Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

Contradictions and inconsistencies in Australia's mandatory data breach notification laws

Dennis Gibson[1,*], *Clive Harfield*[2]

School of Science, Technology and Engineering, University of the Sunshine Coast, Sippy Downs, QLD 4556, Australia

ARTICLE INFO

Keywords:
Data breach notification
Personal information
Identity theft
Notification threshold

ABSTRACT

This article critically examines the objectives and practical operation of Australia's mandatory data breach notification [MDBN] law. We find that the scope and application of Australia's law do not reflect the legislative objectives underpinning the law. The wording of the law is ambiguous, and it is beset by conceptual inconsistencies. The law also fails to adequately consider the needs of individuals whose personal information has been compromised in a data breach. As a result, Australia's MDBN law is unlikely to meet the needs of organisations that have experienced a data breach, or of individuals who are notified. We conclude by identifying options for reform to better reflect the law's rationale and to better achieve its objectives. Comparisons are made with similar laws in force in the United States and with the General Data Protection Regulation.

1. Introduction

Mandatory data breach notification (MDBN) laws have proliferated over the last two decades. Policy-makers and legislators in several jurisdictions have resorted to mandatory reporting as a means of simultaneously mitigating the risks posed by data breaches, recognising individuals' interest in being informed about the security and (mis)use of their personal information, and incentivising organisations to adequately secure the data they hold.[3] Nevertheless, MDBN laws remain a relatively new legal phenomenon; the fiftieth state to adopt such laws in the United States was Alabama on 28 March 2018,[4] while the European Union General Data Protection Regulation

* Corresponding author: Dennis Gibson.
E-mail addresses: dennis.gibson01@gmail.com (D. Gibson), charfiel@usc.edu.au (C. Harfield).
[1] Associate Lecturer, School of Science, Technology and Engineering, University of the Sunshine Coast.
[2] Associate Professor, School of Science, Technology and Engineering, University of the Sunshine Coast.

[3] Mark Burdon, 'Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws' (2010) 27(1) Santa Clara Computer & High Tech LJ 63, 78-80; Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' (2008), 1668-1670, 1688-89. See, for example, the General Data Protection Regulation scheme applicable across the European Union; the Personal Information and Electronic Documents Act 2019 in Canada; and the Privacy Act 2020 in New Zealand. The rationale for the Australian MDBN law was asserted by the Minister for Justice to be "that, if an individual is at likely risk of serious harm because of a data breach involving their personal information, receiving notification of the breach can allow that person to take action to protect themselves from harm." Commonwealth, *Parliamentary Debates*, House of Representatives, 19 October 2016, 2430 (Michael Keenan).

[4] Bernold Nieuwesteeg and Michael Faure, 'An Analysis of the Effectiveness of the EU Data Breach Notification Obligation' (2018) 34(6) Computer Law & Security Review 1232, 1235.

https://doi.org/10.1016/j.clsr.2021.105600
0267-3649/

(GDPR) only came into force on 25 May 2018.[5] Australia's MDBN scheme, which is the focus of this article, predated the GDPR by only a few months, coming into force on 22 February 2018.[6] Many jurisdictions across the world have yet to introduce such laws, and even in countries where MDBN laws have been enacted, there are sometimes significant gaps within their legal frameworks. In Australia, for example, none of the states or territories have introduced such laws, effectively exempting state government agencies from data breach reporting, while most businesses with an annual turnover of AUD 3 million or less are also exempt.[7]

There are also significant disparities between jurisdictions. These disparities reflect the idiosyncrasies of different legal systems as well as the contrasting rationales and priorities underlying different privacy law regimes – for example, whether MDBN laws are enacted within a comprehensive information privacy regime that provides rights-based protections to individuals, or whether the laws are enacted in the absence of such a legal framework, and are intended as a market-based solution to the specific problem of identity theft.[8] These differences manifest in almost every aspect of MDBN laws, including the types and combinations of personal information captured by the MDBN scheme; the range of organisations covered by the scheme; the threshold for notification and whether separate thresholds trigger notification to regulators as compared to individuals whose personal information has been compromised (affected individuals); the information and advice breached organisations are required (or not required, as the case may be) to provide to affected individuals; and the extent to which breached organisations are required to inform other relevant entities of the breach. These divergences are also indicative of the experimental nature of these laws.

This paper examines how one jurisdiction – Australia – has structured its MDBN law, and evaluates the extent to which the current scheme achieves its objectives and provides a workable framework for breached organisations and affected individuals responding to data breaches. The first part of the paper elaborates the impetus for, and objectives of, Australia's MDBN scheme. This is followed by a discussion of how the scheme operates, including the organisations it applies to, the types of personal information captured, the threshold for notification, and the requirements associated with notification. The third part of the paper identifies several ambiguities and deficiencies in the operation of the law, the difficulties these present for both breached organisations and affected individuals, and some of the unintended consequences and harms that flow from the current operation of the law. The paper concludes by identifying several avenues for reform, based in part on comparisons with other jurisdictions. The central contentions of the paper are that the operation of Australia's MDBN law does not reflect its objectives or purpose, nor does it account sufficiently or accurately for the data breach response process. That being so, the current law is unlikely to meet the needs of either breached organisations or affected individuals.

2. The problem of identity theft

The impetus for MDBN laws stems from the unprecedented amounts of personal information being collected and used by government agencies and private organisations, and the risks individuals face when those entities fail to secure the personal information they hold from unauthorised access and disclosure.[9] Sharing one's personal information has become a necessity for accessing many goods and services, and a precondition to meaningful participation in society.[10] The primary importance of personal information in this context is as a means of verifying an individual's identity, particularly where transactions are conducted over the Internet or otherwise do not take place face-to-face. Organisations rely on combinations of personal information, identity tokens and credentials to authenticate an individual's identity – for example, an individual may be required to provide some combination of their name, email address, date of birth, driver's license number, passport number, and password. Unauthorised access to, or disclosure of, this information exposes individuals to the risk of what is commonly referred to as "identity theft";[11] that is, the risk that a third party will fraudulently represent themselves as that individual for unlawful activity.[12] The types of fraud that may occur in the course of identity theft include: unauthorised access to, and use of, financial accounts, including banking and superannuation accounts; unauthorised use of credit or debit cards; creating new financial accounts or obtaining credit under the victim's name; creating new accounts with other institutions such as telecommunications providers; filing fraudulent tax returns; and obtaining government benefits.[13]

These frauds expose individuals to a range of financial and non-financial harms. In 2019, Australians who experienced the misuse of their personal information spent, on average, 34 non-consecutive hours responding to the incident and taking actions to protect their identity. The estimated average out-of-pocket loss for victims over the same period was nearly AUD

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[6] Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

[7] Privacy Act 1988 (Cth), ss 6 (definition of 'APP entity'), 6C, 6D, 26WE (Privacy Act).

