Louder bark with no bite

Privacy protection through the regulation of mandatory data breach notification in Australia

Alazab, Mamoun; Hong, Seung Hun; Ng, Jenny

Published in:
Future Generation Computer Systems

DOI:
10.1016/j.future.2020.10.017

Published: 01/03/2021

Document Version
Peer reviewed version

Louder Bark with No Bite: Privacy Protection through the Regulation of Mandatory Data Breach Notification in Australia

Abstract

The disruptive shift of technologies in the Internet age poses the challenge of securing our digital asset and cyberspace from large-scale, sophisticatedly targeted offences and cybercrimes. As a response, many governments have introduced mandatory notification schemes in which an entity bears an obligation to notify the regulator and affected individuals if personal data it holds is compromised. Focusing on Australia's Notifiable Data Breach (NDB) scheme introduced in 2018, this paper points out that the NDB scheme gives entities which should be responsible for data protection much leeway while holding individuals, only victims of a data breach, responsible for dealing with the consequences. This is problematic as redressing the grievances caused by a data breach is difficult in the Australian context. It is difficult for a victim of a breach of privacy to bring an action in court mainly because there is no established tort of privacy in Australia. Further, bringing a class action for data breaches is a difficult process. We suggest that the real effect of the NDB scheme requires an understanding in a broader context of Australian Privacy Principles (APPs). Regulated in a broader APPs context, the NDB scheme could become a part of the privacy protection regime that requires public agencies and businesses to have better accountability and responsibility mechanisms.

Keywords

Cybercrime, privacy protection, mandatory notification, notifiable data breach, regulation, tort of privacy

1. Introduction: Risk of personal information leakage

The continued growth of the Internet since the 1990s has resulted in the increasing sophistication of tools and methods to conduct computer attacks and intrusions. Machine Learning and Artificial Intelligence, Robotics, Internet of Things (IoT), Surveillance and Drones, Crypto-currencies and Darknet represent the disruptive shift of technologies in the Internet age. This shift poses the challenge of securing our digital asset and cyberspace from large-scale, sophisticatedly targeted offences, and organised crimes, as highlighted by the widely-respected criminologists Roderic Broadhurst and Peter Grabosky [1-3]. Trends in malicious binaries or computer code designed for financial fraud show increasing complexity around new opportunities arising from automated financial activities. The Internet has become the preferred platform for sending phishing spam emails [4] and deploying malware attacks by exploiting vulnerabilities in software systems and critical applications to disrupt intentionally, or to subvert them. These malicious codes are used to install computer programs that purport to steal sensitive information (to be sold or used later), using the infected victim for sending spam, and installing other malicious codes like fake anti-virus services. These obfuscatory crime tools have far-reaching implications, which need further exploration and investigation [5].

This paper focuses on one of many different types of cybercrimes: data breach or the risk of personal information leakage. Data breach may involve serious cybercrime as a breach of personal identifying information not only imposes considerable costs on individuals and organisations but also deprives of "their right to confidentiality, privacy and integrity of their personal information," which is hardly quantifiable [6]. Data breaches impose financial, reputational, and lost opportunity costs on individuals, organisations and governments. Data breaches may also threaten critical infrastructure and jeopardise national security.

Countries including the United States, Canada, Australia, New Zealand and the European Union have attempted to tackle data breaches by enacting legislation that requires companies and organisations to notify, voluntarily or not, to the regulatory authority if personal data they hold is compromised as a result of data breach [7-9]. The purpose of the legislation, though contents vary, is to alert personal information breach to individuals so that they could take necessary actions to protect their privacy from identity theft. The legislation is a significant improvement in privacy protection and data security, as literally speaking all of our personal information is kept online.

