laws will provide a necessary incentive for corporations and organizations to take adequate steps to secure personal information held within their organization. In this sense, exposing security breaches of corporations will shine "sunlight" onto an organization's security practices, and will "disinfect" those problematic security areas requiring change. Article

The scope of such notification and disclosure schemes varies greatly from country to country. Many jurisdictions such as the United States, the European Union and Australia have tabled Bills or passed Acts legislating mandatory data breach disclosure. Other jurisdictions such as Canada and Japan have instituted voluntary guidelines. In many jurisdictions, data breach notification is currently sector specific (Eg. banking and financial sector or the telecommunications sector). Many of the current proposals, guidelines, and laws take from the experience of the United States, most notably with California which in 2002 passed strict data breach notification laws. Jurisdictions borrowing from the American experience have gained insight into aspects from some of these initial laws. However, some elements from current proposals in Australia, Canada and the EU highlight and ignore problematic aspects of the U.S. legislation.

A recent study by Fred Cate of the Centre for Information Policy Leadership exposes 5 key risks which other jurisdictions such as the European Union and Australia have overlooked:[3]

---

* Alana Maurushat is Lecturer, Deputy Director of the Cyberspace Law and Policy Centre, and PhD Candidate – all within the Faculty of Law, the University of New South Wales.

bepress Legal Repository

Hosted by The Berkeley Electronic Press

1. Defining "security breach" so broadly that it makes the term, and notice it prompts, less meaningful;

2. Focusing too much on notices to address security breaches;

3. Justifying notices as a response to identity fraud;

4. Ignoring the limits of notices and the negative consequences of their inappropriate use; and

5. Applying a twentieth-century response to a twenty-first century problem.

Two major deficiencies of a number of proposals and frameworks have emerged. The first, and most notable, is whether data breach notification obligations actually reduce financial fraud and identity theft. The second relates to "trigger mechanisms" and duty to report to overseeing body.

The question of whether data breach laws will impact on the level of financial fraud and identity theft is largely unproven. [4] In one of the only empirical studies done to date, researchers at Carnegie Mellon University compared levels of financial fraud and identity theft with states that had data breach notification law with those states who did not. Researchers used data from the Federal Trade Commission from 2002 to 2006 and found that there was no "statistically significant result" of data breach laws. This is a significant finding given that many jurisdictions have introduced such laws to incentivize better security practices – *"sunlight as disinfectant"*. It must be acknowledged, however, that there were a number of acknowledged factors in the Carnegie Mellon study who may have impacted on the statistical findings:[5]

1. The use of reported crime data may not reflect actual crimes.

2. Financial fraud and identity theft are generally under-reported.

3. Financial fraud and identity theft may not originate from data breaches, but rather, from other types of actions such as social engineering. If so, the effectiveness of a data breach law is bound to be limited.

4. Not enough time has elapsed since legislation was passed for organizations to fully implement the level of required change to security practices to make an impact on the statistics.

5. The security controls implemented by organizations are ineffective at preventing breaches.

6. Consumers, once notified, are not making the required changes to their consumption patterns to better secure their personal information.

bepress Legal Repository

More studies are required to statistically analyse the effectiveness of data breach notification laws. So far, all studies have been performed in the United States.[6] Additional studies will be needed to assess a country's data breach laws as measured internally, as well as to measure how a country's data breach laws compare with the laws of other countries. In the latter case, particular heed should be paid to the "trigger mechanism" and duty to report to an overseeing body such as the Privacy Commissioner.

The most important data breach component is the "trigger mechanism". In California, the obligation to notify an individual of a security breach is triggered in the likelihood that the breach will result in a "serious harm" or involves a "serious risk". The threshold of "serious harm" or "serious risk" is an external determination. Security breaches must further be reported to the relevant overseeing body. Failure to report results in sanction. In Canada[7] and Australia[8] the standard is again "serious harm" or "serious risk". It is the internal organization itself, however, that determines what compromises a "serious harm" or "serious risk". There is no external body that performs this function. Additionally, there is no requirement to report to an overseeing body nor is there sanction for failing to notify individuals of a security breach. The "trigger mechanism" is thus assumed to at a lower level than jurisdictions like California.