[8] Burdon (n 3), 82-86.

[9] Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (W W Norton & Co 2018) 137-38.

[10] David Lacey and Suresh Cuganesan, 'The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic' (2004) 38(2) Journal of Consumer Affairs 244.

[11] It is more accurately conceived of as "identity usurpation" since the victim loses control of their identification information but is not permanently deprived of their actual identity; however, for the sake of consistency and clarity, the term "identity theft" will be used throughout this paper.

[12] ibid 246-252.

[13] Christie Franks and Russell G Smith, 'Identity Crime and Misuse in Australia: Results of the 2019 Online Survey' (Australian Institute of Criminology, Statistical Report 27, 21 September 2020) <www.aic.gov.au/publications/sr/sr27> accessed 5 February 2021.

4000.[14] Because most credentials do not change over time, victims of identity theft – as well as individuals whose personal information has been compromised but not yet misused – face an ongoing risk of identity theft for months and even years after the initial compromise.[15] Identity theft can lead to wrongful arrests and difficulties obtaining secure employment or credit, and victims may avoid activities that require them to disclose personal information, thereby limiting their capacity to participate meaningfully in society.[16] Victims of identity theft also experience significant emotional and psychological impacts. A University of Texas, Austin, study found that emotional distress, ranging from medium to high levels of emotional trauma, was the impact most commonly reported by victims of identity theft.[17] A recent study of Australian victims of identity misuse identified "mental/emotional distress" as the second-most prevalent consequence after refusal of credit.[18] Victims often report feeling angry, frustrated, violated, untrusting and unsafe, powerless or helpless, sad and depressed, and betrayed.[19] The emotional and psychological impacts can be sufficiently severe to manifest physical symptoms, including sleep problems, anxiety and nervousness, appetite problems and weight loss, headaches, and gastrointestinal problems.[20]

Identity theft creates significant costs for organisations that authenticate individuals' identities by relying on their personal information and identity credentials; when those credentials are compromised and subsequently used to fraudulently complete transactions, it is the organisations relying on those credentials which typically bear the immediate financial losses. The total estimated cost of identity crime and misuse in Australia in from 1 July 2018 to 30 June 2019 was estimated at AUD 3.1 billion. This figure included AUD 2.1 billion in direct costs and AUD 1 billion in indirect costs (indirect costs included intangible harms, lost output and prevention and response costs).[21] Safeguards can be implemented to reduce the risk of identity theft – for example, Australia has implemented a 100-point identity check method, which is used by organisations to verify an individual's identity and prevent financial fraud. Different identity credentials are prescribed different values (a passport and birth certificate are each worth 50 points, a driver licence is worth 60 points, and a Medicare card is worth 40 points).[22] In order to complete significant actions or transactions, particularly establishing new financial accounts, individuals are required to present 100 points of identity credentials. While the 100-point system is intended to reduce the risk of identity theft and financial fraud, full 100-point identity packages can be purchased through dark net markets for relatively small sums.[23] The problem of personal information compromise and identity theft thus remains unresolved.

3. The role of MDBN laws

There is a well-established relationship between data breaches and identity theft. A 2019 survey of identity misuse in Australia found that in 11.7 per cent of occasions where personal information was misused, the personal information was obtained through a data breach. The actual figure was likely higher; 12.1 per cent of respondents did not know how their personal information was obtained. Moreover, the majority of identity misuse events occurred where personal information was obtained through the theft or hacking of a computer or device (30.3 per cent), email (21.5 per cent), or via telephone or text message (17.3 per cent).[24] These methods of personal information compromise are typically the result of phishing attacks. While data breaches are by no means the sole cause of phishing attacks, such attacks are known to occur following breaches involving individuals' contact information; scammers use this limited personal information to contact the relevant individuals, purporting to represent the breached organisation or another entity. Under this pretext, a scammer may obtain access to more valuable forms of personal information, infect a user's device with malware (including ransomware), or obtain access to an individual's computer (for example, by purporting to represent a telecommunications or IT services provider and requesting remote access to the individual's device).[25]

[14] ibid.

[15] IDCARE, 'Beyond the Breach: How Post-Notification has Become the Real Race' (July 2020) 2-3 (Beyond the Breach); Megan Wyre, David Lacey and Kathy Allan, 'The Identity Theft Response System' (Australian Institute of Criminology, Trends & Issues in Crime and Criminal Justice 592, 14 July 2020) <www.aic.gov.au/publications/tandi/tandi592> accessed 5 February 2021.

[16] Lacey and Cuganesan (n 10) 244; Brendan St Amant, 'The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches' (2007) 44(2) Harv J on Legis 505, 508-9; Penny Jorna and Russell G Smith, 'Identity Crime and Misuse in Australia 2017' (Australian Institute of Criminology, Statistical Report 10, 10 August 2018) <www.aic.gov.au/publications/sr/sr10> accessed 5 February 2021.

[17] Jim Zeiss and others, '2019 International Identity Theft Assessment and Prediction Report' (University of Texas at Austin Center for Identity, July 2019) <https://identity.utexas.edu/sites/default/files/2020-09/CID_ITAP_Report_2019.pdf> accessed 5 February 2021.

[18] Franks and Smith (n 13) 29.

[19] Identity Theft Resource Centre, 'The Aftermath: The Non-Economic Impacts of Identity Theft' (2018) <www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf> accessed 4 February 2021.

[20] Tracy Sharp and others, 'Exploring the Psychological and Somatic Impact of Identity Theft' (2004) 49(1) J Forensic Sci 1, 2-3.

[21] Russell G Smith and Christie Franks, 'Counting the Costs of Identity Crime and Misuse in Australia, 2018-19' (Australian Institute of Criminology, Statistical Report 28, 21 September 2020) <www.aic.gov.au/publications/sr/sr28> accessed 5 February 2021.

