

# *The importance of mandatory data breach notification to identity crime*

Eric Holm

Faculty of Business, Federation University Australia  
PhD Student, Bond University  
Ballarat, Australia  
[e.holm@federation.edu.au](mailto:e.holm@federation.edu.au)

Geraldine Mackenzie

Faculty of Law, Bond University  
Robina, Australia  
[gmackenz@bond.edu.au](mailto:gmackenz@bond.edu.au)

**Abstract—** The relationship between data breaches and identity crime has been scarcely explored in current literature. However, there is an important relationship between the misuse of personal identification information and identity crime as the former is in many respects the catalyst for the latter. Data breaches are one of the ways in which this personal identification information is obtained by identity criminals, and thereby any response to data breaches is likely to impact the incidence of identity crime. Initiatives around data breach notification have become increasingly prevalent and are now seen in many State legislatures in the United States and overseas. The Australian Government is currently in the process of introducing mandatory data breach notification laws. This paper explores the introduction of mandatory data breach notification in Australia, and lessons learned from the experience in the US, particularly noting the link between data breaches and identity crime. The paper proposes that through the introduction of such laws, identity crimes are likely to be reduced.

**Keywords—***identity crime; data breaches; mandatory breach reporting; privacy*

## I. INTRODUCTION

The Australian Government has raised considerable debate around the introduction of data breach notification as a way of preserving data arising through breaches of data [1]. Public instances of data breaches have attracted awareness of the need for greater protection of personal data [1]. The heightened public awareness of these issues has prompted the Australian Government to introduce laws in Australia to deal with data breach notification [2], the fundamental purpose of which is that the person whose data has been breached has a “right to know” of this breach [3]. Mandatory data breach notification is a legal requirement on the holder of data to notify those affected in the event of a data breach [1]; thus, through being notified of a breach, the person whose data has been misused may take appropriate action to prevent further harm resulting [4].

There is scarce data on the link between the notification of data breaches and identity crime, however, based on data from the United States it is argued that a discernable reduction in the incidence of identity crime can occur through the introduction of mandatory breach notification laws [5]. Australia is in the

process of introducing mandatory breach notification laws, which are in their final stages of legislative enactment, which will provide new opportunities to consider the relationship between mandatory breach notification and crime, in particular, identity crime.

## II. THE VULNERABILITIES OF PERSONAL IDENTIFICATION INFORMATION

Advances in technology have resulted in increased volumes of information being stored electronically, particularly on the Internet [5], which, include personal identification information [6]. Personal identification information is information that is unique to the person, for example their name and credit card number [7]. In the event of a data breach, it is this information that can present vulnerabilities for identity crime to the individual [8]. Indeed, 33% of the information exposed through data breaches includes personal identification information like names, addresses and credit card numbers [9].

In many countries there is no compulsion to record breaches of data. Further, in Australia, at present, there is no formal requirement to such breaches [1], however Australia will introduce data breach notification requirements in 2014 [10]. Prior to enactment, the approach to regulating privacy has been regulated by the *Privacy Act 1988* (Cth), under which organisations and agencies storing personal information are subject to requirements to provide adequate security protection [11]. The Privacy Act applies to the use of information which is sensitive, including personal identification information [11]. There are criminal sanctions for the possession of personal identification information with the purpose of committing an offense in many States, for example Queensland [12]. However, when it comes to data breaches, the responsibility for the protection of private information is less clear in Australia, where an organisation or agency is not compelled to report data breaches, and the responsibility for this notification is therefore voluntary and falls back to the organisation concerned. This lack of mandatory reporting can have ramifications for identity theft.

### III. EXPLORING THE LINKS BETWEEN DATA BREACHES AND IDENTITY CRIME

The cost of data breaches has steadily increased [13]. At the same time, the number of identity crimes has increased, with for example the United States having over 15 million peoples that are victims of this crime each year [14]. A proportion of identity crime can be definitively traced back to data breaches. Hence, the causal relationship between data breach and identity crime has significance. Noteworthy is the statement by the United States Federal Trade Commission that the introduction of data disclosure laws has reduced identity theft by at about 6 percent [7]. This points toward a reduction, albeit a small one, in the incidence of identity crime as a direct result of regulatory implementation. Although early to predict, it is probable that the same trend will be evident with the introduction of a mandatory breach notification in Australia.