The following table examines the specifics of data breach notification frameworks in multiple jurisdictions. Over the year of 2008, Alana Maurushat of the Cyberspace Law and Policy Centre, with research assistance from David Vaile and student interns Renee Watts, Nathalie Pala, Michael Whitbread, Eugenie Kyung-Eun Hwang and David Chau, compiled the data. The table represents a detailed survey of data breach disclosure requirements in 25 countries, conducted by surveying those current or proposed statutory or similar instruments setting out the nature and conditions of such requirements to give notice. The Centre hopes that the table will be useful to compare and contrast elements of data breach notification schemes. The researchers at the CLPC will research the effectiveness of such schemes in future projects.

bepress Legal Repository

Hosted by The Berkeley Electronic Press

Information Compiled January 2009	1. The United States	SB1386 California Security Breach Information Act	S-239 (scheduled for debate in congress(?))	S-P 248	S-495 (scheduled for debate in congress(?))	S-806	S-1178 (scheduled for debate in congress(?))	S-1260	2. Canada: Privacy Breach Guideline	3. Australia	Privacy Amendment Bill 2007	Draft Guide 2008	ALRC Discussion Paper	4. New Zealand: Privacy Breach Guidelines	5. South Africa: SALRC Draft Bill on Privacy 2009	6. Japan	7. South Korea	8. China	9. Hong Kong: Personal Data (Privacy) Ordinance Code of Practice on Consumer Credit Data (2003); Privacy at Work (2004); Code of Practice on the Identity Card	10. India: Information Technology Act 2000 and Amendment Act 2006	11. European Union: Directive (Privacy)	EU Commission Proposal	12. United Kingdom: Proposal by House of Lords Committee	UK: Privacy and Electronic Communications Regulations	13. Ireland: Data Protection Act (1988) and Amendment Act (2003); and	14. Spain: Personal Data Protection Act: Telecommunications Act	15. Italy: Data Protection Code	16. Sweden: Electronic Communications Act	17. The Netherlands: Telecommunications Act	18. France: Postal and Electronic Communications Code	19. Germany: § 93 Telecommunications Act	20. Denmark: Act on Processing of Personal Data 2000	21. Norway: Personal Data Act 2000	22. Hungary: On the Protection of Personal Data and the Disclosure of	23. Slovakia: Protection of Personal Data Act 2002 and Amendment Act 2005	24. Malta: Data Protection Act 2001
Actual (A) or Proposed (P) or Guideline (G)		A	P	P	P		P	P	G		P	G	G		P	G	P	?	A	A	P	P	G	A	A and G	A	A	A	A	A	A	A	A	A	A	A	A
Broad Non-Specific Definition of Personal Information															Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y						Y	Y	Y	Y	Y	Y
Driver's License Number		Y	Y	Y	Y		Y	Y	Y			Y	Y	Y	Y																						
Financial Account Number		Y	Y		Y		Y	Y	Y			Y	Y	Y	Y																						
Debit Card Number		Y	Y	Y	Y		Y	Y	Y			Y	Y	Y	Y																						
Credit Card Number		Y	Y	Y	Y		Y	Y	Y			Y	Y	Y	Y																						
Checking Account Number			Y		Y		Y	Y							Y																						
Savings Account Number			Y		Y		Y	Y							Y																						
Personal identification Number			Y	Y	Y		Y	Y							Y																						
Electronic Identification Number			Y												Y																						
Employer Identification Number			Y				Y								Y																						
National ID (eg. Social Security)		Y	Y	Y	Y		Y	Y	Y					Y	Y				Y (Code: Identity)																		
Routing Code					Y										Y																						
Digital Signature																																					
Biometric Data			Y	Y	Y										Y																					Y: Special rules	
Fingerprints			Y		Y			Y							Y																						
Account Passwords			Y		Y		Y								Y																						
Mother's Maiden Name				Y	Y																																
Address					Y		Y								Y																						
Date of Birth			Y		Y										Y																						
Medical Information									Y				Y	Y	Y																			Y	Y		Y: Special rules	
Telecommunications Device			Y																																		
Other			Y	Y																																	
Encrypted Data Safe Harbour		Y	Y		Y			Y							Y																						
Likelihood of 'serious harm' provision OR "significant risk"				Y			Y	Y	Y			Y	Y	Y		N	N				Y	N	Y	Y		Y	Y	Y	Y	Y	Y					
External determination			Y		Y											N	N		Y		Y	N															
Self Determined Standard				Y	Y		Y	Y	Y		Y	Y	Y	Y		N	N		Y: (Code: Consumer Credit)			N												Y			
Any Harm' provision		Y	Y		Y						Y	Y				N	N					N															
Notice to Privacy Commissioner (or equivalent).			Y	Y	Y		Y	Y	Y			Y	Y	Y	Y	Y	Y	Y	Y: (Code: Consumer Credit)		Y	Y	Y	N	y			Y						Y	y	Y	Y
Data Owner/ Licenser Notify Individuals		Y	Y	Y	Y		Y	Y	Y		Y	Y		Y	Y	Y	Y																	Y		Maybe	
ISP or Network Operator Notify Subscribers not all users															Y limitations							Y		Y		Y	Y		Y	Y	Y					Maybe	
Data Maintainer (including ISP in Europe) Notify Individuals			Y		Y		Y	Y	Y		Y			Y	Y	Y	Y									Y	Y										
Electronic Notice Allowed		Y	Y	Y	Y		Y	Y	Y		Y	Y	Y	Y	Y																						
Substitute Notice Allowed		Y		Y			Y	Y	Y		Y	Y	Y	Y	Y																						
Set Time Period to Notify Individuals							Y		Y		N		Y	Y	Y																						
Safeguarding of Information Required			Y	Y	Y		Y	Y	Y					Y	Y	Y	Y		Y	y		Y			Y								Y	Y		Y	Y
Appropriate Security Measures' Specified															Y		Y		Y: (Code: Consumer Credit)				N	N	Y	Y	Y	N	N	N	N				Y		
Specific Monetary Penalties Outlined		Y	Y		Y								Y			Y	Y		Y	Y					y							Y	Y to liability		Y	Y
Security Credit Freezes						Y	Y																														
Best Practice Security Program								Y	Y																											Y	
Data Destruction and Disposal		Y		Y	Y		Y							Y	Y		Y		Y						Y							Y	Y		Y	Y