[22] Financial Transaction Reports Regulation 2019 (Cth), ss 9-10; Financial Transaction Reports Act 1988 (Cth), s 20A.

[23] Christie Franks and Russell G Smith, 'Identity Crime and Misuse in Australia 2019' (Australian Institute of Criminology, Statistical Report 29, 21 September 2020) <www.aic.gov.au/publications/sr/sr29> accessed 5 February 2021.

[24] Franks and Smith (n 13) 20.

[25] Pedro Tavares, 'Spear-Phishing is the Next Threat After a Data Breach' (*Cyber Defence Magazine*, 27 March 2019) <www.cyberdefensemagazine.com/spear-phishing-is-the-next-threat-after-a-data-breach/> accessed 5 February 2021; Office of the

Several objectives converge in the enactment of MDBN laws, including the promotion of transparent data management practices, and incentivising organisations to improve their privacy and data security practices so as to prevent data breaches from occurring.[26] Without a legal requirement to do so, organisations have strong disincentives to reporting data breaches; they may experience public embarrassment and reputational damage, and may face legal action either from regulators or from individuals affected by the breach – particularly if the occurrence of the data breach can be attributed to the failure of the organisation to implement appropriate information security controls.[27] Thus, by enacting a requirement for entities to report data breaches, MDBN laws encourage entities to avoid the occurrence of such breaches and, when breaches do occur, to take steps to mitigate the risks faced by affected individuals.

The "primary rationale"[28] and "key objective"[29] of Australia's law, however, is to mitigate the potential harm to affected individuals following a data breach, foremost of which is identity theft.[30] By requiring breached organisations to notify individuals of the compromise of their personal information, the law aims to place individuals in a position where they can take measures to protect themselves from the misuse of their personal information.[31] These measures may include changing passwords, implementing additional security measures across financial and other accounts, cancelling credit cards and having them reissued, being alert for phishing attacks, and obtaining credit reports and credit reporting bans to identify and prevent any fraudulent credit applications.

4. The scope of MDBN laws

There are typically four elements or criteria that determine the scope of any given MDBN law.[32] The first criterion is the types of personal information that, when subject to unauthorised access or disclosure, may require notification. Under the Australian Privacy Act 1988 (Cth) (the Privacy Act), "personal information" is defined relatively broadly to include "information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not."[33] Other MDBN laws apply more narrowly to types or combinations of personal information that are particularly susceptible to misuse. California's law, for example, applies to "computerized data that includes [unencrypted] personal information." "Personal information" is defined to only include an individual's first name (or first initial) and last name in combination with particular types of personal information, such as an individual's social security, driver's license, tax identification or passport number, or an individual's account, credit card or debit card number in combination with any security or access code or password that would permit access to an individual's financial account, or an individual's medical information, or an individual's biometric data. "Personal information" also includes an individual's user name or email address in combination with their password or security question and answer that would permit access to an online account.[34]

The second criterion identifies the entities to which the law applies. The law may apply to all businesses and government agencies,[35] or there may be exemptions. Australia's MDBN law applies to entities already regulated under the Privacy Act: Australian Privacy Principle (APP) entities. APP entities include federal government agencies and private sector organisations with an annual turnover in excess of AUD 3 million. Most businesses with a turnover of AUD 3 million or less are exempt (the small business exemption), and are only considered APP entities if they fall within certain categories – for example, health service providers, organisations that trade in personal information, or organisations that are contracted service providers for a federal government contract.[36] Certain organisations, such as registered political parties and state and territory government authorities, are exempt regardless of their annual turnover.[37] APP entities are named as such because their primary obligation under the Act is compliance with the Australian Privacy Principles (APPs). The APPs set out principle-based standards for the collection and handling of personal information. Organisations excluded from the definition of "APP entity" are thus exempt from compliance with both the APPs and the MDBN scheme.

Australian Information Commissioner, 'Notifiable Data Breaches Scheme 12-Month Insights Report' (13 May 2019), 15 <www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf> accessed 4 February 2021 (Insights Report).

[26] Australian Law Reform Commission, (n 3) 1670, 1688-89; Burdon (n 3) 78-80; Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth), 25 [114], [116], 26 [119], 35 [171] (Explanatory Memorandum to the Notifiable Data Breaches Bill).

[27] Ross Schulman, 'Disincentives to Data Breach: Problems with Notification and Future Legislative Possibilities' (2009) 1 Legis & Pol'y Rountable 54, 58-59; Nieuwesteeg and Faure (n 4) 1238-39.

[28] Australian Law Reform Commission (n 3) 1688.

[29] Explanatory Memorandum to the Notifiable Data Breaches Bill, 25 [113].

[30] ibid, 14 [62], 17-18 [75]-[80], 54 [263]-[265]; Australian Law Reform Commission (n 3) 1688-89.

[31] Explanatory Memorandum to the Notifiable Data Breaches Bill, 25 [113]; Australian Law Reform Commission, (n 3) 1669; Office of the Australian Information Commissioner, 'Data Breach Preparedness and Response: A Guide to Managing Data Breaches in Accordance with the Privacy Act 1988 (Cth)' (July 2019), 9 <www.oaic.gov.au/assets/privacy/guidance-and-advice/data-breach-preparation-and-response.pdf> accessed 4 February 2021 (Data Breach Preparedness); Commonwealth, *Parliamentary Debates*, House of Representatives, 19 October 2016, 2430 (Michael Keenan).

[32] Amant (n 16) 510-11; Sara Smyth, 'Does Australia Really Need Mandatory Data Breach Notification Laws – and if so, What Kind? (2012) 22(2) Journal of Law, Information and Science 159, 161.

[33] Privacy Act, s 6 (definition of 'personal information').

[34] Cal Civ Code §§ 1798.29, 1798.82.

[35] See, for example, Cal Civ Code §§ 1798.29, 1798.82.

[36] Privacy Act, s 6D(4).

[37] ibid s 6C(1).

