ENCRYPTION SAFE HARBOURS AND DATA BREACH NOTIFICATION LAWS

Mark Burdon [a], Jason Reid [a] and Rouhshi Low [a]

ABSTRACT

Data breach notification laws require organizations to notify affected persons or regulatory authorities when an unauthorized acquisition of personal data occurs. Most laws provide a safe harbour to this obligation if acquired data has been encrypted. There are three types of safe harbour: an exemption; a rebuttable presumption and factor-based analysis. We demonstrate, using three condition-based scenarios, that the broad formulation of most encryption safe harbours are based on the flawed assumption that encryption is *the* silver bullet for personal information protection. We then contend that reliance upon an encryption safe harbour should be dependent upon a rigorous and competent risk-based review that is required on a case-by-case basis. Finally, we recommend the use of both an encryption safe harbour and a notification trigger as our optimal choice for a data breach notification regulatory framework.

[a] Queensland University of Technology, Australia.

Keywords: Data breach notification; encryption; information security management; data protection.

1 INTRODUCTION

The conceptual justification for mandatory data breach notification laws is relatively straightforward. An organisation that has suffered a data breach that exposes personal information must notify those persons whose information may have been acquired so they can take action to mitigate potential harms, predominantly arising from identity theft threats. A general safe harbour to notification exists in most data breach notification laws that relates to encryption.[1] Put simply, an organisation that has suffered a data breach involving encrypted personal information does not have to notify those persons who may have been affected by the breach. The general purpose of the safe harbour is twofold. First, to reduce the risks of notification fatigue[2] and the regulatory compliance burden on organisations and regulators, by requiring notification only in circumstances where there is

[1] It should also be noted that other common and broad safe harbours exist particularly in relation to 'good faith' use by employees and to acquired information that is already in the public domain.

[2] Notification fatigue refers to the negative impact of over-notification upon individuals and potentially the overall impact of data breach notification laws. See e.g. A Cavoukian, *A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight* (2009) <http://www.ipc.on.ca/images/Resources/privacy_externalities.pdf> at 19 March 2010, 9 and P M Schwartz and E J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913, 916.

a risk of identity theft related crimes.[3] Second, to encourage both private and public sector organisations to adopt encryption technologies for the collection and storage of personal information thus strengthening their information security management practices.[4] Data breach notification laws have been successful at revealing serious and innumerable instances of ineffective management regarding the security of personal information, but these apparently simple laws have produced outcomes that are conceptually complex, from regulatory, market oriented and legal perspectives.[5] Encryption safe harbours are a case in point.

Three types of encryption safe harbour have been identified.[6] They are: exemptions; rebuttable presumptions and factor-based analysis. However, whilst the issue of different notification triggers has been dealt with extensively in the data breach notification literature,[7] encryption safe harbours have not.[8] This is surprising because both safe harbours and notification triggers play integral roles in the operation of data breach notification laws.

---

[3] See e.g. California Office of Privacy Protection, 'Recommended Practices on Notice of Security Breach Involving Personal Information' (California Office of Privacy Protection, 2008).

[4] See e.g. L Rode, 'Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?' (2007) 43(5) *Houston Law Review* 1597:1628; M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555, 573; K E Picanso, 'Protecting Information Security Under a Uniform Data Breach Notification Law' (2006) 75(1) *Fordham Law Review* 355, 384.

[5] See e.g. F H Cate, *Information Security Breaches: Looking Back and Thinking Ahead* (2008) <http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf> at 19 March 2010; 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; P M Schwartz and E J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913; B St. Amant, 'Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches' (2007) 44 *Harvard Journal on Legislation* 505.

[6] M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555.

[7] See generally P M Schwartz and E J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913; B St. Amant, 'Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches' (2007) 44 *Harvard Journal on Legislation* 505; S a Needles, 'The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law' (2009) 88 *North Carolina Law Review* 267; T J Smedinghoff, *The State of Information Security Law: A Focus on the Key Legal Trends* (2009) S Lee, 'Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs' (2006) 1(1) *Entrepreneurial Business Law Journal* 125; K E Picanso, 'Protecting Information Security Under a Uniform Data Breach Notification Law' (2006) 75(1) *Fordham Law Review* 355; L Rode, 'Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?' (2007) 43(5) *Houston Law Review* 1597.

[8] Those articles that have covered the issue in most depth are M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555 T H Skinner, 'California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation' (2003) 10(1) *Richmond Journal of Law & Technology* ; J Winn, 'Are 'Better' Security Breach Notification Laws Possible?' (2009) *Berkeley Technology Law Journal, Vol. 24, 2009* .

Triggers indicate the situations where notification is required. A higher or lower trigger will have a significant impact on the types, and thus numbers, of data breaches to be notified. Encryption safe harbours operate to exclude a range of breach scenarios from notification. The operation of triggers and safe harbours are therefore important because they define the compliance requirements for data breach notification.

We conduct a critique of the three types of encryption safe harbours using a scenario-based analysis. This is based on a conditional claim for the adoption of an encryption safe harbour, namely, that personal information acquired without authorisation exists in encrypted form. We address this conditional claim by adducing three categories of encryption use based on the requirements of effective encryption and information security management, namely that encryption is: (1) likely to be effective (2) might be effective or (3) ineffective as it can be bypassed. We then demonstrate that an effective safe harbour is dependent on the rigour of risk-based review that is required on a case-by-case basis and the degree of effort with which a safe harbour can be claimed. Finally, we conclude by recommending our preferred encryption safe harbour, factor-based analysis in conjunction with our preferred choice of notification trigger, a two-tier trigger. This type of notification trigger has two forms of notification requirement. The first relies on a broad acquisition-based trigger that requires notification by a breached entity to relevant regulatory authorities where there has or believed to have been an unauthorised acquisition of personal data. The second is based on a narrower risk-based trigger that requires notification by the breached entity to individuals where a reasonable risk of harm materialises. The use of a two-tier trigger therefore attempts to ensure that regulators are notified of all data breaches promptly and individuals are notified only if a risk-based assessment determines a risk.

2 ENCRYPTION, CRYPTOGRAPHY AND INFORMATION SECURITY

Before we embark on our critique of encryption safe harbours, it is important to provide an overview of encryption from a technical perspective and the related field of cryptography as a foundation for examining how these concepts have been applied in data breach notification laws and legislative proposals.

Mao defines encryption as "a process to transform a piece of information into an incomprehensible form... The input to the transformation is called *plaintext* and the output is called *ciphertext*. The reverse process of turning ciphertext into plaintext is called

decryption."[9] Together, the encryption and decryption transformations are known as *cryptographic algorithms* or *ciphers*. They are controlled by a cryptographic key or keys, which are typically long random numbers.[10] A cipher is said to be *breakable* (and therefore insecure) if the plaintext can be recovered from the ciphertext without knowledge of the decryption key within a specified period of time.[11] It is a fundamental principle of cryptography that the encryption and decryption algorithms may be publicly known without weakening the security of the cipher, which rests solely in the secrecy of the decryption key.[12] There are two related reasons for this: firstly, if a supposedly secret algorithm becomes known, the entire system must be replaced with a new cipher. This is considerably less convenient than simply changing a key. Secondly, experience has repeatedly shown that keeping an algorithm secret over any reasonable length of time is extremely difficult.[13]

The apparent benefit of cryptography is that it substitutes the problem of protecting the secrecy of a potentially large amount of plaintext, for the problem of protecting the secrecy a much smaller key. Based on the critical assumption that the decryption key is only available to people authorised to access the plaintext, the ciphertext requires no further protection and can transmitted over insecure communication channels such as the Internet or stored on electronic devices that are routinely lost or stolen such as laptop computers and USB drives. Since knowledge of a ciphertext and the corresponding decryption key is equivalent to knowledge of the plaintext, the controlled distribution of keys is the principal challenge in using cryptography. In practice it has proven to be very difficult. Indeed, successful attacks

[9] W Mao, *Modern Cryptography: Theory and Practice* (2004), 24.

[10] S*ymmetric* cryptographic algorithms such as DES and AES use the same key for encryption and decryption. Asymmetric algorithms such as RSA use a different key for encryption and decryption.

[11] See A J Menezes, P C Van Oorschot and S a Vanstone, *Handbook of Applied Cryptography,* CRC Press series on discrete mathematics and its applications. (1997), 14. All ciphers can be broken given sufficient time and computational resources by systematically trying all possible keys. If the number of keys is sufficiently large, a so called *exhaustive search* of the keyspace is infeasible because it exceeds the minimum specified time for which the cipher must remain secure. The goal of cipher design is therefore to ensure that the fastest way to break the algorithm is exhaustive search.

[12] A system that relies on the secrecy of an algorithm for its security violates Kerckhoff's principle which states that no inconvenience should occur if the system falls into the hands of an adversary, because all security should reside in the secrecy of the keys. See A Kerckhoffs, 'La Cryptographie Militaire' (1883) *Journal des Sciences Militaires* 5.