### IV. THE DRIVERS FOR MANDATORY BREACH NOTIFICATION LAWS IN AUSTRALIA

In the existing regulatory environment in Australia, an organisation or agency involved in a data breach often exercises some discretion in dealing with that breach. As a consequence, many breaches may not be reported and appropriately actioned through notifying those involved or the Privacy Commissioner [6]. However, despite the largely voluntary nature of reporting, examples exist that demonstrate that some organisations and agencies, irrespective of the lack of compulsion to do so, actively take responsibility for data breaches and act accordingly by notifying those affected. [13]. However, because it is discretionary, this does not always occur.

For localities that do not have mechanisms that compel data breach notifications such as Australia (at present), this results in difficulty in obtaining accurate data on the extent of data breaches. Symantec estimates that the cost of data breaches in Australia at \$2.16 million in 2011 [13]. Nonetheless, examples of significant data breaches are still reported to the Privacy Commissioner, are from companies such as Sony [15] and Lego [16]. Other notable data breaches relate to Telstra [17] and Vodafone [18]. Likewise, significant instances of data breaches are also evident in other countries [19]. An advantage of having mandatory notification is that it may highlight a hidden societal problem [20].

Romansky, Telang and Acquisti suggest that while a person has a right to know of a data breach involving their personal information, another driver for compelling such notification is information dissemination more broadly to increase communal knowledge of the occurrence [7]. Such dissemination of information means that the practices undertaken by organisations and agencies relating to the management of information may become more transparent [21], meaning that individuals are better aware of where the greater and lesser risks arise.

Anecdotally, in Australia there is mixed support for the introduction of mandatory breach notification. In 2012, a

representative sample of 700 Australians who were surveyed by eBay found that 80% of respondents supported the introduction of laws requiring notification of breaches in Australia [22]. Interestingly, many of those surveyed were most concerned about identity theft and the loss of financial data resulting from data breaches, and it was these considerations that drove their support [22]. Therefore a driver for regulatory change is the very real threat of identity crime [22]. This sentiment is similarly reflected other jurisdictions [23].

According to the Australian Privacy Breach Notification Discussion paper, earlier recommendations by the Australian Law Reform Commission (ALRC) in relation to mandatory breach notification were subject to criticism [1]. However, it was clear that some response to dealing with data breaches through the privacy regulatory responses available was still needed. The Office of the Australian Information Commissioner introduced a guide to handling security breaches as a measure to mitigate the impacts of data breaches [1], providing a guide to practical steps to handle data breaches, among other things [11]. However, a limitation of this is that it does not compel any notification in respect of a breach or prescribe penalties [1]. Nonetheless, the guide is helpful in assisting organisations and agencies with data breaches until more formalised rules and regulations take effect in Australia [1].

An important driver for the introduction of laws around mandatory data breach notification is that this could serve as a deterrent to overcome poor information management practices [1]. This is based on the consequences that flow to the organisation or agency that does not deal with personal identification information in an appropriate manner [1]. According to the Australian Privacy Breach Notification Discussion paper, there is merit in the identification of bodies that do not take appropriate steps in responding to data breaches [1]. In addition, a side benefit, is that the broader community confidence in the approaches that are taken to manage information [1]. These are powerful motivators to having such laws introduced in Australia.

According to the Australian Privacy Breach Notification Discussion paper, mandatory data breach notification could serve as a deterrent to overcome poor information management practices [1]. This is based on the consequences that flow to the organisations or agencies that do not deal with personal identification information in an appropriate manner [1]. There is merit in the identification of these bodies and a side benefit is that the broader community has greater confidence in the approaches that are taken to manage information [1]. These are powerful motivators to having such laws introduced in Australia.

Laws relating to mandatory notification of data breaches have been implemented in a number of countries including, the United States (mentioned above), Germany, Norway and Japan [23]. In the United States for instance, such approaches to dealing with data breaches go historically as far back as

2003 in California [24]. There are lessons to be learnt from those who have developed similar laws in the past, such as moderating the number of warnings to avoid fatigue [1]. Despite the obvious improvement to policy and practice that relates to the overall improvement to privacy that such a regulatory change makes, there are others that relate to the relationship between privacy and other crimes.