The legislation has attracted criticism as well as attention. Romanosky et al. [10] argue that data breach notification laws are effective in preventing data breach, reporting that those state laws in the United States reduced identify theft by 6.1 per cent. Others criticise that individuals, after being notified of a data breach, fall short of significant means to rectify breach of their privacy against companies [11] or that imposing 'voluntary' duty for data breach notification to organisations become a hardly effective way of regulating it [6]. Notwithstanding previous studies on the effectiveness of data breach legislation, however, the regulatory aspect of those reforms has seldom received scholarly attention. This is partly because data breach regulation is a relatively new field of regulation which has rarely explored and trialled. This paper explores the regulatory aspect of the recent legal reform in Australia that introduces the Notifiable Data Breaches (NDB) scheme, focusing on whether the new mandatory scheme is designed to assure privacy protection better than the previous voluntary scheme.

The NDB scheme of Australia was later amended by including the rules on Mandatory Data Breach Notication (MDBN) that are set out in the *Privacy Amendment (Notification of Data Breaches) Act 2017 (Cth)* (hereafter the Amendment). The MDBN is important as the former

voluntary scheme administered by the Office of Australian Information Commissioner (OAIC) had met with some criticisms. For example, the former voluntary scheme was criticised as having 'little bark, [and] no bite' [12]. The Amendment tries to address this issue by making it mandatory for a regulated entity to inform the OAIC and the affected individuals of a serious data breach. However, is the law on MDBN a louder bark than the former voluntary scheme? Does it bite any deeper? What avenues of redress are there for the victims of data breaches upon being notified? Can they bring an action for a breach of privacy in court? The problem with data breaches in Australia is that it is difficult for a victim of a breach of privacy to bring an action in court as there is no established tort of privacy in Australia.

This paper tackles three tasks. Section 2 provides features of malicious attacks in cyberspace attempting to acquire personal data and presents a critical review of the NDB scheme. We particularly point out that entities have considerable latitude in establishing what constitutes serious harm and they also have flexibility in determining when they are required to inform the regulator and those who had their data breached. Section 3 provides an analysis that redressing the grievances caused by a data breach is difficult in the Australian legal context, focusing on the lack of a tort of privacy in Australia and illustrating the difficulties in bringing a successful class action in cases of data breaches. Section 4 discusses the degree to which the newly introduced NDB scheme differs from the previous voluntary scheme by comparing the legal aspects. It points out that the NDB scheme gives entities, which should be responsible for data protection, much leeway while holding individuals, only victims of a data breach, much responsibility to deal with the consequences. However, victims of privacy breaches would still have difficulties with class actions under the new scheme, mainly because no statutory right for a claim for a breach of privacy stands under Australian law. This paper suggests that regulated in a

broader context of Australian Privacy Principles (APPs), the NDB scheme could become a part of the privacy protection regime that requires public agencies and businesses to have better accountability and responsibility mechanisms.

2. Data Breach and the NDB Scheme in Australia

2.1. Australia's NDB scheme

The costs of a data leak or data loss are rapidly growing. Some research provides an approximate guide, with the annual IBM Security sponsored Ponemon Institute's Cost of a Data Breach report indicating the average cost to Australian organisations in 2019 was AUD 2.9 million, or AUD 157 per data unit [13]. Moreover, the average cost per lost or stolen record has reached AUD 141, while the average number of breached records per incident has been just under 25,000. A recent report estimates that the cost of data breaches would also quadruple to about AUD 2.1 trillion [14]. While the cost of a data breach is rising dramatically, so is the number of cases. In the last few years, many high-profile hacks and leaks targeting such companies and governments as the US government's Office of Personnel Management, LinkedIn, Apple iCloud, Yahoo, Dropbox, Ashley Madison, MySpace, NSW Trainlink, Gumtree, Cabcharge, Menulog, Kmart, and Sydney University within Australia and globally. Some examples in Australia over the past couples of years are presented in <Table 1> below.