[13] Secret algorithms such as COMP128 and A5 used in the early days of GSM mobile telephony were subsequently reverse engineered, and significant weaknesses were identified. They are now considered broken. See E Barkan, E Biham and N Keller, 'Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication' (2008) 21(3) *Journal of Cryptology* 392.

on key management systems and procedures are far more common than those that exploit weaknesses in the cryptographic algorithms themselves.[14]

One of the reasons why key management is hard is that cryptographic keys for secure algorithms are too long for humans to remember so they must be recorded somewhere.[15] However, for convenience of access the decryption key must be available on demand, but only to those authorised to see the plaintext. This is actually a problem of authentication and access control.[16] Ensuring selective and controlled access to the decryption key presents a vexing problem. Take for example a laptop computer that stores a file containing encrypted personal information. The authorised user should be able to easily access the information so the decryption key will need to be available to the laptop to recover the plaintext. However, an attacker that gains access to the laptop should not be able to decrypt the file. A fundamental but common key management mistake is to store the decryption key on the same device as the ciphertext with inadequate protection. In the worst case, the decryption key may simply be stored in another file on the laptop. This offers very little additional protection compared to not encrypting the data at all.[17] A more common approach is to encrypt the decryption key itself under a different *memorable* key known as a passphrase or password. Thus, encryption and passwords are often used together. Unfortunately, in practice, the security of their combination does not exceed the security offered by the password: if it is easy to guess, the fact that the personal information is encrypted using a secure algorithm with a random key of adequate length is immaterial.[18] Experience has shown that without very specific guidance and enforced selection constraints, people choose

[14] See R J Anderson, 'Why Cryptosystems Fail' (1994) 37(11) *Communications of the ACM* 32.
[15] For example, a common key length used with the widely accepted AES algorithm is 128 bits (bits are zeros and ones). When encoded as a decimal number, a 128 bit key requires up to 39 digits.
[16] See e.g. R J Anderson, 'Why Cryptosystems Fail' (1994) 37(11) *Communications of the ACM* 32. Passwords are the most widely used authentication mechanism but they have significant and well documented shortcomings.
[17] Access to the laptop's filesystem is controlled at first instance by password authentication enforced by the operating system at log on. However, this can be easily bypassed by removing the laptop's hard disk and accessing it using another operating system. Removal is not necessary if the laptop is configured to boot from the optical drive or USB port.
[18] See e.g. Narayanan, A. and Shmatikov, V. Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff. In *Proceedings of the 12th ACM Conference on Computer and Communications Security CCS '05,* Alexandria, VA, USA, November 07 - 11, 2005, 364-372. The authors report a password guessing algorithm that successfully guessed 67% of passwords from a real database of 150 user selected passwords.

passwords that are easy for password guessing programs to guess.[19] Passwords are also increasingly susceptible to key-logging malware and so-called *phishing* attacks.[20]

The best approach for protecting decryption keys is to store them on a dedicated key management device, separate to the device that stores the ciphertext. Financial institutions, the pioneers of the civilian use of cryptography, stored cryptographic keys in hardware-based security modules, mainly to ensure that programmers and system developers could not access them.[21] As cryptography came to be more widely used by business and government organisations, particularly by end-users, smart cards were promoted as a secure place to store cryptographic keys. However, they have proved to be expensive to deploy and maintain and have not been widely adopted. Notwithstanding the cost and inconvenience, separate storage of cryptographic keys on dedicated hardware devices represents best practice.[22]

These are important practical considerations given the proliferation of data breach notification laws throughout the world.[23] Both qualitative[24] and quantitative evidence suggests that the effect of encryption safe harbours has been an increased uptake of encryption technologies. The Ponemon Institute in 2009 surveyed 997 US-based managers and executives with information technology responsibilities. The survey found that 67% of respondents stated that their organisation primarily used encryption technologies to mitigate against data breaches.[25] This figure was a small decrease from the 71% of respondents who were asked the same question in 2008 and an increase from the 66% who replied in 2007.[26] Furthermore, 64% of respondents stated that they had adopted encryption

[19] See J Yan, A Blackwell and R Anderson, 'Password Memorability and Security: Empirical Results' (2004) 2(5) *IEEE Security & Privacy* 25.
[20] See A Emigh, 'The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond' (2006) 1(3) *Journal of Digital Forensic Practice* 245 for an overview of tools and attack methods.
[21] R J Anderson, 'Why Cryptosystems Fail' (1994) 37(11) *Communications of the ACM* 32.
[22] See National Institute of Standards and Technology, *Publication SP 800-57 Part 1, Recommendation for Key Management - Part 1: General (Revised)* (2007) <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf> at 20 March 2010.
[23] A Maurushat, *Data Breach Notification Law Across the World from California to Australia* (2009) <http://law.bepress.com/unswwps/flrps09/art11/> at 20 March 2010.
[24] Samuelson Law Technology & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers* (2007) <http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf> at 21 March 2010, 17.
[25] Ponemon Institute, 'US Enterprise Encryption Trends' (2009), 11.
[26] Ibid.

to comply with privacy or data security regulations which represented an increase from 58% in 2008 and 51% in 2007.[27]

The contention that data breach notification laws have increased the uptake of encryption technologies is supported by the same Ponemon survey conducted in Australia in 2009. Only 33% of 482 respondents stated that encryption was used to mitigate data breaches. Whereas 15% indicated that encryption was used to comply with privacy or data security regulations but 57% of respondents stated encryption was used to ensure that privacy commitments were honoured.[28] A further 3% of respondents stated that the purpose of using encryption was to avoid notification following a breach. As regards the use of encryption to address data privacy compliance, 79% of respondents used encryption to comply with the Privacy Act 1988 (Cth). The relationship between the uptakes of encryption technologies to mitigate data breaches is much less prominent in Australia than the US which is perhaps not surprising given that Australia does not have a data breach notification law whereas a majority of US states do.[29]

The results of the Ponemon surveys do have to be treated with a degree of caution given the low response rates received which may give rise to concerns about non-response biases and may therefore affect extrapolated results.[30] Winn has also suggested that the uptake of encryption technologies for the purpose of data breach notification is not as great as suggested above which either indicates that encryption safe harbours have provided weak incentives or the cost of implementation is perceived to be greater that the risks arising from not encrypting data.[31]

3 ENCRYPTION SAFE HARBOURS

As a framework for our analysis, we have adopted Jones's classification of encryption safe harbours and notification triggers. In his review of 2007 developments, Jones contends that

---

[27] Ibid.

[28] Ponemon Institute, 'Encryption Trends - Australia' (2009), 8.

[29] However, see also Office of the Privacy Commissioner, 'Portable Storage Devices and Australian Government Agencies Personal Information Survey' (2009), 22 which also suggests that there has been a degree of uptake amongst Australian Government agencies regarding protections for portable storage devices.

[30] For example in, 2009 997 usable responses out of 14,893 surveys (6.7%); 2008 975 usable responses out of 13,448 (7.3%).

[31] J Winn, 'Are 'Better' Security Breach Notification Laws Possible?' (2009) *Berkeley Technology Law Journal, Vol. 24, 2009*, 25. It should be noted however that Winn's article is concerned with the effects of the Californian data breach notification law.

two important issues faced data breach notification legislators: the type of notification trigger and the type of encryption safe harbour to be adopted.[32]

Two types of notification trigger were adduced: acquisition based and risk-based triggers that represent differing approaches to notification. Acquisition based triggers require notification in situations where there has been an actual breach or there is a reasonable belief of an unauthorised acquisition of personal data. Accordingly, notification may be required even when there is no actual evidence of data having been acquired.[33] Jones contends that data breach notification laws based on an acquisition trigger are more consumer oriented because broad notification means that consumers are made aware of potential data breaches and can therefore take action to mitigate potential harms before they arise.[34] However, problems can arise from the use of an acquisition trigger in the form of notification fatigue and because of the underlying reliance upon the causal link between data breaches and identity theft concerns.[35]

Risk-based triggers, on the other hand, set a different standard as these triggers only require notification in situations where a risk assessment determines that a risk of harm exists to consumers. Jones further contends that risk-based triggers are business oriented because they generally require the corporate entity to make a determination whether a risk of harm will or is reasonably likely to arise.[36] Moreover, it should also be noted that different standards exist as to what triggers notification under a risk-based assessment. For example, some laws require a reasonable likelihood that harm may arise[37] where others require a

[32] M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555, 573.
[33] Ibid., 562.
[34] Ibid., 563. See also P M Schwartz and E J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913 regarding the role and purpose of 'pure notification' data breach laws predicated on an acquisition trigger.
[35] This causal link has been a controversial element of data breach notification laws. For a summary of the issue see F H Cate, *Information Security Breaches: Looking Back and Thinking Ahead* (2008) <http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf> at 19 March 2010 and M Burdon, B Lane and P Von Nessen, 'The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments' (2010) 26(2) *Computer Law & Security Review* 115, 126.
[36] M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555 563.
[37] See e.g. ALASKA STAT. § 45.48.010 (Michie 2009); ARK. CODE ANN. § 4-110-105 (Michie 2005); FLA. STAT. § 817.5681 (2005); LA. REV. STAT. ANN. §§ 51:3071 (West 2005).

significant or material real risk of identity theft[38] or a reasonable likelihood of substantial economic loss.[39] Some risk-based triggers therefore operate on higher standards for notification than others.