#### V. THE LINK BETWEEN DATA BREACHES AND IDENTITY CRIME

Romanosky, Telang and Acquisti suggest that the link between identity theft and data breaches is tenuous due to the lack of data available to conclusively support this relationship [7], and that further, the data around identity crime is questionable. Needles also suggests that the relationship is not significant due to the lack of data available to support such a link [25]. However, Cate, Abrams, Bruening and Swindle aver that the nexus between data breaches and identity theft is under stated because the true extent of identity crime is not known [26].

However, Romanosky, Telang and Acquisti state that up over 30% of identity thefts are caused by data breaches by corporations [7], and Burdon notes that an important link exists between data breach notification and the mitigation of identity theft [27]. Likewise, Regan highlights that mandatory breach notifications can positively reduce identity crime through increasing awareness [28]. Therefore despite the difficulties in drawing direct linkages between data breaches and identity crime, there is a relationship [29].

The ALRC notes that in the United States, a key rationale for the introduction of mandatory breach notification laws was around mitigating the potential for identity theft [30]. Accordingly, the ALRC suggests that in Australia, without regulatory oversight of data breaches and the appropriate notifications stemming from these, the risks associated with identity theft will only increase [30]. Therefore, the ALRC argues that through regulating the reporting of data breaches it may be possible to mitigate the damage arising from identity crime [30]. Consequently, there is more work that is needed to explore the relationship between these variables.

#### VI. HOW MIGHT THE REGULATORY RESPONSE LOOK?

In Australia, the approach proposed to mandate the reporting of data breaches is based on the privacy frameworks and related technologies [31]. Australian governmental agencies, as well as private sector organisations [32], are guided by principles outlining how information can be used, disclosed and stored [33]. This is different from the approach in the United States, which emphasises specific uses of personal information such as health information, [34] and that of driver's licenses [35]. However, there is often many forms of personal identification information that can become susceptible through data breaches. The principles in the United States are not founded on privacy principles in the same way as the Australian approach, and rather represent disparate approaches driven by state specific regulatory needs than an

overarching approach, which means the approach in Australia is likely to be different to the United States.

#### VII. LESSONS LEARNED FROM THE US: WHAT SHOULD BE REPORTED?

The response to the question of what should be reported is dependent on the stringency of response applied to the reporting requirement. A broader policy question that needs consideration is what breaches should be reported? This has been referred to as the 'trigger' for the notification of a breach in parts of the United States [36]. Reporting data breaches has a cost associated with it, and the more stringent the reporting requirement then the more costly it becomes [1]. However, not adequately reporting a breach renders the reporting process unworkable, and any remedial responses arising from the breach unattainable. Therefore, there is a delicate balance in the reporting process in terms of identifying the incidence of data breach that should be reported and in this respect, the response needs to be substantive enough to make it worthwhile. In the United States, for instance, a negative consequence has been observed through the overuse of notification mechanisms which can result in complacency due to fatigue [1]. It is hoped that this is will not be the outcome of regulatory reform in Australia.

The ALRC suggested models for data breach notification in Australia which were largely based on the United States approach [6]. Jurisdictions in the United States tend to have stringent triggers for reporting data breaches but tend to vary between States; For instance, Indiana requires a database owner who knows or should know that the data has been breached to report such incidence [37]. This places a responsibility on the organisation concerned to report instances where there might be a suspicion of data loss. This may be a reasonable approach for Australia however there are diverging views about what information should qualify for mandatory breach notification; and the organisation or agency involved may not be in the best position to make determinations as to what should be reported. Therefore deferring such responsibility to another authority such as the Privacy Commissioner may be preferable [1]. Ideally data that is likely to have an adverse effect on the individual is the data that should be reported and this can be construed broadly [1].

Key to the effectiveness of any such notification of breach will be the speed in which such notification take place, so as to mitigate any possible consequences flowing from that breach [1]. Further the way in which this communication takes place will invariably impact on the speed of such a response [1]. In the United States, in California, the requirement is the most expedient manner to avoid unreasonable delay [36]. What unreasonable delay is, and how it might be applied in an Australian context, is not yet clear. Regardless, any notification of breach must be timely to be effective particularly given the speed in which misuse of data can take place [32].

## VIII. PROPOSALS FOR CHANGE IN AUSTRALIA

A Federal approach to mandatory data breach notification could provide uniformity in respect of the approach taken and potentially avoid issues arising through a mixture of responses based on State laws or similar [28]. Similar to the United States this may overcome the issue of variability in State based approaches to mandatory breach notification and inconsistencies [37]. Another advantage of a Federally regulated approach is that it would provide consistent remedies for the victims of such data breaches [37]. This is the proposed approach to be adopted within Australia.