The third criterion of MDBN laws specifies the circumstances in which notification must occur. Notification may be required where there is unauthorised access to, or disclosure of any personal information, or it may only be required where there is a certain risk of harm to the individuals concerned (the notification threshold). The former is more commonly found in jurisdictions such as California, where personal information is narrowly defined to only include specific types or combinations that are likely to enable identity theft or misuse. Where personal information is defined more broadly, the notification threshold is crucial as it is the primary determinant of whether or not a data breach is sufficiently serious to require notification. Under the Privacy Act, notification is required for "eligible data breaches"; that is, where a data breach occurs "and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates" (the serious harm test).[38]

Finally, MDBN laws typically specify the requirements for notification – who must be notified, how they must be notified, the time within which they must be notified, and what information must be included as part of the notification. Under the Privacy Act, if an APP entity has reasonable grounds to suspect that an eligible data breach has occurred, it must carry out an assessment to determine if an eligible data breach has occurred. The entity must take all reasonable steps to ensure the assessment is completed within 30 days.[39] If the entity is aware that there are reasonable grounds to believe that the data breach is an eligible data breach, it must notify the Office of the Australian Information Commissioner (OAIC)[40] and the individuals at risk of serious harm (alternatively, if it is not practicable to notify the individuals at risk, the entity can publish a copy of the notification statement on its website and take reasonable steps to publicise the statement).[41] These steps must be completed as soon as practicable.[42] The notification statement must include the identity and contact details of the entity, a description of the data breach and the types of personal information involved, and recommendations about the steps that individuals should take in response to the breach.[43]

5. Assessing harm under Australia's MDBN law

The preceding discussion may have given the impression that Australia's MDBN law is – with the possible exception of the way in which the Privacy Act determines which entities are subject to the scheme – reasonably intuitive and prescriptive. This is not the case. The uncertainty surrounding the notification threshold and how APP entities should assess the risk of "serious harm" has largely negated the objectives of the scheme. The legislative intention behind the serious harm test was to establish a high notification threshold so as to reduce compliance costs for APP entities and avoid unnecessary notification.[44] Another objective was to reduce the risk of notification fatigue; if individuals receive notifications for data breaches that do not present a serious risk, they are less likely to pay attention to more urgent notifications and to take the necessary steps to protect themselves from identity theft or other harms.[45] In practice, however, the MDBN scheme has operated far more expansively than intended. This is largely due to the failure to define clearly the scope of "serious harm." Section 26WG provides a list of factors intended to guide organisations when assessing the risk of harm. These factors include: the kinds of information and the sensitivity of information involved in the breach; whether the information is encrypted or protected by other security measures and whether the encryption or those security measures could be circumvented or overcome; the person or persons who obtained or could obtain access to the information; the nature of the potential harm; and "any other relevant matters."[46] There is no indication of the relative importance of each factor, or how they ought to be weighed. The inclusion of "any other relevant matters" as a relevant consideration is indicative of the indeterminate nature of this guidance; APP entities are effectively advised to consider all of the relevant circumstances surrounding the data breach.

No guidance is provided on the distinction between harm *per se* and "serious" harm. (No organisation, presumably, would want to be in the position of explaining that, while it thought "harm" to affected individuals was a likely consequence of a data breach, it decided against notification on the basis that it did not deem the harm to be sufficiently "serious".) Nevertheless, the explanatory materials accompanying the legislation insist that not all breaches should result in notification – mere distress or upset at the unauthorised access to or disclosure of personal information will generally not require notification.[47] That said, serious harm can arise in multiple ways and contexts. "Serious harm" can include physical, psychological, emotional, economic, financial and reputational harm.[48] These harms are not limited to circumstances involving the risk of identity theft. They may occur in the context of "stalking, embarrassment, or discrimination,"[49] as well as loss of business or employment opportunities, humiliation and damage to reputation or relationships, and workplace bullying or social marginalisation.[50] In some instances, a data breach may result in serious harm simply by revealing the fact that an individual accessed a particular service or engaged

[38] ibid s 26WE(2).
[39] ibid s 26WH(2).
[40] ibid s 26WK(2)(a)(ii).
[41] ibid s 26WL(2).
[42] ibid s 26WK(2)(b), 26WL(3).
[43] ibid s 26WK(3).

[44] Explanatory Memorandum to the Notifiable Data Breaches Bill, 38 [184], 65-66 [7], 71 [34], 81 [90].
[45] ibid 4 [11], 28-29 [131]-[132], 65-66 [7]; Nieuwesteeg and Faure (n 4) 1237.
[46] Privacy Act, s 26WG.
[47] Explanatory Memorandum to the Notifiable Data Breaches Bill, 3 [9], 4 [11].
[48] ibid 3 [9]; Office of the Australian Information Commissioner, 'Data Breach Preparedness' (n 31) 33.
[49] Explanatory Memorandum to the Notifiable Data Breaches Bill, 13 [60].
[50] Office of the Australian Information Commissioner, 'Data Breach Preparedness' (n 31) 36.

with a particular business.[51] Serious harm in the form of emotional, psychological or reputational harm may also arise in the disclosure of sensitive types of personal information, such as an individual's health information.[52] In effect, while Australia's MDBN scheme was primarily concerned with the risk of identity theft,[53] the text of the legislation goes far beyond this, both in theory and in practice; the health sector reports more data breaches than any other sector, and contact information is compromised in eligible data breaches more frequently than any other type of personal information (followed by identity information, financial information and health information).[54]

The unauthorised access to or disclosure of contact information illustrates the ambiguity in assessing harm under Australia's MDBN law. While contact information is often compromised in data breaches, it presents no direct or immediate risk of harm. Unlike other, more sensitive, forms of personal information, contact information cannot, on its own, be used to access existing accounts, create new accounts or obtain credit, nor is it a source of reputational harm or embarrassment. (One exception to this general rule would be where the very fact of the individual having accessed a particular service would result in reputational harm. The Ashley Madison data breach of July 2015, which revealed the identities of individuals who had accessed the service for the purpose of extramarital affairs, is one such example.[55]) Nevertheless, while contact information generally does not present an immediate risk of misuse it can lead to serious harm, including identity theft; as discussed earlier, scammers may use this information to obtain access to more valuable forms of personal information, often through spearphishing attacks. The OAIC has indicated that notification is required in such instances.[56] This would suggest that data breaches involving most types and combinations of personal information may require notification, the only clear exception being where the breach is not the result of malicious action by a third party, but is a single, accidental disclosure to an unsuspecting third party who has no malicious intent.