Our research indicates that a small number of US federal bills and the European Union's (EU) updated e-Privacy Directive[40] also have a trigger that incorporates both elements of an acquisition and risk-based trigger but operate in a broader two-tier regulatory manner.[41] For example, the bill, the Identity Theft Protection Act of 2005 required entities to notify the Federal Trade Commission, or other appropriate regulator, of a data breach affecting the sensitive personal information of 1,000 or more individuals.[42] Notification at this level is therefore based on a restricted acquisition trigger of a certain number of persons who may be affected. Consumer notification was also required for data breaches that cover one or more persons and where there was a basis for concluding that a reasonable risk of identity theft existed.[43] This two-tier form of notification therefore attempts to ensure that regulators are notified of large data breaches promptly upon unauthorised acquisition and consumers are notified only if a risk-based assessment determines a risk.[44] Finally, the new Article 4(3) of the e-Privacy Directive requires notification of a personal data breach to national authorities based on an acquisition trigger and to subscribers and individuals on a risk-

[38] See e.g. KAN. STAT. ANN. §§ 50-7a01 (2006); MD. CODE ANN. §§ 14-3501 (2008); MASS. GEN. LAWS 93H §1 (2007); MICH. COMP. LAWS § 445.72 (2007); OHIO REV. CODE ANN. § 1349.19 (West 2005); R.I. GEN. LAWS § 11-49.2-1 (2005); UTAH CODE ANN. §§ 13-42-101 (2006); WIS. STAT. § 895.507 (2006).

[39] See e.g. ARIZ. REV. STAT. § 44-7501 (2007).

[40] Directive of the European Parliament and of the Council 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.

[41] See also P M Schwartz and E J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913, 933 regarding the two-tier approach of the Interagency Guidelines. These are guidelines developed by a collection of agencies involved in financial regulation that inform financial institutions about how and when to notify a breach. See Office of the Comptroller of the Currency et al, 'Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice' (2005).

[42] S3(a)(1) Identity Theft Protection Act of 2005, S. 1408, 109th Cong. (2005) .

[43] S3(a)(2) Identity Theft Protection Act of 2005, S. 1408, 109th Cong. (2005).

[44] However, it should be noted that the consumer notification provisions were removed in the version of the bill reported to the Senate and regulatory notification was also changed to a risk-based trigger that was subsequently adopted by other bills.

based trigger in situations where the breach is likely to adversely affect their personal data or privacy.[45]

Jones also adduced three types of encryption safe harbour based on an analysis of 10 US federal bills that were introduced in the 110th US Congress. The first type, *exemptions*, provide a general safe harbour meaning notification is not required if personal data has been acquired in encrypted form. For example, the definition of personal information in Californian Civil Code §.1789.29(a), the first and most influential US state-based data breach notification law, states that notification is required if a Californian organisation has suffered or believes it has suffered an unauthorised acquisition of *unencrypted* and computerised personal information.[46] The Californian law therefore does not define encryption.[47] Further guidance has been produced by the Californian Office of Privacy Protection which provides additional information as to what would constitute acceptable encryption in conjunction with other information security practices. It recommends that the National Institute of Standards and Technology's (NIST) Advanced Encryption Standard should be used as the encryption algorithm.[48] However, the guidance is clear that the "recommendations are not regulations and are not binding" so the extent they are adhered to in practice either in California or indeed in states that have adopted the Californian law is open to question.[49]

Our research also indicates that all US state-based encryption safe harbours can be classified as exemptions.[50] However, there are significant differences between state-based laws regarding the construction of encryption exemptions that can be broadly categorised in two

[45] See M Burdon, B Lane and P Von Nessen, 'The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments' (2010) 26(2) *Computer Law & Security Review* 115, 127 and complications related to notification under the amended e-Privacy Directive.

[46] See CAL. CIV. CODE (West 2003)§.1798.29(e) "For purposes of this section, personal information means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted".

[47] T H Skinner, 'California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation' (2003) 10(1) *Richmond Journal of Law & Technology*

[48] California Office of Privacy Protection, 'Recommended Practices on Notice of Security Breach Involving Personal Information' (California Office of Privacy Protection, 2008), 10.

[49] Ibid., 8. See also at page 6, "The recommendations offered here are neither regulations, nor mandates, nor legal opinions. Rather, they are a contribution to the development of "best practices" for businesses and other organizations to follow in managing personal information in ways that promote and protect individual privacy interests."

[50] Only one state, Wyoming, has a data breach notification law with no encryption exemption. Instead, it has a redaction only exemption. See WYO. STAT. ANN. §§ 40-12-501 (Michie 2007). The District of Columbia also has an exemption to notification that has no reference to encryption. The law's notification trigger states that if personal data has been rendered secure so that it is unusable by an unauthorized third party, then notification is not required. See D.C. CODE ANN. § 28-3851 (2007).

ways: (1) non-explicit exemptions, such as the Californian law, which do not attempt to define encryption[51] and (2) explicit exemptions, such as the North Carolina[52] and Ohio[53] laws that do attempt to define encryption.[54] A majority of US states have adopted legislation based on the Californian law and some have directly copied California's notification trigger and its definition of personal information.[55] However, other states have included additional provisions in their definition of personal information that specify situations in which unencrypted personal information could still be exempt from notification because the information is unintelligible.[56] A majority of states with explicit exemptions are based on two statutory elements that set different standards for indicating when data will be encrypted. They are through the use of an algorithmic process to transform data into a form in which: (1) data is rendered unreadable or unusable[57] and (2) there is a low probability of assigning

[51] See also ALASKA STAT. § 45.48.010 (Michie 2009); ARK. CODE ANN. § 4-110-105 (Michie 2005); CAL. CIV. CODE (West 2003); COLO. REV. STAT. § 6-1-716 (2006); CONN. GEN. STAT. § 36a-701b (2006); 6 DEL. CODE ANN. §§ 12B-101 (2005); FLA. STAT. § 817.5681 (2005); GA. CODE ANN. §§ 10-1-911 (2005); IDAHO CODE § 28-51-104 (Michie 2006); 815 ILL. COMP. STAT. 530/1 (2005); LA. REV. STAT. ANN. §§ 51:3071 (West 2005); MINN. STAT. § 325E.61 (2006); MONT. CODE ANN. § 30-14-1704 (2006); NEV. REV. STAT. §§ 603A.010 (2006); N.J. STAT. ANN. § 56:8-163 (West 2006); N.Y. GEN. BUS. LAWS §§ 899-aa (2005); N.D. CENT. CODE §§ 51-30-01 (2005); R.I. GEN. LAWS § 11-49.2-1 (2005); S.C. CODE ANN. § 39-1-90 (Law Co-op 2009); TENN. CODE ANN. § 47-18-2101 (2005); TEX. BUS. & COMM. CODE. §§ 48.001 (2005); UTAH CODE ANN. §§ 13-42-101 (2006); WASH. REV. CODE § 19.255.010 (2005); WIS. STAT. § 895.507 (2006).

[52] N.C. GEN. STAT. §§ 75-60 (2005).

[53] OHIO REV. CODE ANN. § 1349.19 (West 2005).

[54] See also ARIZ. REV. STAT. § 44-7501 (2007); HAW. REV. STAT §§ 487N-1 (2007); IND. CODE §§ 24-4.9-3-1 (2006); IOWA CODE § 715C.1 (2008); KAN. STAT. ANN. §§ 50-7a01 (2006); MD. CODE ANN. §§ 14-3501 (2008); MICH. COMP. LAWS § 445.72 (2007); MO. REV. STAT. § 407.1500 (2009); NEB. REV. STAT. §§ 87-801 (2006); N.H. REV. STAT. ANN. §§ 359-C:19 (2007); OR. REV. STAT. § 646A.600 (2007); 73 PA. CONS. STAT. § 2303 (2006); 9 VT. STAT. ANN. §§ 2430 (2007); VA. CODE ANN. § 18.2-186.6 (Michie 2008); W. VA. CODE §§ 46A-2A-101 (2008).

[55] See e.g. 6 DEL. CODE ANN. §§ 12B-101 (2005); FLA. STAT. § 817.5681 (2005); IDAHO CODE § 28-51-104 (Michie 2006); MONT. CODE ANN. § 30-14-1704 (2006); NEV. REV. STAT. §§ 603A.010 (2006); OKLA. STAT. § 74-3113.1 (2006); R.I. GEN. LAWS § 11-49.2-1 (2005); TENN. CODE ANN. § 47-18-2101 (2005); TEX. BUS. & COMM. CODE. §§ 48.001 (2005); WASH. REV. CODE § 19.255.010 (2005).

[56] Additional provisions include "redaction", see e.g. ARK. CODE ANN. § 4-110-105 (Michie 2005) or data that is protected "by another method to make it unreadable or unusable", see e.g. UTAH CODE ANN. §§ 13-42-101 (2006).