The ALRC has suggested that market based incentives remain an important tool for improving information security measures [30]. The threat to reputation is a market driven force that is important in mitigating data breaches [38]. Arising from this threat, the damage to reputation for such bodies can be extensive [27]. The ALRC recognise reputational damage as an incentive for organisations to improve information security but ultimately they also take the view that this alone was not an adequate measure and needed to be accompanied by a regulatory response prompting action [6]. Nonetheless, it is important to acknowledge the role that is played by these other factors in mitigating the effect of data breaches.

There has been debate around the sanctions that should apply to organisations or agencies that fail to notify of a data breach [1]. Therefore, if the penalties are civil and monetary then what should these be in terms of a sanction amounts? If these are non-monetary, then how should this be framed? The United Kingdom, for instance, applies a fixed penalty of a thousand pounds to data breaches [39]. Alternative options to civil penalties include administrative penalties, in addition to naming organisations and agencies that do not report data breaches [1]. This has implications for reputation which have been identified above. Perhaps an appropriate penalty involves a mixture of these options. The governmental approach to these remains unclear in Australia at present and these are matters that need to be actively debated.

An important part of mitigating data loss is to encourage organisations and agencies to engage with better data management practices, including acknowledging the steps that have been taken by organisations and agencies to mitigate risk attached to potential breaches. This might include for instance, what emphasis is placed on encryption or similar steps to mitigate data breaches, which is recognised in other jurisdictions [40]. The ALRC considered this important for reducing liability in instances of data breaches [6]. The implementation of preventative measures needs to be recognised as a deterrent to data breaches, but the extent of this needs to consistently.

In Australia, those against mandatory data breach reporting argue that such reporting can impose unreasonable financial burdens on organisations [41]. The cost stems from the cost in

making contact with the person whose data has been breached [7]. This is reflected in Australia, at present by the voluntary reporting requirements/expectations under the Office of the Australian Information Commissioner [1]. However, at present, there is little incentive for organisations and agencies to comply with reporting of data breaches [42], and the ALRC similarly asserts that this poor market incentives result in low levels of reporting [43]. If the status quo in dealing with data breaches was working effectively it would be unlikely that such debate would be occurring regarding the need for mandatory notification of breach laws in Australia nor elsewhere.

In Australia, the regulatory change is set to commence early in 2014. The new regulatory requirements will oblige organisations to provide notifications where the data breach will result in harm that is ‘serious’ [44], including injury to feelings, reputation, financial or economic harm [45]. This requirement provides, among other things, for the entity concerned to as soon as practicable notify the Commissioner and each individual significantly affected by the data breach [46]. The regulatory change modifies the *Privacy Act 1988* (Cth) by establishing mandatory notification through the changes proposed in the Privacy Amendment (Privacy Alerts) Bill 2013 [47]. This amendment provides the right for the Privacy Commissioner to take enforcement action, investigate complaints as well as obtain undertakings from organisations about compliance. Similarly civil penalties will also be available under this regime [47].

The trend to recognise legislative requirements for the notification of data breaches has certainly been a factor in introduction of such rules into Australia [45]. In particular, in this context, strong reference is made to the United States that has adopted some regulatory approach to dealing with data breaches. Further, reference has also been made to the European Union which similarly requires telecommunication and internet service providers to disclose certain data breaches to national authorities [48]. Importantly, within this jurisdiction, a further draft data protection regulation document broadens these obligations [49].

A concern expressed by the ALRC was that they wish to reduce the burden of compliance [1], a sentiment that is similarly reflected in other jurisdictions and certainly identified as an area of concern in the European Union [1]. Thereby care has been taken to identify breaches as ‘serious data breaches’ for the purposes of the legislation as the trigger upon which action must be taken [47]. What is interesting about the developments in the regulatory responses to data breach disclosure is that increasingly there is an awareness of the need for an appropriate regulatory response, and the government is tentatively approaching this. It will be interesting to observe the response.