The expansive meaning of "serious harm" results in striking inconsistencies: while many data breaches that do not present an immediate or obvious risk of identity theft require notification, the small business exemption under the Privacy Act – an exemption not found in comparable jurisdictions and one that is estimated to account for 94 per cent of Australian enterprises[57] – means that, in many circumstances where a data breach does present a clear or immediate risk of identity theft, no notification is required. Moreover, because organisations that are exempt from the MDBN scheme are also exempt from the APPs, they are less likely to have implemented reasonable information security protections, and may therefore be more susceptible to the occurrence of serious data breaches.[58]

6. Conceptual inconsistencies underlying australia's mdbn law

The current state of Australia's MDBN law appears to result, in part, from a seemingly flawed interpretation of comparable schemes. The explanatory memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth), which introduced the MDBN scheme under the Privacy Act, stated that the chosen notification threshold meant "notification would be required less often compared to jurisdictions such as California and the European Union."[59] At least in the case of California, a close reading of the law suggests this is not the case. As noted earlier, while California's law does not include a notification threshold, "personal information" is defined to only include specific combinations of personal information, which significantly narrows the law's scope. The Californian law also applies only to "computerized data" – in other words, it excludes data breaches that involve physical documents or files.[60] (The contrast between the Privacy Act and the GDPR is less stark, the latter adopting a broad definition of "personal data" and requiring notification when a data breach "is likely to result in a high risk to the rights and freedoms of natural persons."[61])

The drafters of Australia's MDBN law also opted not to adopt an earlier proposal put forward by the Australian Law Reform Commission (ALRC).[62] In 2008 the ALRC recommended mandatory reporting of data breaches where there

[51] Explanatory Memorandum to the Notifiable Data Breaches Bill, 77 [66].
[52] ibid 73 [42].
[53] ibid 2 [3], 14 [62], 16-18 [72]-[81], 24 [107], 45 [220], 54 [263].
[54] Office of the Australian Information Commissioner, 'Insights Report' (n 25) 13-14; Office of the Australian Information Commissioner, 'Notifiable Data Breaches Report: July-December 2020' (28 January 2021) 3, 5, 9-10 <www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/2020-2/Notifiable-Data-Breaches-Report-July-Dec-2020.pdf> accessed 5 February 2021 (July-December 2020 Report)
[55] Office of the Australian Information Commissioner, 'Ashley Madison Joint Investigation' (24 August 2016) <www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/ashley-madison-joint-investigation/> accessed 12 February 2021.
[56] Office of the Australian Information Commissioner, 'Insights Report' (n 25) 15; Office of the Australian Information Commissioner, 'Data Breach Preparedness' (n 31) 39.
[57] Explanatory Memorandum to the Notifiable Data Breaches Bill, 38 [184].
[58] It is relevant to note that the Privacy Act is currently under review. The scope and application of the Act are being considered as part of the review. However, while the Issues Paper considers the removal of the small business exemption, it does so in the context of considering APP compliance. The question of whether small businesses ought to comply with the MDBN scheme is not explicitly addressed. See Australian Government, Attorney-General's Department, 'Privacy Act Review: Issues Paper' (October 2020) <www.ag.gov.au/system/files/2020-10/privacy-act-review–issues-paper-october-2020.pdf> accessed 12 February 2021.
[59] Explanatory Memorandum to the Notifiable Data Breaches Bill, 40-41 [197].
[60] Cal Civ Code §§ 1798.29, 1798.82.
[61] GDPR, arts 4(1), 34(1).
[62] The Minister of Justice drew particular attention to pre-legislative policy consultation with the ALRC when commending the Privacy Amendment (Notifiable Data Breaches) Bill to Parliament in his Second Reading speech: Commonwealth, *Parliamentary Debates*, House of Representatives, 19 October 2016, 2430 (Michael Keenan). The findings of the ALRC's report also featured

was "a real risk of serious harm to any affected individual."[63] This formulation was intended to set a sufficiently high threshold to reduce the compliance burden on organisations and the risk of notification fatigue,[64] but it was rejected on the grounds that the phrase "real risk" lacked sufficient certainty. The concern was that entities might adopt "a more risk adverse approach to notification by taking a narrow interpretation that could lead to notification fatigue and create resourcing issues at the OAIC."[65] The substitution of the "reasonable person" test and "likely risk" threshold were intended to address this risk by providing more certainty and reducing notifications.[66] As highlighted previously, the present scheme – and particularly the notification threshold – fails to provide much certainty. Furthermore, because of the broad definition of "personal information" adopted under the Privacy Act as compared to that recommended by the ALRC, it is likely that the current scheme results in more notifications than would have been the case under the ALRC's proposal. The ALRC recommended adopting the concept of "specified personal information" for the purposes of the MDBN scheme. Notification would only be required where particular types and combinations of personal information were compromised, such as an individual's name or address in combination with one of the following: their driver's licence, a unique identifier such as their Medicare number or tax file number, their account numbers or their credit or debit card numbers together with any access codes that would permit access to the individual's information, and "sensitive information" as defined under the Privacy Act, which includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, and criminal record, as well as an individual's health information.[67]

In effect, the definition of specified personal information aimed to address the primary risk of identity theft, while also, through the incorporation of the definition of "sensitive information," recognising many of the other harms that can stem from the unauthorised acquisition of personal information, including humiliation, reputational harm, and discrimination.[68] To use the example discussed earlier, the Ashley Madison data breach would likely fall within scope, since "sensitive information" includes information about an individual's "sexual orientation or practices."[69] The adoption of the ALRC's concept of "specified personal information" might have been accompanied by disadvantages. The exclusion of some types of personal information, particularly contact information, could present a risk of serious harm in certain circumstances – for example, an individual fleeing an abusive partner may be at risk of serious harm if their name and address were disclosed. (That said, if an organisation was aware of such circumstances, they would arguably owe a duty of care to notify such individuals regardless of whether notification was required under the MDBN scheme.) Incorporating the concept of "specified personal information" would have also complicated the operation of the Privacy Act by effectively introducing a second definition of personal information. For present purposes, however, what is relevant is the deviation from the ALRC's proposal by the drafters of Australia's current law, and the reason for this deviation. The ALRC's proposal was rejected in pursuit of providing organisations with certainty and reduced compliance costs, and preventing unnecessary notifications and notification fatigue. In practice, the version passed by parliament is more ambiguous and has a broader scope, likely leading to greater compliance costs and more notifications.