Table 1 Recent examples of data breach in Australia

Date	Organisation	Details of Data Breach
September 2015	Kmart Australia	External privacy breaches to customers' personal information
October 2016	David Jones	The firm's website was hacked, exploiting a vulnerability and resulting in stolen customer information
October 2016	Red Cross Blood Service Australia	1.28 million personal and medical records of Australian citizens donating blood to the RCBS were formatted back to 2010
November 2016	Big W	Customers' data leak
December 2016	National Australia Bank	Personal details of 60,000 customers were sent to a wrong website
December 2018 (discovered in May 2019)	Australian National University	ANU became the victim of a data breach, which included access to up to 19 years' worth of data in the university's Enterprise Systems Domain. Approximately 200,000 people were affected
February 2019	Toyota Australia	The firm became the victim of cyber-attack that took out its email and other online systems
February 2019	Melbourne Hospital	A cybercrime syndicate accessed the medical files of 15,000 patients at Melbourne Heart Group at Melbourne's Cabrini Hospital
June 2019	Australian Catholic University	ACU became the victim of cyber-attack that compromised a number of staff email accounts and some university systems
October 2019	Optus	50,000 customers' mobile numbers mistakenly published in the White Pages
November 2019	ZoneAlarm	Personal details of 4,500 forum subscribers were obtained by hackers

An attempt to legislate a mandatory data breach notification regime in Australia was dated back in 2013 when the Labour government introduced the Privacy Amendment (Privacy Alerts) Bill 2013 to amend the Privacy Act. However, it was after the public release of an exposure draft two years later in December 2015 when a series of public consultation on the introduction of mandatory data breach notification regime took place. The Attorney-General's Department released an exposure draft for public comment and received 45 submissions from industry and consumer groups, regulators, government departments, and Australian and international companies. The final form of the bill was introduced into the Federal Parliament and passed in February 2017. The new law took into effect in February 2018. The Act differed

from the previous voluntary scheme in that it imposed a duty on a regulated entity to inform the authority and affected individuals of a serious data breach. The Act governs the data protection regime of a variety of private and public organisations, from government agencies and financial institutions to almost all online services, whose capacity for data protection and data breach detection may vary. Accordingly, organisational capacity to implement the legal requirement of mandatory notification also varies, which in turn poses a serious challenge to the regulation of data breach.

The notifiable data breach amendments to the Privacy Act, which introduced a mandatory data breach notification (MDBN), define that "an eligible data breach" comprises two elements. First, "unauthorised' compromise of personal information needs to take place. The compromise includes any access, disclosure, or loss and usually is undertaken by external actors such as hackers. However, it may involve internal actors or take the form of cyber espionage [6]. Second, the compromise needs to "result in serious harm to any of the individuals to whom the information relates." This means that not all data compromise is subject to mandatory notification and thus needs to be reported to the regulator, the Office of the Australian Information Commissioner (OAIC). Unauthorised access or disclosure of personal information neither constitutes an eligible data breach, nor imposes a duty of notification. MDBN also notes that as long as an entity takes actions to ensure the access or disclosure not to impose serious harm to anyone to whom the breach is related, the entity is not obliged to notify the regulatory authority. These include remedial actions which prevent any disclosure, loss or access to personal information from causing harm to any individuals. So even if unauthorised access to personal information took place, the entity does not bear the obligation to notify OAIC as long as the entity holding that personal information detects the breach in a very early stage and prevents

the information from being divulged and abused against individual privacy.

This means that essentially it is up to the entity to determine what constitutes a serious data breach and serious harm. The legislation further states that a "reasonable person" of the compromised entity would determine whether the leaked data is harmful if they believe as stated in Division 2, subsection 26WG (iv) "have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates..." This again, places an emphasis on the power and latitude that entities have, to determine what they believe is harmful to those individuals whose information has been leaked.

Once an eligible data breach happened, an entity must notify OAIC. The entity has to notify OAIC even if it only has "reasonable grounds to believe" that an eligible data breach has happened. This means that even without the actual detection of a data breach, entities must notify the regulator if it comes to believe that there is such a breach. Once entities reach this belief, they must assess the data breach and complete it in 30 days. The assessment result should be handed over to the OAIC and also disseminated to individuals with whom the compromised information relates "as soon as practicable". By mentioning "as soon as practicable" the Australian NDB scheme is as ambiguous as legislations of other countries, especially the US, where most states set out that notification of data breach should be made in "the most expedient time possible" or "without unreasonable delay" [8]. It displays an attempt to rule out the ambiguity of when the notification needs to take place by giving out a specific time frame of 30 days.