## IX. SIGNIFICANCE OF THE STUDY

This paper brings together existing literature on the relationship between identity crime and mandatory breach notification laws. Given the increased prevalence of both data breaches and of identity crime it is important to acknowledge the existence of the relationship between these variables. Further, where laws are introduced to deal with mandatory breach disclosure, as they are at present in Australia, it is vital to consider the implications such laws will have on the reduction of identity crime. This will only be measurable post-implementation, and can form the basis of future discussion.

## X. CONCLUSION

Both the literature and issues currently being experienced in practice suggests that there is a need to be able to mitigate data breaches, which will in turn assist in the prevention of identity crime. It is not clear whether regulating the notification of data breaches is going to have discernible impact on identity crime, and only time will reveal the true extent of this. However, what is clear from this conceptual research is that there is a relationship between data breaches and identity crime that means that a reduction in one (data breaches) are likely to result in a reduction in the other. Hence, it is reasonable to suggest that the introduction of mandatory breach notification laws in Australia will have a direct impact on the incidence of identity crime in that country.

## ACKNOWLEDGMENT

We would like to acknowledge the support of Faculty of Business at Federation University Australia and the support of the Law Faculty at Bond University.

## REFERENCES

- [1] Australia. Australian Government, Discussion Paper: Australian Privacy Breach Notification. Barton: Attorney-General's Department; 2012. [Online]. Available: <http://www.ag.gov.au/Consultations/Documents/AustralianPrivacyBreachNotification/AustralianPrivacyBreachNotificationDiscussionPaper.doc>. [Accessed: 17 Jan 2013].
- [2] Australia. Australian Government, Media Release: Business warned to be ready for data breaches. Sydney: Office of the Australian Privacy Commissioner; 2012. [Online]. Available: <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/business-warned-to-be-ready-for-data-breaches> [Accessed: 5 Nov 2012].
- [3] L. C. Rode, "Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?", *Houston Law Review*, vol. 43, no. 5, pp. 1597-1621, Spring 2007.
- [4] S. Romanosky, and A. Acquisti, "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives," *Berkeley Technology Law Journal*, vol. 24, no.3, pp. 1072-1074, December 2009.
- [5] Canadian Internet Policy and Public Interest Clinic. "Approaches to Security Breach Notification: A White Paper," <https://www.cippic.ca/>. [Online]. Available: [https://www.cippic.ca/sites/default/files/BreachNotification\\_9jan07-print.pdf](https://www.cippic.ca/sites/default/files/BreachNotification_9jan07-print.pdf). [Accessed: Nov. 5, 2012].
- [6] Australia. Australian Government, For your Information: Australian Privacy Law and Practice (ALRC Report 108) - Data Breach Notification. Sydney: Australian Law Reform Commission; 2008. [Online]. Available: <http://www.alrc.gov.au/publications/51.%20Data%20Breach%20Notification/rationale-data-breach-notification>. [Accessed: 5 Nov 2012].
- [7] S. Romanosky, R. Telang, and A. Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?", *Journal of Policy Analysis and Management*, vol. 30, No.2, pp 256-286, March 2011.
- [8] M. Turner (2006, Jun. 21). "Towards a Rational Personal Data Breach Notification Regime," Information Policy Institute [Online]. Available: [http://www.perc.net/wp-content/uploads/2013/09/data\\_breach.pdf](http://www.perc.net/wp-content/uploads/2013/09/data_breach.pdf). [Accessed: Jan. 17, 2013].
- [9] Symantec. "Threat Activity Trends – Data Breaches that Could Lead to Identity Theft," [www.symantec.com](http://www.symantec.com). [Online]. Available: [http://www.symantec.com/threatreport/topic.jsp?aid=data\\_breaches\\_that\\_could\\_lead&id=threat\\_activity\\_trends](http://www.symantec.com/threatreport/topic.jsp?aid=data_breaches_that_could_lead&id=threat_activity_trends). [Accessed: Jan. 17, 2013].