7. Deficiency of notification as a remedy to data breaches

The preceding analysis described the inconsistencies and apparent contradictions in the purpose and formulation of Australia's MDBN law. The following discussion will highlight the law's failure to reflect the realities of the data breach response process and address the needs of affected individuals.

7.1. *Notification as an end in itself*

As the name suggests, MDBN laws are primarily concerned with the *notification* of data breaches. In the case of Australia's law in particular, notification is effectively defined as an end in itself; once an APP entity has notified the regulator and affected individuals of the data breach in accordance with the requirements of ss 26WK-26WL, that organisation can be said to have fulfilled its legal obligations. There is no further responsibility to mitigate harm – whether by providing credit monitoring services or identity theft protection services, setting up dedicated communication channels to address affected individuals' questions or concerns, or referring affected individuals to relevant third party organisations, such as credit reporting agencies or entities that provide specialised advice or counselling. The law's preoccupation with notification tends to narrow organisations' focus to the question of regulatory compliance, rather than prioritising the substantive objectives underlying the law: the avoidance and mitigation of harm to individuals, particularly identity theft. This shift in perspective manifests in various ways – for example, APP entities notifying the OAIC and affected individuals of data breaches that do not meet the notification threshold.[70] Unnecessary notification carries little regulatory risk for APP entities and, given the ambiguity of the notification threshold and the repercussions that may stem from an incorrect decision not to notify, risk-averse organisations may view an approach of "if in doubt, notify" as the safest strategy. However,

prominently in the explanatory memorandum, which asserted that the model adopted was "retaining the core elements of the ALRC's recommended test while improving ease of compliance for regulated entities": Explanatory Memorandum to the Notifiable Data Breaches Bill, 29 [132].

[63] Australian Law Reform Commission (n 3) 1690 [51.83].

[64] ibid 1691 [51.86].

[65] Explanatory Memorandum to the Notifiable Data Breaches Bill, 28 [131].

[66] ibid 29 [132].

[67] Australian Law Reform Commission (n 3) 1693-94 [51.96]-[51.97].

[68] ibid 1694 [51.98].

[69] Privacy Act, s 6 (definition of 'sensitive information').

[70] Office of the Australian Information Commissioner, 'Insights Report' (n 25) 8.

unnecessary notification causes its own type of harm. Individuals often have a strong negative reaction to the news that their personal information has been compromised in a data breach. Common reactions include feelings of stress, panic and anxiety.[71] Unnecessary notification is also likely to result in notification fatigue. Thus, while one of the aims of Australia's MDBN law was to avoid notification in circumstances where there was little risk of harm to individuals and to avoid causing unnecessary anxiety, the ambiguity of the notification threshold has, to some extent, resulted in the opposite.

7.2. *Inadequate notifications*

In other instances, organisations have provided unclear, confusing, insufficient, or incorrect information in their notifications. For example, they have provided a notification statement that indicates a low level of risk to affected individuals, while simultaneously advising individuals to undertake a number of preventative measures which suggest a high level of risk.[72] On other occasions, organisations have failed to clearly identify the types of personal information compromised in the breach, or the steps individuals should take to protect themselves.[73] Some entities have advised individuals to take steps that are either not possible or of limited utility. In the case of driver's licences, one of the most commonly targeted credentials for identity theft in Australia,[74] some organisations have advised individuals across Australia to seek the reissue of their licence with a new number, when this measure is only possible in particular states and territories.[75] Even in those jurisdictions where it is possible, individuals are required to provide proof that their licence has been misused.[76] The OAIC has suggested that organisations' maturity in assessing harm must develop.[77] However, for many organisations, more guidance is needed on how to respond to breaches and what advice to provide to affected individuals. Most organisations lack the expertise and experience required to carry out a response that adequately addresses the needs of affected individuals. They would likely benefit (as would individuals) from greater assistance in identifying what risks the compromise of particular types of personal information present, what steps individuals can take to address those risks, and how organisations should seek to support those individuals.[78] That said, there is no definitive best practice guide to data breach response; regulators, too, are developing maturity in this area. The expertise and experience necessary to inform official guidance and so provide greater assistance can be accumulated through MDBN scheme compliance, and this objective was acknowledged in the enactment of Australia's MDBN law.[79] (Viewed in this context, significant omissions or exemptions from such schemes present a knowledge gap vulnerability for policy-makers, regulators and data mangers alike.) Nevertheless, in the absence of such guidance, organisations are likely to continue focusing on meeting the minimum requirements of notification, rather than addressing the ultimate objectives of the law by actively assisting or supporting individuals to mitigate the harm stemming from a data breach.

7.3. *Premature and progressive notifications*

A further shortcoming in the practical application of the MDBN scheme is the occurrence of premature notifications; that is, organisations informing affected individuals of a data breach before completing a thorough assessment of the breach and the risks it presents.[80] This can also result in progressive notifications – multiple notifications that contain varying or conflicting information and advice. Progressive notification can result in further harm to affected individuals, as it conveys a sense of uncertainty or instability in the status of individuals' personal information, resulting in additional stress and anxiety.[81] (One exception to this is where each notification is seen to build upon the preceding notifications, rather than contradicting or retracting previous advice.) The phenomena of premature and progressive notifications may be driven, in part, by the legislative timeframes for notification as interpreted by the OAIC. As noted earlier, the Privacy Act requires APP entities assessing a suspected data breach to "take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware" that there are reasonable grounds to suspect an eligible data breach may have occurred.[82] If it is an eligible data breach, the entity must proceed to notification as soon as practicable.[83] In its guide to data breach response, the OAIC says it "expects that wherever possible entities treat

[71] Office of the Australian Information Commissioner, 'Data Breach Preparedness' (n 31) 21; IDCARE, *Beyond the Breach* (n 15) 9.

[72] Office of the Australian Information Commissioner, 'Insights Report' (n 25) 20.

[73] Office of the Australian Information Commissioner, 'July-December 2020 Report' (n 54) 15; Office of the Australian Information Commissioner, 'Notifiable Data Breaches Report: July-December 2019' (28 February 2020) 8 <www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-July-December-2019.pdf> accessed 5 February 2021.

[74] Jorna and Smith (n 16) 24.

[75] IDCARE, *Beyond the Breach* (n 15) 3.

[76] Franks and Smith (n 23) 26-27.