bepress Legal Repository

Register of notifications to be maintained											Y								Y: (Code: Consumer Credit)															Y	Y

bepress Legal Repository

Hosted by The Berkeley Electronic Press

[1] Australian Law Reform Commission, Review of Australian Privacy Law, Discussion Paper 72, September 2007, page 1293.

[2] The idea comes from a paper written by Sasha Romanosky, Rahul Telang, Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft? Seventh Workshop on the Economics of Information Security, June, 2008. These phrases are attributable to Justice Louis Brandeis, 1933, http://www.brandeis.edu/investigate/sunlight (accessed Janaury 30, 2009).

[3] Fred Cate, "Information Security Breaches: Looking Back & Thinking Ahead" The Centre for Information Policy Leadership (2008) available at www.informationpolicycentre.com/

[4] Elizabeth Garner, "Is Comprehensive Federal Data Security Legislation Necessary to Protect U.S. Businesses, Consumers and the Government From Identity Theft and Other Crimes?" available at https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/32775/Thesis.Final.May.16.2008.pdf (accessed January 28, 2009).

[5] See note 3 above.

[6] See, for example, reports by the Federal Trade Commission. "FTC Identity Theft Survey Report: 2003" and "FTC Identity Theft Report: 2007".

[7] Public Interest Advocacy Centre (PIAC), "Submission to Industry Canada Following the Stakeholder Consultation on the Proposed Model for Data Breach Notification: April 25, 2008 available at

[8] Graham Greenleaf, Lee Bygrave and Nigel Waters, "Strengthening uniform privacy principles: an analysis of the ALRC's proposed principles'", Submission to the Australian Law Reform Commission on the Review of Australian Privacy Laws Discussion Paper 72, December 2007, Data Quality (UPP 7).

bepress Legal Repository