- [10] Privacy Amendment (Privacy Alerts) Bill 2013.
- [11] Australia. Australian Government, National Privacy Principles. Sydney: Office of the Australian Information Commissioner; 2001. [Online]. Available: <http://www.privacy.gov.au/materials/types/download/8774/6582>. [Accessed: 17 Jan 2013].
- [12] Criminal Code 1899 (Qld) s 408D(1).
- [13] Symantec. "2011 Cost of Data Breach Study: Australia," [www.symantec.com](http://www.symantec.com). [Online]. Available: [http://www.symantec.com/content/en/us/about/media/pdfs/b-pomon-2011-cost-of-data-breach-australia-us.pdf?om\\_ext\\_cid=biz\\_socmed\\_twitter\\_facebook\\_marketwire\\_linkedin\\_2012Mar\\_worldwide\\_CODB\\_Australia](http://www.symantec.com/content/en/us/about/media/pdfs/b-pomon-2011-cost-of-data-breach-australia-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide_CODB_Australia). [Accessed: Jan. 17, 2013].
- [14] Identitytheft.info. "Identity Theft Victim Statistics," <http://www.identitytheft.info/>. [Online]. Available: <http://www.identitytheft.info/victims.aspx>. [Accessed: Feb. 6, 2014].
- [15] I. Paul, (2011, Apr. 29). "Sony Hackers Claim to Have Credit Cards," PC World, [Online]. Available: [http://www.pcworld.com/article/226692/sony\\_hackers\\_claim\\_to\\_have\\_credit\\_cards.html](http://www.pcworld.com/article/226692/sony_hackers_claim_to_have_credit_cards.html). [Accessed: Jan. 17, 2013].
- [16] NBCNews. "Data Breach Toppled Australian Lego Fans," NBCNEWS.com. [Online]. Available: [http://www.msnbc.msn.com/id/4762171/ns/technology\\_and\\_science-security/#.T81Lt8U0K1c](http://www.msnbc.msn.com/id/4762171/ns/technology_and_science-security/#.T81Lt8U0K1c). [Accessed: Jan. 17, 2013].
- [17] L. Battersby, "Telstra Red-Faced after Email Error," *Sydney Morning Herald*, p. 7, Dec 7, 2010.
- [18] A. Langmaid (2011, Jan. 9). "Vodafone Mobile Records Leaked onto the Internet," *Herald Sun* [Online]. Available: <http://www.heraldsun.com.au/news/victoria/vodafone-mobile-records-leaked-onto-the-internet/story-e6frf7l6-1225984469970>. [Accessed: Jan. 17, 2013].
- [19] IT Security Training. "IT Security Training Australia: Data Breach Notification in Australia," IT Security Training. [Online]. Available: <http://www.itsecuritytraining.com.au/content/data-breach-notification-australia-whitepaper-available> [Accessed: Jan.17, 2013].
- [20] F.J. Garcia, "Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time" *Fordham Intellectual Property, Media and Entertainment Law Journal*, Vol. 17, no. 3, pp 693-727, March 2007.
- [21] P. M. Schwartz, and E. J. Janger, "E. Notification of data security breaches" *Michigan Law Review*, Vol. 105, no. 5, pp.913-984, March 2007.
- [22] A. MacGibbon and N. Phair, (2012, Apr). "Privacy and the Internet: Australian Attitudes Towards Privacy in the Online Environment". Centre for Internet Safety [Online]. Available: <http://www.canberra.edu.au/cis/storage/Australian%20Attitudes%20Towards%20Privacy%20Online.pdf>. [Accessed: Jan. 17, 2013].
- [23] A. Moses, (2011, Jul. 27). "Thousands of Privacy Breaches Going Unreported". The Age [Online]. Available: <http://www.theage.com.au/technology/technology-news/thousands-of-privacy-breaches-going-unreported-20110727-1hzes.html>. [Accessed: Jan. 17, 2013].
- [24] California Civil Code § 1729.98(a) 2003.
- [25] S.A. Needles, "The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law" *North Carolina Law Review*, vol. 88, no. 1, pp. 267-272, December 2009.
- [26] F. Cate, M. Abrams, P. Bruening and O. Swindle, (2009, Mar. 16). "Dos and Don'ts of Data Breach and Information Security Policy". [www.huntonfiles.com](http://www.huntonfiles.com), [Online]. Available: [http://www.huntonfiles.com/files/webupload/CIPL\\_Dos\\_and\\_Donts\\_White\\_Paper.pdf](http://www.huntonfiles.com/files/webupload/CIPL_Dos_and_Donts_White_Paper.pdf). [Accessed: Jan. 17, 2004].