[57] The first state to use this definition of encryption was North Carolina and was subsequently adopted by other states. See e.g. N.C. GEN. STAT. §§ 75-60 (2005). See also ARIZ. REV. STAT. § 44-7501 (2007); HAW. REV. STAT §§ 487N-1 (2007); IOWA CODE § 715C.1 (2008); MO. REV. STAT. § 407.1500 (2009); NEB. REV. STAT. §§ 87-801 (2006); OR. REV. STAT. § 646A.600 (2007); 9 VT. STAT. ANN. §§ 2430 (2007).

meaning to the data.[58] Furthermore, there are two explicit exemptions found in the Massachusetts and Maine laws that have very different definitions of encryption to those found in the majority of explicit exemptions.[59]

Rebuttable presumptions are safe harbours that create a presumption that no risk exists if encrypted data is acquired which can be rebutted if evidence is found to the contrary. Under a rebuttable presumption safe harbour, no notification is required unless it can be established that harm exists.[60] For example, under the US federal bill, the Data Accountability and Trust Act (DATA) of 2009, an organisation would be exempt from notification if personal information was encrypted and appropriate safeguards were in place to protect the encryption key. If an organisation could show that effective encryption had been applied to the acquired personal data, then a presumption would be established that there was not a significant risk of identity theft arising from the data breach. This explicit presumption could be rebutted by showing that the "method of encryption has been or is likely to be compromised."[61] Furthermore, the DATA bill extended its rebuttable presumption, in line with the other 2009 bills,[62] to cover additional methodologies or technologies, other than encryption, "which rendered data in electronic form unreadable or indecipherable."[63] The presumption again could be rebutted by showing that the method or technology was compromised or was likely to be compromised. In December 2009, DATA was the first data breach notification bill to be passed by either the House of Representatives

[58] Likewise, the first state to adopt this definition was Ohio which was again followed by other states. See e.g. OHIO REV. CODE ANN. § 1349.19 (West 2005). See also IND. CODE §§ 24-4.9-3-1 (2006); KAN. STAT. ANN. §§ 50-7a01 (2006); MD. CODE ANN. §§ 14-3501 (2008); MICH. COMP. LAWS § 445.72 (2007); N.H. REV. STAT. ANN. §§ 359-C:19 (2007); OHIO REV. CODE ANN. § 1349.19 (West 2005); 73 PA. CONS. STAT. § 2303 (2006); VA. CODE ANN. § 18.2-186.6 (Michie 2008); W. VA. CODE §§ 46A-2A-101 (2008).

[59] See MASS. GEN. LAWS 93H §1 (2007). The full definition of encryption reads "encryption is the transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation." and ME. REV. STAT. ANN. 10, §§ 210-B-1346 (West 2007). "'Encryption' means the disguising of data using generally accepted practices."

[60] M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555

[61] S. 3(f)(2)(A)&(B) Data Accountability and Trust Act of 2009, H.R. 2221, 111th Cong. (2009).

[62] See Data Breach Notification Act of 2009, S. 139, 111th Cong. (2009); Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009).

[63] S3(f)(2)(B) Data Accountability and Trust Act of 2009, H.R. 2221, 111th Cong. (2009).

or the Senate. It is therefore possible that a federal data breach notification law could be enacted in 2010 and the encryption safe harbour will be a rebuttable presumption.[64]

Finally, under the third safe harbour, *factor-based analysis*, encryption is merely a "factor to use in determining whether harm will reasonably result from the breach."[65] For example, the data breach notification proposal put forward by the Australian Law Reform Commission (ALRC) indicates that one of the key considerations as to whether a data breach could give rise to "a real risk of serious harm" was whether the specified personal information was "encrypted adequately."[66] Likewise, with the new e-Privacy Directive, a public telecommunications service provider will not have to provide notification if it can demonstrate to the satisfaction of a competent authority that it has implemented appropriate technological protection mechanisms. Such mechanisms would be a factor to demonstrate that data had been rendered unintelligible and the measures were applied to the personal data involved in the breach.[67]

4 CRITIQUE OF ENCRYPTION SAFE HARBOURS

We now critique encryption safe harbours through a scenario based analysis involving a conditional claim for reliance upon an encryption safe harbour. The scenarios outlined below are based upon the two most common forms of data breach, namely, loss of storage media or a laptop and a hacking incident.[68] However, as we outline below, both of these types of data breach potentially engender different types of response.

[64] It should also be noted that the Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009) was also recommended by committee for a full senate vote. This bill has an acquisition based trigger but with a risk-based exemption that provides similar effect to a risk-based trigger.

[65] M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555.

[66] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (2008): 1692.

[67] Art. 4(c) e-Privacy Directive.

[68] See Open Security Foundation, *Dataloss Statistics* (2009) <http://datalossdb.org/statistics> at 19 August 2009. The DataLossDB website has chronicled a dramatic increase in the number of data breach incidents from the inception of the first data breach notification law. In 2003, 24 incidents were notified but 725 incidents were notified in 2008 and 442 in 2009. The most common type of data breaches were stolen laptops (20%), computer hacking incidents (16%) and inadvertent publication on the Internet (13%).

4.1 A CONDITIONAL CLAIM FOR RELIANCE UPON AN ENCRYPTION SAFE HARBOUR

A threshold condition for encryption to be considered a safe harbor against an obligation to notify is that the potentially breached personal information[69] exists in encrypted form. There are three categories of encryption use satisfying this condition that can be distinguished based on the varying efficacy of the encryption in preventing unauthorised access to the personal information. They are that the potentially breached personal information was

1. *Adequately encrypted in a manner that is likely to be effective.* The unauthorised party only has access to the ciphertext, with no access to decryption keys or other material that may be used to assist in decrypting the ciphertext. The likelihood that an unauthorised party can access the plaintext is very low.
2. *Encrypted in a manner that may or may not be effective*. It is possible that a sufficiently skilled and motivated unauthorised party may be able to recover the plaintext from the ciphertext.
3. *Encrypted in a manner that may have been bypassed and is therefore ineffective.* The potentially breached personal information exists in encrypted form but the information that was acquired or lost may not have been encrypted.

Category 1 deals with situations where encryption is used according to best practice, as a component of a comprehensive information security program. The encryption algorithm, its implementation and its mode of use conform to recognised standards. Key management practices similarly conform to standards-based recommended practice, ensuring that the decryption key(s) are only accessible to authorised users and were therefore not compromised. A simple example of this scenario is the loss of a USB drive containing a file encrypted with the Advanced Encryption Standard (AES) algorithm using a 128 bit randomly generated key that was not stored in any form on the drive or any other location accessible to an unauthorised party.

Category 2 covers scenarios where an unauthorised party with the necessary skill, resources and motivation, may be able to recover the plaintext personal information from ciphertext to

[69] For this sub-section, we use the phrase "potentially breached personal information" to represent personal information that may or may not have been acquired in a data breach involving encryption protections because the data will only be acquired if the encryption can be defeated (e.g. in category 2 by a sufficiently skilled and motivated party and in category 3 if the encryption used was bypassed).

which they have access. The possibility arises because the unauthorised party may be able to exploit weaknesses present in the encryption algorithm, its implementation, its mode of use, or weaknesses in the management of decryption keys. An example of Category 2 encryption use involves personal information transmitted over a wireless network secured with the Wired Equivalent Privacy (WEP) protocol.[70] The WEP encryption protocol is known to be insecure[71] and tools are freely available to quickly tap into WEP-protected wireless networks simply by monitoring and analysing a small amount of the encrypted traffic.[72] The attackers who perpetrated the much-publicised TJX data breach, which involved the leaking of 94 million records of personal information, initially gained access to TJX's internal computer networks via a WEP-secured wireless network.[73]

Laptop computers with encrypted hard disks are another example of category 2 encryption use.[74] Hard disk encryption systems including Microsoft's Bitlocker[75] and the open source Truecrypt[76] are susceptible to a range of attacks on the key management system. For example, the decryption key can be recovered from system memory if an unauthorised party can gain access to the laptop in a running or suspended state.[77] Freely available commercial tools exist to mount such attacks.[78]

---

[70] WEP is an encryption protocol for IEEE 802.11 wireless networks. Wireless networks broadcast network traffic on standard frequencies that can be received by an adversary who is within broadcast range. The ciphertext of network traffic is therefore assumed to be publicly known.

[71] See R Housley and W Arbaugh, 'Security Problems in 802.11-based Networks' (2003) 46(5) *Communications of the ACM* 31.

[72] Tools such as the freely available Aircrack key cracking program can recover WEP encryption keys from protected 802.11 wireless signals in a matter of minutes. See Aircrack-Ng, *Homepage* (2009) <http://www.aircrack-ng.org/> at 20 March 2010.

[73] 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 2007, A1.

[74] Given that 20% of data loss incidents involve stolen laptop computers, hard drive encryption is an increasingly popular strategy to mitigate the risk of personal information loss arising from stolen laptop computers. See Open Security Foundation, *Dataloss Statistics* (2009) <http://datalossdb.org/statistics> at 19 August 2009.

[75] See Microsoft, *Bitlocker* (2009) <http://www.microsoft.com/windows/windows-7/features/bitlocker.aspx> at 20 March 2010.

[76] See Truecrypt, *Homepage* (2009) <http://www.truecrypt.org/> at 20 March 2010.

[77] Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., Feldman, A. J., Appelbaum, J., and Felten, E. W. 2008. Lest We Remember: Cold Boot Attacks on Encryption Keys. In Proceedings of the 17th Conference on Security Symposium (San Jose, CA, July 28 - August 01, 2008). USENIX Association, Berkeley, CA, 45-60.

[78] For example, see Passware Kit Version 9.5 from Passware Inc. as reported in L Seltzer, *New Passware Can Crack PGP and BitLocker-Protected Systems"* (2009) <http://blogs.pcmag.com/securitywatch/2009/12/new_passware_can_crack_pgp_and.php> at 3 March 2010.