[77] Office of the Australian Information Commissioner, 'Insights Report' (n 25) 15.

[78] IDCARE, Submission to the Commonwealth Government's 2020 Privacy Act Review (November 2020) 6-7 <https://www.ag.gov.au/sites/default/files/2020-12/idcare.PDF> accessed 28 February 2021.

[79] Explanatory Memorandum to the Notifiable Data Breaches Bill, 25 [115].

[80] IDCARE, *Beyond the Breach* (n 15) 4; Office of the Australian Information Commissioner, 'Notifiable Data Breaches Report: January-June 2020' (31 July 2020) 7 <www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-Jan-Jun-2020.pdf> accessed 5 February 2021.

[81] IDCARE, *Beyond the Breach* (n 15) 4, 7.

[82] Privacy Act s 26WH(2)(b). As a point of comparison, the GDPR (art 33(1)) requires notification to the relevant regulatory authority within a much shorter timeframe: "without undue delay and, where feasible, not later than 72 hours after having become aware of [the personal data breach]." When notification occurs after 72 hours, a reason must be provided for the delay.

[83] Privacy Act, ss 26WH(2), 26WK(2)(a)(ii).

30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time."[84] This advice is inconsistent with the explanatory memorandum to the MDBN law, which states that the 30-day timeframe reflects "a preferable timeframe in which an assessment should be undertaken wherever possible, though importantly it does not require entities to complete an assessment within 30 days."[85] The reason for this flexibility is that, in the case of large and complex data breaches, 30 days may not provide enough time to carry out a proper assessment.[86] What appears to be occurring is that organisations are instead providing incomplete and multiple notifications. While there are valid reasons for insisting on prompt notification – the likelihood of misuse occurring increases the longer notification is delayed – the current regulatory advice does not reflect legislative intent, and may be leading to additional issues in the application of the scheme.

7.4. *The data breach response system*

The most significant impediment to the effective operation of Australia's MDBN law is the efficacy of the response system that affected individuals navigate following notification. Regardless of how effective or prompt notification is, individuals almost always face difficulties in trying to secure their personal information from misuse. Following notification, the affected individual, not the breached organisation, is responsible for securing their personal information and identity from misuse. This process may include contact with financial institutions, government agencies, law enforcement, telecommunications providers, and credit reporting agencies. Individuals are required to act as intermediary, receiving and sharing information between entities, as most of these organisations do not communicate with each other directly.[87] Where identity misuse occurs, individuals have been found to spend, on average, 34 non-consecutive hours responding to the fraud.[88] The response process can involve a combination of 63 different tasks, including those identified above. No other crime type requires so much reporting or communication on the part of the victim.[89] These tasks and responsibilities fall to the affected individual – despite the fact that the breached organisation was the entity responsible for securing the personal information and, as an APP entity, is required to take reasonable steps to protect the personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.[90] Moreover, many of the steps taken by the individual serve to protect organisations from loss; in the event the individual's personal information is fraudulently relied upon to obtain access to goods or services, it is the organisations providing those goods or services that will usually bear the resultant loss. Consequently, the primary harm to affected individuals following a data breach stems not from the actual financial consequences of the data breach (such as through identity theft), but through the time, money and stress expended in contacting organisations to protect one's identity.[91] Harm is even more likely where the information and advice received by individuals is incorrect or inaccurate.

8. Options for reform

The observations and critiques made thus far can be summarised as follows. First, the primary objective of Australia's MDBN law was to mitigate the risk of identity theft following data breaches that exposed personal information. The wording of the law and regulatory guidance go far beyond this, contemplating notification in many other circumstances. Conversely, the exemption of most Australian businesses from the scheme means that in many instances in which identity theft is a likely risk, notification is not required. Second, the purpose of the high notification threshold, and the reason for deviating from the ALRC's recommended formulation, was to reduce the compliance burden on organisations and to ensure that individuals did not receive excessive or unnecessary notifications. In practice, the ambiguity of the phrase "serious harm" and the broad scope of "personal information," as well as the lack of guidance surrounding the assessment of harm and the regulator's interpretation of the 30-day assessment period, make it more likely that organisations will proceed to notification when doing is unnecessary or before conducting a thorough assessment of the breach. Third, the purpose of the scheme was to reduce the harm flowing to individuals following a data breach. Instead, individuals are liable to receive unnecessary, inaccurate or incomplete notifications, and are often left to take primary responsibility for protecting their personal information from misuse – despite them being in no way responsible for the data breach. There are several ways in which some or all of these issues may be addressed.

8.1. *Two-tiered notification*

The incidence of unnecessary notification could be reduced by providing for a more active role by the regulator. A two-tiered system for notification, whereby a lower risk of harm required notification to the regulator (as opposed to notifying affected individuals), would enable organisations that were unsure of the risk of harm to first consult with the OAIC. The GDPR provides a model: entities are required to notify the regulator of data breaches unless the breach "is unlikely to result in a risk to the rights and freedoms of natural persons."[92] Notification to individuals is only required where the data breach "is likely to result in a high risk to the rights and freedoms of natural persons."[93] If a regulated entity incorrectly decides that notifi-

[84] Office of the Australian Information Commissioner, 'Data Breach Preparedness' (n 31) 46.
[85] Explanatory Memorandum to the Notifiable Data Breaches Bill, 83 [98].
[86] ibid.
[87] Wyre, Lacey and Allan, (n 15) 9.
[88] Franks and Smith (n 13) xiii.
[89] Franks and Smith (n 23) 41.
[90] Privacy Act, sch 1 cl 11.1.
[91] Emily Matta, 'Kansans at Risk: Strengthened Data Breach Notification Laws as a Deterrent to Reckless Data Storage' (2019) 67(4) U Kan L Rev 823, 840.
[92] GPDR, art 33(1).
[93] ibid, art 34 (1).

cation to individuals is not required, the regulator can compel notification.[94]

An alternative model, and one suggested by the ALRC, would be maintain a single threshold for notification to both the regulator and to affected individuals, but to enable organisations to consult with the regulator before proceeding to notify affected individuals.[95] Either option would require more oversight and resourcing on the part of the OAIC; however, it would curb excessive notification while providing reassurance to breached organisations. It may enable the OAIC to encourage organisations to carry out more thorough assessments in circumstances where they have incomplete information. The first model would also provide the OAIC with a more holistic view of the data breach landscape. This in turn could facilitate more accurate and relevant advice for organisations.[96]