- [27] M. Burdon, The Conceptual and Operational Compatibility of Data Breach Notification and Information Privacy Laws. Ph.D. dissertation Faculty of Law., Queensland University of Technology., Brisbane, 2011.
- [28] P. M. Regan, "Federal Security Breach Notifications: Politics and Approaches," *Berkeley Technology Law Journal*, Vol. 24, no. 3, pp. 1103-1126, June 2009.
- [29] J. K. Winn, "Are Better Security Breach Notification Laws Possible?," *Berkeley Technology Law Journal*, Vol. 24, no.3, pp. 1133-1166, June 2009.
- [30] Australia. Australian Government, Review of Australian Privacy Law. Sydney: Australian Law Reform Commission: 2007 [Online]. Available: <http://www.austlii.edu.au/au/other/alrc/publications/dp/72/DP72.pdf>. [Accessed: 19 Jan 2013].
- [31] Privacy Act, 1988 (Cth). Parliament of Australia.
- [32] Australia. Australian Government, Inquiry into Cyber Crime and its Impact on Australian Consumers. Sydney: Office of the Australian Information Commissioner; 2009. [Online]. Available: [http://www.oaic.gov.au/images/documents/migrated/2009-08-05053022/HoR\\_Comms\\_Cte\\_Cyber\\_Crime.pdf](http://www.oaic.gov.au/images/documents/migrated/2009-08-05053022/HoR_Comms_Cte_Cyber_Crime.pdf). [Accessed: 18 Jan 2013].
- [33] A. Langmaid, (2011, Jan. 9). "Vodafone Mobile Records Leaked onto the Internet". Herald Sun [Online]. Available: <http://www.heraldsun.com.au/news/victoria/vodafone-mobile-records-leaked-onto-the-internet/story-e6ffr7l6-1225984469970>. [Accessed: Jan. 17, 2013].
- [34] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191. United States of America.
- [35] Drivers Privacy Protection Act of 1994, 18 U.S.C.x 2721. United States of America.
- [36] California Civil Code § 1798.29 (a) of 2003, [37] Indiana Code, § 24-4.9-3-1(1)(a) United States of America.
- [37] B. Faulkner, "Hacking into Data Breach Notification Laws" *Florida Law Review*, vol. 59, no.5. pp. 1097-1108, March 2007.
- [38] T.M. Lenard and P.H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches" *Emory Law and Economics Research Paper*, No. 05-12. [Online]. Available: <http://dx.doi.org/10.2139/ssrn.765845>. [Accessed: 18 January 2013].
- [39] Privacy and Electronic Communications (EC Directive) (Amendment) Regulations, 2011 United Kingdom.
- [40] Directive on privacy and electronic communications (Directive 2002/58/EC).
- [41] T.M. Lenard and P.H. Rubin, "Much Ado about Notification" *Regulation*, vol. 29, no. 1. pp.44-50, April 2006.
- [42] B. G. Arnold, "Losing It: corporate Reporting on Data Theft" *Privacy Law Bulletin*, vol. 3, No. 8. pp. 101-102, March, 2007.
- [43] M. Turner, Towards a Rational Personal Data Breach Notification Regime. PERC Information Policy Institute; Emory Law and Economics Research Paper No. 05-12. [Online]. Available: [http://perc.net/files/downloads/data\\_breach.pdf](http://perc.net/files/downloads/data_breach.pdf). [Accessed: 18 January 2013].
- [44] Australia. Australian Government, Australias better protected with mandatory breach notification. Sydney: Office of the Australian Information Commissioner; 2013. [Online]. Available: <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australians-better-protected-with-mandatory-data-breach-notification>. [Accessed: 18 Jan 2013].
- [45] Mondaq. "Australia: Mandatory data breach reporting bill introduced into parliament," www.mondaq.com. [Online]. Available: <http://www.mondaq.com/australia/x/247692/data+protection/Mandatory+Data+Breach+Reporting+Bill+Introduced+Into+Parliament>. [Accessed: Jan. 18, 2013].
- [46] Privacy Amendment (Privacy Alerts) Bill, 2013, Div. 2 s 6 ZB (f)(g). Canberra: Parliament of Australia.
- [47] Privacy Amendment (Privacy Alerts) Bill, 2013, Explanatory Memorandum. Canberra: Parliament of Australia.
- [48] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC; Directive 2002/58/EC (EC) No 2006/2004. [Accessed: 18 Jan 2013].
- [49] European Commission. "Proposal of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement (General Data Protection Regulation)," www.ec.europa.eu. [Online]. Available: [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf). [Accessed: Jan. 18, 2013].