The third category of encryption use deals with scenarios where an unauthorised party can access plaintext personal information without the need to acquire the decryption key to execute the explicit step of decrypting the ciphertext. Network-accessible or online applications are a common example. The decryption key is not required because the application provides an automatically decrypting channel to authorised users. In this scenario, it is the authentication that is defeated, not the encryption.[79] The personal information exists in encrypted form but the system provides an interface by which authenticated and authorised users can access the plaintext.

For example, an online medical records system may store personal information and other sensitive health data in a database that is encrypted. Access to the system is controlled via password authentication and only authorised users are able to access the plaintext records. If an unauthorised party is able to discover the username and password of an authorised user, they can access the personal information without knowing the decryption key. They merely log on to the application and will be treated as an authorised user. As explained in section 2, passwords have a host of well-known vulnerabilities: they can be compromised via phishing attacks or via key logging malware installed on an authorised user's computer. They can also be guessed by automated password guessing programs. Though the practice violates recognised security management standards, usernames and passwords are commonly transmitted over internal networks unencrypted and are therefore susceptible to compromise via snooping. In the TJX data breach incident, once the attackers had gained access to the internal network, they snooped unencrypted usernames and passwords submitted by legitimate users as they logged into transaction processing applications.[80]

The third category of encryption use is potentially the least reliable as a basis for claiming a safe harbour from the obligation to notify affected individuals in case of a suspected data breach. In the case of compromised login credentials, an unauthorised party can access any personal information that an authorised user is permitted to access. Encryption provides no protection. Moreover, it is not immediately obvious when an authorised user's credentials such as a password have been compromised. Illicit access may occur for months or years

[79] For a further discussion of weaknesses of authentication methods see: L O'Gorman, 'Comparing Passwords, Tokens, and Biometrics for User Authentication' (2003) 91(12) *Proceedings of the IEEE* 2021.
[80] 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 2007, A1.

before it is detected.[81] It is therefore dangerous to assert or conclude that personal information has not been disclosed, simply because password authentication, encryption or other protection measures are in place. It is very difficult for organisations to know what an unauthorised party may have done, and what personal information may have been accessed, when a hacking incident is suspected, particularly if best-practice logging, audit and review procedures are not being followed.

The use of encryption certainly does not provide a guarantee of protection. It is therefore arguable that a general notification safe harbor that can be claimed simply because these fallible methods are in place is misguided. When a breach is suspected, a better approach would be to require affected organisations to undertake a competent review to estimate the likelihood that personal information has actually been disclosed, irrespective of the protective security mechanisms that are in place. The notification obligation should be informed by a process of review and we address this important point in our next section.

4.2 A SCENARIO BASED CRITIQUE

Our three scenarios demonstrate that the effective use of encryption requires a complex management process that goes beyond the simple act of encrypting a given set or piece of data. We therefore agree that encryption should not be considered as a silver bullet.[82] Accordingly, legal exclusions to notification, as exemplified by an encryption safe harbour, should only be available to a breached entity following a competent review of the circumstances of a breach which includes a critical analysis of all information security management protections, and not just encryption.

One of the key aims of data breach notification laws is to encourage effective information security management protections. Smedinghoff has placed the development of data breach notification laws within the wider ambit of a developing legal duty to provide effective

[81] For example, in the TJX data breach it is estimated that the unauthorised party had access to internal systems for 18 months before the intrusion was detected.

[82] See T H Skinner, 'California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation' (2003) 10(1) *Richmond Journal of Law & Technology* ; J Winn, 'Are 'Better' Security Breach Notification Laws Possible?' (2009) *Berkeley Technology Law Journal, Vol. 24, 2009*, 14.

information security measures.[83] Laws that seek to develop this legal duty do so from a range of perspectives that can focus on the requirements of information protection in specific industrial sectors[84] or specific types of corporately held information.[85] However, regardless of their focus all of these laws intend to ensure that corporate entities have implemented appropriate information security controls in relation to the sensitive or personal information that they hold.[86] Concomitant with the development of these laws, there has been a regulatory shift from the imposition of generally accepted standards that apply to all circumstances[87] to a more sophisticated and nuanced process-based approach to be applied on a case-by-case basis. Corporate entities are therefore required to

> "[E]ngage in an ongoing and repetitive process that is designed to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments."[88]

This process-based approach therefore requires corporate information security management measures to be commensurate and responsive to the entity's own fact-specific risk assessments. Accordingly, it is insufficient to simply implement a seemingly strong type of security measure, because that measure may not necessarily address the particular threats an entity may face. Drawing on the example in our scenario, the loss of an encrypted laptop with a small amount of personal information and the decryption key may, on its face, be less of a concern than a hacking attack on a database holding millions of personal information records. However, if the laptop was lost or stolen from a military or intelligence related government agency, and the personal information held was classified, then the threats

---

[83] T J Smedinghoff, 'Trends in the Law of Information Security' (2005) 17 *Intellectual Property & Technology Law Journal* 1(5). See also J Winn, 'Are 'Better' Security Breach Notification Laws Possible?' (2009) *Berkeley Technology Law Journal, Vol. 24, 2009*, 4; J Winn, 'Can a Duty of Information Security Become Special Protection for Sensitive Data Under US Law?' (2008) *SSRN eLibrary* ; A M Matwyshyn, *Harboring data: Information Security, Law, and the Corporation* (2009), 7-13.

[84] See T J Smedinghoff, *The State of Information Security Law: A Focus on the Key Legal Trends* (2009), 16 regarding regulation of the health care sector under the Health Information Portability and Accountability Act of 1996 and financial sector under the Gramm Leach Bliley Financial Services Modernization Act of 1999.

[85] Ibid., 10 such as corporate financial data under the Sarbannes Oxley Act of 2002

[86] T J Smedinghoff, 'Trends in the Law of Information Security' (2005) 17 *Intellectual Property & Technology Law Journal* 1(5), 1.

[87] For example, see the discussion about reasonable or appropriate security at T J Smedinghoff, *The State of Information Security Law: A Focus on the Key Legal Trends* (2009), 16.

[88] T J Smedinghoff, 'Trends in the Law of Information Security' (2005) 17 *Intellectual Property & Technology Law Journal* 1(5), 3. See also T J Smedinghoff, *The State of Information Security Law: A Focus on the Key Legal Trends* (2009), 17.

arising are potentially much greater for the individuals involved because the breach could possibly lead to a loss of life.[89] As such, the instigation of appropriate security measures must be context specific and must be proportionate to the potential risks arising from a data breach involving the protected information and the context in which that information is being held, including the nature of the entity.

We contend that the same should apply to the use of encryption as a basis for a safe harbour in data breach notification laws. The evolution of encryption safe harbours indicates a changing view of the efficacy of encryption in securing data. In the Californian law and its direct descendents, encryption equates to security.[90] But as we highlighted in Section 2 and in our scenarios, there are many ways to use encryption ineffectively. Therefore, an encryption safe harbour that implicitly equates the use of encryption with effective protection of personal information is arguably based on a false premise because it does not accurately reflect the complexities of comprehensive information security management of which encryption of personal data is a mere component and not a total solution.[91]

The simple fact that an entity has employed some form of encryption should not be used to found a basis for a safe harbour that precludes notification obligations. Instead, the use of encryption should be viewed as one component of a broader information security management process. In case of a data breach, the disclosure risk needs to be assessed by examining the effectiveness of this broader management system since on its own, the use of encryption does not indicate the absence of risk. Moreover, the risk assessment process must be undertaken for each and every data breach and must examine the facts specific to each data breach. We now address these points against each encryption safe harbour to examine the extent that a risk assessment process is required before the safe harbour can be relied