8.2. *The scope of "personal information"*

An alternative reform, and one that could be taken in addition to the preceding option, would be to narrow the types of personal information that potentially require notification. This would narrow the scope of the MDBN scheme and potentially reduce the uncertainty associated with its operation. As highlighted previously, the disadvantage of this option would be to complicate the broader application and scope of the Privacy Act, as it would effectively introduce a second definition of personal information. Given the already convoluted process of determining whether an organisation is an APP entity, introducing different definitions or lists of personal information may only add to the inconsistency and opacity of the legislation. A second risk is that the types of personal information identified as requiring notification may be excessively narrow or broad. It is not possible to accurately foresee the different ways in which personal information will be used and misused; personal information that is innocuous in one context may be devastating in another. The Ashley Madison data breach is an example of this principle. The publication of individuals' personal and contact information would, in other contexts, not have been harmful. The advantage of a "context dependant" assessment of harm is the recognition that the nature and significance of personal information must be determined by considering the social context within which the personal information is used.[97] (That said, it is questionable how useful notification to affected individuals would have been in such a situation, aside from giving them advanced notice of the impending harm to their reputations.) An alternative to this approach, and one that would involve less consultation and legislative action, would be for the regulator to provide clearer guidance on the meaning (or, more precisely, its interpretation) of "serious harm," the distinction between serious and non-serious harm, and guidance on how to assess harm and assist affected individuals. Organisations may also be assisted if the OAIC's guidance on the 30-day assessment period was updated to reflect the legislative intention.

8.3. *Coordinating the response system*

The above measures may all go some distance to improving the clarity and consistency of Australia's MDBN law. Nevertheless, a fundamental defect may remain: most of the harm to affected individuals occurs subsequent to notification. Individuals are left primarily responsible for protecting their personal information from misuse, and doing so involves an inordinate amount of complexity and time. This problem could be addressed in several ways. Firstly, clarifying the threshold for notification may reduce unnecessary notifications, and a more active role by the regulator may ensure individuals receive informative and accurate notifications, and specific advice. Even so, MDBN laws do not reflect the reality of the response process; notification marks the start of the process, not the end. Part of the problem (and the solution) lies in the capabilities of the organisations that individuals contact subsequent to notification. Many of these organisations do not (or cannot) communicate with each other, significantly increasing the onus on individuals. Some organisations also lack the necessary capabilities – as apparent in the earlier discussion of reissuing driver licences.

Several US states provide examples of alternative approaches to notification and mitigation. Many states require organisations to notify credit reporting agencies following a large-scale data breach (for example, where a breach affects more than 1000 individuals).[98] A smaller number of states require breached organisations to investigate whether personal information misuse has in fact occurred.[99] Some states also include specific requirements on what to include in a notification – for example, entities may be required to provide consumers with information about remediation services available, including the contact details of credit reporting agencies, how to obtain a credit reporting freeze, as well as information about a consumer's ability to file or obtain a police report.[100] These measures could be adapted to varying extents in Australia; given the expansive application of "personal information" and "serious harm," not all data breaches would necessarily require referrals to law enforcement or credit reporting agencies. It may also be reasonable to set the threshold for contacting credit reporting agencies at a lower number than 1000 affected individuals.

9. Conclusion

There are significant variations between different MDBN schemes, including the types of personal information re-

[94] ibid, art 34(4).

[95] Australian Law Reform Commission (n 3) 1691 [51.88].

[96] Paul M Schwartz and Edward J Janger, 'Notification of Data Security Breaches' (2007) 105 Mich L Rev 913, 966-68.

[97] Mark Burdon, Bill Lane and Paul von Nessen, 'Data Breach Notification Law in the EU and Australia – Where to Now?' (2012) 28(3) Computer Law & Security Review 296, 302-3.

[98] See, for example, Kan Stat Ann § 50-7a02(f). For an overview of the various MDBN laws in force across the US, see National Conference of State Legislatures, 'Security Breach Notification Laws' (17 August 2020) <https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> accessed 22 February 2021.

[99] See, for example, NH Rev Stat § 359-C:20(I)(a).

[100] See, for example, RI Gen Laws §§ 11-49.3-4.

quiring notification, the range of organisations to which the schemes apply, and the requirements associated with notification, including how notification must occur, who must be notified, and what information must be included as part of a notification. Generally speaking, the more narrowly and specifically a MDBN law applies, the more stringent it can be in its requirements without imposing undue compliance costs on regulated entities. Conversely, broader MDBN schemes require organisations to do more in terms of interpreting notification thresholds and assessing breaches. In other words, if the law only requires notification for data breaches involving types of personal information that readily lend themselves to identity theft, it is not unreasonable for that law to apply to all or most businesses and government agencies. In contrast, where organisations are required to notify consumers and regulators of a wide range of data breaches (for example, those likely to result in "serious harm"), and where difficult questions of legislative interpretation and assessments of harm are involved, it may be reasonable to limit the scope of the law, both in terms of the organisations regulated and the steps they are required to complete subsequent to the breach.

While there are complex considerations and subjective judgments involved in seeking an appropriate balance, Australia's MDBN law is characterised by inconsistencies and contradictions. While the primary objective of the law was to address the risk of identity theft following a data breach, the majority of Australian businesses are not required to notify individuals of data breaches, even where there is a real or likely risk of identity theft or other forms of personal information misuse. Conversely, of the relatively small proportion of organisations required to notify individuals, a broad range of data breaches potentially require notification, and organisations are left to interpret an ambiguous notification threshold, likely leading to unnecessary notifications.

The objective of the law is consumer protection, yet insufficient emphasis has been placed on the supports and capabilities required post-notification. Notification is defined as an end in itself. As a result, most affected individuals receive little support following a data breach. Instead, they often receive unnecessary, incomplete or inaccurate notifications, and are left responsible for securing their personal information. The data breach response process is confusing and stressful, and often causes more harm than the actual compromise of personal information. Many of the measures undertaken by individuals serve to protect other organisations from loss. There are myriad options for legislative reform. Each is attended with its own advantages, costs, and considerations of policy and priority. No clear solution presents itself as superior to all others. Nevertheless, consistency between objective and practice is desirable in the law, and this is currently absent from Australia's MDBN scheme.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.