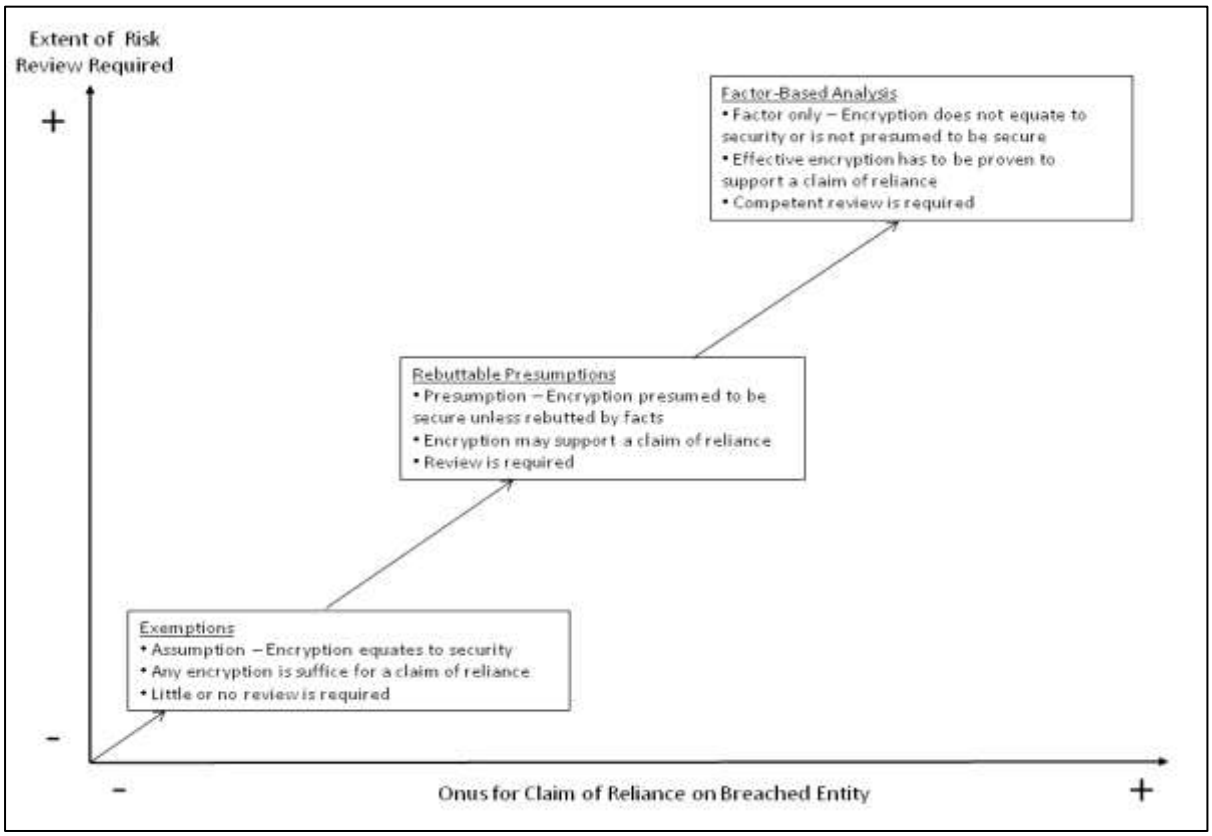
[89] See e.g. M Isikoff, *Missing: A Laptop of DEA Informants* (2004) Newsweek <http://www.newsweek.com/id/53958> at 17 March 2010 regarding the loss of a laptop containing informant details relating to investigations conducted by the Drug Enforcement Administration in the US. See also BBC News, *MoD Inquiry After Laptop Stolen from Headquarters* (2009) <http://news.bbc.co.uk/2/hi/uk_news/8409363.stm> at 17 March 2010 regarding the theft of a laptop from MoD headquarters in the UK and BBC News, *Previous Cases of Missing Data* (2009) <http://news.bbc.co.uk/2/hi/uk_news/8409405.stm> at 17 March 2010 for other instances of security failures involving laptops and sensitive UK government information.

[90] See T H Skinner, 'California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation' (2003) 10(1) *Richmond Journal of Law & Technology*

[91] Ibid. "Encryption, however, is not supposed to be the primary source of security. It is designed to supplement an overall risk-based program. It is part of the solution, not the solution".

upon. Our analysis is based on the scenarios outlined above and Figure 1 provides a diagrammatical summary of our analysis.

Figure 1. – Assessment of Encryption Safe Harbours



Exemptions provide the least amount of risk review particularly so for the Californian type encryption exemptions with their broad-brush exclusion based on "unencrypted personal information." Under the non-explicit exemptions it is possible that all categories of encryption use, as outlined in our scenarios, could provide a basis for relying upon the exemption safe harbour because the exemptions only require personal information to be encrypted. Category 2 and category 3 types of encryption usage could therefore be exempt from notification even though they may not provide effective protections. Accordingly, the broad-ranging and expansive basis of the Californian type exemptions create a potential loophole because any type of encryption, including potentially ineffective encryption, will be sufficient for a breached entity to claim an exemption from notification. An organisation can simply install a protection measure that includes encryption regardless of its

effectiveness, to avail itself of the exemption.[92] This is because the Californian type exemptions require little or no process of review before an exemption can be relied upon and it is based on a misguided underlying assumption that encryption equates to security. In effect, these laws adopt a broad acquisition trigger but also employ an equally broad encryption based exemption.

Those laws that have blanket exemptions for encrypted personal information, such as Californian Civil Code 1729(a), indicate a tacit acceptance of this underlying assumption because they treat encrypted information is information which is secure regardless of the circumstances. This explains why data breaches that involve encrypted personal information do not need to be notified because there is little or no risk of an identity theft incident occurring from the unauthorised acquisition of protected information.

The weaknesses of the non-explicit, Californian exemption has been recognised by other state-based data breach notification laws but attempts to alleviate potential problems have focused on one of two remedial fixes, as highlighted above: (1) the inclusion of additional terms to the original Californian definition of *unencrypted personal information* in non-explicit exemptions or (2) the construction of explicit definitions of encryption combined with a tendency towards a risk-based trigger.[93] However, both remedial fixes have caused further problems. For example, the inclusion of additional terms has resulted in non-explicit exemptions that have conflicting elements. Many state-based laws have adopted the wording of the Californian law but have also added an additional statutory term relating to redaction.[94] A major problem arises from the combination of redaction and encryption in an exemption because redaction is given the same weight as encryption when in many cases it

[92] See J Winn, 'Are 'Better' Security Breach Notification Laws Possible?' (2009) *Berkeley Technology Law Journal, Vol. 24, 2009*, 14 "companies can enjoy the benefit of the safe harbor by the use of weak encryption technologies without adopting a systemic, risk management-based approach to information security". See also C Carlson, *Storm Brews Over Encryption Safe Harbor in Data Breach Bills* (2005) <http://www.eweek.com/c/a/Government-IT/Storm-Brews-Over-Encryption-Safe-Harbor-in-Data-Breach-Bills/> at 11 January 2010 and the comments by Bruce Schneier.

[93] See e.g. ARIZ. REV. STAT. § 44-7501 (2007); HAW. REV. STAT §§ 487N-1 (2007); IND. CODE §§ 24-4.9-3-1 (2006); KAN. STAT. ANN. §§ 50-7a01 (2006); ME. REV. STAT. ANN. 10, §§ 210-B-1346 (West 2007); MD. CODE ANN. §§ 14-3501 (2008); MASS. GEN. LAWS 93H §1 (2007); MICH. COMP. LAWS § 445.72 (2007); MO. REV. STAT. § 407.1500 (2009); N.H. REV. STAT. ANN. §§ 359-C:19 (2007); N.C. GEN. STAT. §§ 75-60 (2005); OHIO REV. CODE ANN. § 1349.19 (West 2005); W. VA. CODE §§ 46A-2A-101 (2008).

[94] See e.g. ALASKA STAT. § 45.48.010 (Michie 2009); ARK. CODE ANN. § 4-110-105 (Michie 2005); COLO. REV. STAT. § 6-1-716 (2006); GA. CODE ANN. §§ 10-1-911 (2005); 815 ILL. COMP. STAT. 530/1 (2005); LA. REV. STAT. ANN. §§ 51:3071 (West 2005); N.Y. GEN. BUS. LAWS §§ 899-aa (2005); S.C. CODE ANN. § 39-1-90 (Law Co-op 2009); 9 VT. STAT. ANN. §§ 2430 (2007); WIS. STAT. § 895.507 (2006).

should not be because it is trivially reversible. Guidance produced by the US Government's Department of Health and Human Services in relation to security rules for the Health Information Portability and Accountability Act (HIPAA)[95] make it clear that redaction should not be considered as secure as encryption and should only be used with paper records.[96] Accordingly, the lower standard that redaction sets nullifies the higher standards offered by properly implemented encryption when combined together.

The explicit encryption exemptions provide a greater degree of process review than their Californian type counterparts[97] but they are nevertheless still prone to exempt notification based on category 2 and category 3 type encryption usage because of the difficulties that arise from attempts to explicitly define encryption either through the combination of conflicting terms or through internal inconsistencies. As highlighted above, different state-based laws set higher and lower standards as to what constitutes encryption and problems emerge with laws that combine both elements. For example, the Indiana law[98] uses different terms that are based on a combination of both low probability and unreadable or unusable.[99] The use of the phrase "low probability" is different from "unreadable or unusable" because it is not an absolute (i.e. the data is either readable or usable or it is not). The use of low probability therefore connotes that encrypted data is never believed to be absolutely secure. These laws effectively have two different operational standards with one element operating at a higher level than another.

The two states with unique definitions of encryption, Massachusetts and Maine also encounter problems. The definition of encryption employed by Massachusetts is internally inconsistent. The use of a statutory term "transformation of data using 128 bits or higher"

[95] Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191).
[96] Department of Health and Human Services, '45 CFR Parts 160 and 164 - Breach Notification for Unsecured Protected Health Information' (2009), 42742 "Because redaction is not a standardized methodology with proven capabilities to destroy or render the underlying information unusable, unreadable or indecipherable, we do not believe that redaction is an accepted alternative method to secure paper-based protected health information. As such, under the guidance redaction should not given the same weight as encryption and other methods of securing technology. Only destruction of paper records will suffice as a requirement and redaction is not enough. The note makes clear that redaction is only to be used with paper records".
[97] Such exemptions require a limited process of review based on whether the encryption adopted meets a specified definition of encryption, before an exemption can be relied upon.
[98] See e.g. IND. CODE §§ 24-4.9-3-1 (2006)§9-2-5 "Data are encrypted for purposes of this article if the data: (1) have been transformed through the use of an *algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key*; or (2) *are secured by another method that renders the data unreadable or unusable"*[emphasis added].
[99] See also KAN. STAT. ANN. §§ 50-7a01 (2006); MD. CODE ANN. §§ 14-3501 (2008); MICH. COMP. LAWS § 445.72 (2007); N.H. REV. STAT. ANN. §§ 359-C:19 (2007).

indicates that the transformation must use a key since 128 bits refers to the key length. Therefore the subsequent *confidential process* element is redundant because confidential process transformations are not key-based. Furthermore, the Maine law employs a unique definition of encryption that is based on "generally accepted practices." However, "general accepted practices" is so broad that it does not necessarily equate to effective encryption. For example, the implementation of a certain encryption software package could be considered as a generally accepted practice even though it may not provide an acceptable level of protection in a given circumstance. Indeed, part of the motivation for data breach laws has been recognition of the fact that the general standard of protection of personal information by both corporate and government entities has been woefully inadequate. When improvements in practice are clearly needed, that which is *generally accepted* may not be the best indicator of what is effective and adequate.

Rebuttable presumptions provide a greater degree of process review than exemptions because they are inherently linked to the risk assessment that is required from a risk-based notification trigger. For example, the DATA bill has a general exemption to notification if there is "no reasonable risk of identity theft, fraud, or other unlawful conduct."[100] A presumption is created under the bill which states that encrypted data does not give rise to a reasonable risk and this presumption is rebuttable by facts that demonstrate encryption has or is reasonably likely to be compromised.[101] As such, whether data is or is not encrypted is a key element of the risk-based exemption and the extent to which the implemented encryption protections are effective has to be reviewed for an entity to rely on the presumption that encrypted data is secure. Unlike exemptions, rebuttable presumptions require a breached entity to review its encryption processes before it can rely on the presumption as a safe harbour to notification.

In terms of our scenario, a safe harbour based on a rebuttable presumption would require a review of category 2 and category 3 types of encryption use so it therefore has advantages over the use of an exemption and it is less likely to create the potential for the same wide-ranging loophole because it introduces the notion of effectiveness rather than treating technology as infallible. However, several concerns arise from the use of rebuttable presumptions as a basis for a safe harbour. The strongest concern is that the onus to rebut the presumption is left with the breached organisation itself or by other forms of regulation

[100] S3(f)(1)Data Breach Notification Act of 2009, S. 139, 111th Cong. (2009).
[101] S3(f)(2)Data Breach Notification Act of 2009, S.139, 111th Cong. (2009).

developed by key regulators.[102] Leaving the rebuttable process to the breached entity is problematic because the historical development of data breach notification laws has recognised the reluctance of corporate entities to notify individuals, regulators or law enforcement agencies about a data breach, predominantly due to fears of an adverse effect on reputation and share price.[103] Even though the reporting of data breaches is now much more common the embarrassment factor is still likely to be a prominent concern of corporate entities. Accordingly, the extent to which a breached entity will undertake a review to seek facts that rebut an encryption based presumption is questionable. The uncertainty and technical complexity of intrusion detection and forensic analysis in determining what an hacker has actually done, and which records have been accessed, particularly in the case of category 3 encryption use mean that organisations may chose to hide behind a veil of plausible deniability. Indeed, an unfortunate side effect of risk-based notification safe harbours may be that some organisations chose to expend less effort in trying to detect category 3 compromises since detection may lead to an obligation to notify.

Strictly defined regulatory rules may also be problematic as they have the potential to suffer from the same predicaments as encryption defined exemptions and technical advancements that outpace the use of specific types or generations of technologies.[104] Whilst rebuttable presumptions offer a level of review that is higher than exemptions they are still questionable as a basis for an encryption safe harbour. They would not automatically exempt category 2 and category 3 type uses of encryption, as exemptions could do, but they potentially place too much faith in a breached entity's ability and willingness to competently review the effectiveness of encryption processes in a data breach.

---

[102] For example, S3(f)(2) requires, within 270 days of enactment of DATA that the Federal Trade Commission "identify any additional security methodology or technology, other than encryption, which renders data in electronic form unreadable or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data".

[103] See e.g. Computer Security Institute and Federal Bureau of Investigation, 'Computer Crime and Security Survey' (2006), 21 and the unwillingness of breached entities to notify even law enforcement agencies.

[104] See e.g. S A Needles, 'The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law' (2009) 88 *North Carolina Law Review* 267, 308; K E Picanso, 'Protecting Information Security Under a Uniform Data Breach Notification Law' (2006) 75(1) *Fordham Law Review* 355, 378 and Samuelson Law Technology & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers* (2007) <http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf> at 21 March 2010, 32 commenting "However, because encryption is an evolving technology, it seems better suited for definition and reevaluation by regulatory agencies than strict definitions in statutes."

The potential weaknesses of exemptions and rebuttable presumptions are less likely to arise in the use of a factor-based analysis as a basis for an encryption safe harbour because the onus for claiming reliance on the safe harbour is squarely on the shoulders of the breached entity. In effect, the breached entity has to establish that the encryption adopted was effective before it can rely on a safe harbour that exempts notification. The entity is also required to undertake a competent review for each and every data breach as the claiming of the safe harbour occurs on a case-by-case basis. A factor-based analysis therefore has an inherently critical perspective about the role of encryption in securing personal information and the role of the breached entity in reviewing a data breach.

Factor-based analysis, such as the e-Privacy Directive and the ALRC proposal, reject the notion that encryption automatically equates to security and have attempted to develop less prescriptive definitions that focus on risk-based assessments with reference to effective industry practices or recognised security management standards. As such, they have a broader notion of what constitutes effective security that goes beyond the technical process of encryption. They place a greater obligation on data collecting entities regarding the development and implementation of adequate security measures. However, the fundamental difference between factor-based analysis and the other safe harbours resides in the fact that it is the breached entity which must be able to demonstrate that the encryption or other methods relied upon were effective because they met industry standards of accepted best practice.

Returning to our scenario, it is less likely that a category 2 or category 3 type use of encryption would give rise to reliance on a safe harbour because the breached entity would be required to show that the encryption used in both cases was effective. The complexities of information security management mean that a factor-based analysis will not preclude all types of category 2 and category 3 encryption use from a safe harbour but the rigorous review that it requires is likely to minimise the opportunities for reliance upon these types of encryption use where, in the specific circumstances, the information disclosure risk remains high. Furthermore, a factor-based analysis could provide regulators with a much greater understanding of how data breach problems develop and we address this point in the final section of our article.

5 ENCRYPTION SAFE HARBOUR AND TRIGGER RECOMMENDATIONS

We now put forward our recommendations for the use of our favoured encryption safe harbour in conjunction with a notification trigger.

5.1 FACTOR-BASED SAFE HARBOURS

We consider that factor-based analysis should found the basis for an encryption safe harbour in data breach notification laws. The reasons for our recommendation are outlined above but they can be summarised as the combined benefits of having a more realistic perspective on the fallibility of encryption that places the onus on a breached entity to prove that the encryption adopted was effective which requires a competent risk-based review of each and every data breach. We favour a combined approach that adopts elements of by the ALRC's proposal and the e-Privacy Directive.

The ALRC's proposed factor-based analysis is advantageous because it has the benefit of simplicity and flexibility. The safe harbour plays an integral part of risk-based assessment and therefore inherits the compliance reduction aims that are inherent to all data breach notification laws. The ALRC have unequivocally attempted to avoid defining encryption in any detail. Instead, there is a simple requirement that the type of encryption used is "adequate." The ALRC's encryption safe harbour philosophy is similar in construction to Californian type exemptions. There is however, a significant departure from the use of exemptions as the ALRC's factor-based safe harbour provides a greater conceptual depth as to what constitutes effective encryption, even though it is achieved by a simple statutory term.

The use of "adequate" connotes that encryption is not meant to be defined as a simple one-off technical act, as suggested by exemptions. Instead, the ALRC recognize that effective encryption should be viewed as existing within a broader security management process that entails many different facets and requirements, beyond the mere encryption of data. This would require a deeper analysis of category 3 type encryption uses which the other safe harbours may not provide. Encryption will therefore not be adequate if there is an "easy means of decoding" data. Such a means may be provided by the effective protection of encryption keys.[105] Moreover, because the assessment of adequacy is based on the factors of

[105] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (2008), 1692.

each individual data breach[106] the ALRC require the type of risk process review envisaged by Smedinghoff that ties the operation of the safe harbour to the factual circumstances of each individual data breach. Accordingly, there is a rejection of the underlying assumption prevailing in exemptions that encrypted information is secure *regardless* of the circumstances of the data breach. In fact, the opposite is the case. The ALRC's factor-based safe harbour can only be claimed if an organisation can show that the encryption adopted was adequate and was likely to remain effective in light of the specific particulars of an individual breach.

Furthermore, by not specifying what encryption or adequate encryption is, the ALRC have avoided many of the definitional problems of US state-based exemptions. The simplicity of the ALRC's approach avoids such problems, but at the same time, it captures the complexity of effective information security management. The use of guidance to define issues of adequacy in relation to encryption is also welcomed because it ensures a flexible approach that can adapt over time and thus avoid some of the difficulties that can arise when a specific form of encryption becomes unsecure, unlike regulatory rules relating to rebuttable presumptions. The ALRC's proposed encryption exemption succinctly balances the two competing elements that found the basis of the horizontal tension identified in our first article within the guise of a practical setting, namely, the need for organisations to have a practical and workable definition of encryption and the requirement of effective encryption that is more than a single, technical act of encrypting data thus enhancing consumer protections.

However, as we highlight above in our scenario analysis, the effective protection of personal information goes beyond the process of encryption and must be based on the concept of an ongoing process of risk-based review. The ALRC's proposal fulfils the latter but less so the former. As such, the use of a wider factor-based analysis, such as the e-Privacy Directive's focus on "technological protection measures" is recommended.[107] Nonetheless, we prefer the use of the ARLC's designated standard of "adequate" over the e-Privacy Directive's "appropriate" because an information protection mechanism can still be appropriate but

[106] Ibid. These include the type of personal information breached, the nature of the agency or organisation that encountered the breach, and the risk of harm that would be caused by the breach.
[107] See Art 4 of the e-Privacy Directive "Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it".

inadequate such as the category 2 and category 3 types of encryption used in our scenario.[108] Furthermore, we contend that the use of adequate does not entail any further definitional requirements for a safe harbour, such as, the condition to render data unintelligible to an unauthorised person as stated in the e-Privacy Directive. If a technological protection mechanism is adequate it should render data unintelligible and given the morass of definitions found in US state-based exemptions, we contend that simple and less is the appropriate statutory basis for the construction of a safe harbour.

5.2 TWO-TIER NOTIFICATION TRIGGER

We further recommend that a two-tier notification trigger should be used in conjunction with a factor-based safe harbour. We generally agree with Jones's broad assessment that an acquisition-based trigger has a consumer protection orientation and a risk-based trigger favours corporate compliance reduction.[109] However, we contend that the sole use of either one of these triggers displaces the complex balancing act that data breach notification laws attempt to reconcile. An acquisition-based trigger is too broad and laws that use this trigger have developed equally broad exemptions, such as encryption exemptions or restrictive definitions of personal information and data breaches to counteract fears of over-notification. Moreover, the claim that an acquisition-based trigger supports consumer protection is weakened by the fact that data breach notification laws, by their nature, focus on notification and pay little heed to the consequences of post-notification for individuals.[110] Broad-based notification only provides an effective consumer protection benefit if individual consumers have the skills and knowledge to respond effectively to a notification. This connotes a degree of consumer education which is missing in data breach notification laws. On the other hand, a risk-based trigger, particularly without any regulatory oversight provisions, displaces the balance too much towards corporate compliance especially given

[108] For example, appropriate is defined in the Oxford English Dictionary as "specially fitted or suitable" and appropriate technology can mean "technology considered suitable for a particular application". Whereas adequate is defined as "commensurate in fitness; equal or amounting to what is required; fully sufficient, suitable, or fitting."As such, encryption can be suitable for the purpose of protecting personal information, but as we have shown with our category 2 and category 3 scenarios of encryption use, just because it is considered suitable for a particular purpose it should not presuppose that the use of encryption is commensurate in fitness or fully sufficient to fulfil that purpose.

[109] M E Jones, 'Data Breaches: Recent Developments in the Public and Private Sectors' (2007) 3 *I/S: A Journal of Law and Policy for the Information Society* 555, 580.

[110] See P M Schwartz and E J Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913, 940 and B Lane et al, 'Stakeholder Perspectives Regarding the Mandatory Notification of Australian Data Breaches' (2010) forthcoming *Media and Arts Law Review* .

the motivations and incentives to not report a data breach either directly or by conducting an inadequate review of information security practices.

We contend that a balance can be achieved through the adoption of a two-tier notification trigger. An acquisition-based trigger, based on unauthorised acquisition, would be adopted for notifications to a designated regulatory authority and this would ensure that a greater understanding of the situation "on the ground" was gained from a regulatory perspective. This is an important point as the lack of valid and reliable statistical information has been a problem in the development of data breach notification laws.[111] Regulators would therefore receive a greater number of notifications but this information would greatly assist with the identification of regulatory problems especially at the onset of implementation.

Wider notifications to individuals possibly affected and to other relevant authorities could then be based on a risk-based trigger formulated on a reasonable risk of harm. We have chosen a lower standard for this trigger than some data breach notification laws. Our basis for this standard is straightforward – if a reasonable risk has been identified then an individual or another authority should be notified. The identification of a risk is therefore the important requirement for breached entities. The notified individual should then be left to determine whether the risk is sufficient to warrant mitigation based on their own circumstances and the information presented to them in the notification. Harm should also be construed broadly to consider detrimental impacts such as whether a data breach adversely affects the privacy of an individual[112] and thus go beyond the mitigation of identity theft. In keeping with the process of review outlined in the previous section, a breached entity must determine whether a risk exists but notifications should be conducted in conjunction with the designated regulatory authority. Moreover, a regulatory authority should have powers of regulatory oversight and be able to compel notification if a reasonable belief of harm has been identified but not acknowledged by the breached entity.

One of the significant advantages of this format is that it should lead to the development of a regulatory jurisprudential discourse about what constitutes the key elements of data breach notification requirements, such as an unauthorised acquisition, a reasonable risk of harm or adequate technological protection mechanisms, which has been sorely lacking thus far. The

[111] See e.g. M Burdon, B Lane and P von Nessen, 'The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments' (2010) 26(2) Computer Law & Security Review 115, 123-4.
[112] See Art 4 of the e-Privacy Directive.

format will mean however a greater regulatory role than most data breach notification laws envisage. We believe this is justified by a wider overall regulatory aim for data breach notification that focuses on the development of legal standards for information security. Data breach notification is therefore a component in a spectrum of protections that cross existing disciplinary boundaries relating to the laws of privacy, information management and corporate governance. Data breach notification is not the be all and end all in itself. Rather, it highlights the failings of current legal approaches relating to the corporate protection of sensitive information and the detrimental impacts that arise from those failings. Whilst data breach notification laws provide a lens to view those failings they may not provide the requisite remedies to resolve them because of their limited focus and their conflicting conceptual basis. Laws are required that focus specifically on the development of legal principles related to corporate information security management. These laws could play an essential regulatory role regarding the protection of personal information and the protection of critical information infrastructures which hold our personal information and are now such an integral part of our information-based societies. Data breach notification laws provide us with a glimpse of this bigger-picture requirement but they do not give us the means to construct the regulatory structures to fulfil that requirement.

6 CONCLUSION

We have demonstrated that different safe harbours provide a different degree of risk-based review in order to claim the benefits of a safe harbour. Exemptions provide little or no review before a safe harbour can be relied upon because this safe harbour assumes that encryption equates to security. Rebuttable presumptions provide a greater level of review before a safe harbour can be relied upon but that review is construed in favour of the breached entity. Factor-based analysis requires a competent review and embodies a critical perspective about the role of encryption and the role of a breached entity in reviewing and reporting. We therefore recommend the use of factor-based analysis over exemptions and rebuttable presumptions as a basis for a safe harbour to notification because of this critical perspective the requirement for a rigorous review to be undertaken before the safe harbour can be relied upon. Our recommended safe harbour is based on a combination of the ALRC's proposal and the e-Privacy Directive. In conjunction with a factor-based safe harbour, we further recommend the use of a two-tier notification trigger involving notification to regulators on an acquisition-based trigger and notification to individuals on a risk-based trigger based on a reasonable risk of harm.

Critics of our choice of encryption safe harbour and notification trigger may contest that the combination of a factor-based safe harbour and a two-tier trigger may be difficult for the courts to enforce given its contextual requirement. In turn, this is likely to increase compliance costs for organisations regarding notification of data breaches. That may be so but there needs to be a general recognition that the issues covered in our article are sufficiently important to require a constant revision of the protection of personal information by corporate and government entities. The more we transport our lives to information infrastructures, the greater the requirement is to ensure the implementation of adequate security measures, commensurate to the type of information being held and the nature of the organisation that is holding it. These are complex issues which cannot be resolved by the instigation of a particular type of legal obligation, such as mandatory notification or a specific technological protection measure, such as encryption. Instead, legal and regulatory frameworks must match the complexities inherent in the reality of the information society by developing and employing conceptually rigorous, flexible and adequate controls.

Our research into encryption safe harbours re-emphasises the limits of data breach notification law. The instigation of legal standards relating to corporate information security requires the development of new laws with a clearer conceptual basis and which provide the legislative means to develop effective controls and remedies. Data breach notification laws certainly assist with the direction of future discourse but they are by no means the end of the conversation.

Mark Burdon (m.burdon@qut.edu.au) is a Ph.D Candidate and Research Associate at the Faculty of Law/Information Security Institute, Queensland University of Technology, Australia. Jason Reid (reid@isi.qut.edu.au) is a Senior Research Fellow at the Information Security Institute, Queensland University of Technology, Australia. Rouhshi Low (r.low@qut.edu.au) is a Lecturer in the School of Accountancy, Queensland University of Technology, Australia.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge funding from Australian Research Council Grant DP0879015 "A new legal framework for identifying and reporting Australian data breaches." The authors would also like to thank Jane Winn for her comments on a previous draft.