A failure by an entity to report an eligible data breach to notify affected individuals is considered as an interference with the privacy of the individuals affected by the eligible data breach and could be the subject of a complaint to the Privacy Commissioner (Privacy Act, s 36).

This suggests that entities need to take into account legal and obligations issues when planning for and managing data breaches, as a consequence may compel good behaviour.

2.2. Cyberattacks target personal information

Cybercrime is increasing in scale and impact. Cyberattacks used to acquire identity information such as malware, phishing, spear phishing, to name a few, can have severe consequences for business, government and society. Increasing criminal use of the Internet poses a severe threat to individuals, businesses, industry and governments. Criminals understand the opportunity offered by an online society, and methods of identity theft, financial crime, and other crime have adapted to the Internet. The Internet makes it easy for cybercriminals to operate remotely and to remain anonymous. Figures vary, but cybercrime is estimated to cost the global economy over AUD 450 billion and considered one of the top emerging risks for the 21st century. According to the 2020 Official Annual Cybercrime Report by Cybersecurity Ventures [15], cybercrime will continue to rise and cost businesses globally more than AUD 6 trillion annually by 2021. To Australians, it is estimated to cost over AUD 29 billion each year, and by some estimates, the real impact of cybercrime to Australia could be more severe [16] These costs are expected to rise. Government, critical infrastructure and business, including banking and finance sectors, are likely to remain key targets for cybercriminals and malicious state actors alike.

Many developed countries, including Australia also have rules requiring organisations to notify individuals and regulators of data breaches that's included unauthorised access to, or unauthorised disclosure of personal information. According to the Office of the Australian Information Commissioner (OAIC) in the 'Notifiable Data Breaches Scheme 12-month Insights Report,' the statistics show that there were 964 data breach notifications under the NDB scheme

between 1 April 2018 to 31 March 2019 in Australia [15]. The total data breach notifications had increased by 712% as compared to the previous 12 months when it was under the voluntary scheme. 60% of the data breaches were due to malicious or criminal attacks, attacks that are deliberately crafted to exploit known vulnerabilities for financial or other gain, attacks included cyber incidents such as phishing and malware, data breaches caused by social engineering or impersonation, theft of paperwork or storage devices, and actions taken by a rogue employee or insider threat. One hundred fifty-three of these breaches were caused by phishing or spear phishing. It also remains unknown how credentials have been obtained in 28% of the breaches. 35% of the data breaches were caused by human error unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient via email, unintended release or publication of personal information, and sending personal information to the wrong recipient via post. While 55% of these data breaches that were caused by human error occurred in the health sector. Furthermore, 41% of the data breaches in the financial sector were caused by human error. It is also noted that 83% of the data breaches affect lesser than 1,000 people, and 86% of the data breaches involved the disclosure of contact information.

The case examples in the 'Notifiable Data Breaches Scheme 12-month Insights Report' which were taken from eligible data breaches reported to the OAIC in the first year of implementation illustrated that companies or entities that have reported data breaches have taken remedial steps [15]. These include implementing enhanced security measures such as CAPTCHA and identity verification checks multi-factor authentication, secure customer relationship management system for document transfer new security program for employees and new policy frameworks.

3. Avenues of Legal Redress

The MDBN rules that are set out in the Amendment are important as the old voluntary scheme administered by the OAIC had met with some criticisms. However, there appears to be little avenues for legal redress as it is difficult to bring an action in court as there is no established tort of privacy in Australia. Class actions have also been unsuccessful as the nature of privacy breaches is as such that the victims usually experience embarrassment or anger, rather than actual harm.

3.1. The lack of a tort of privacy in Australia and the Australian Law Reform Commission's suggestion of a tort of privacy

It would be difficult for victims of data breaches to bring an action in court for a breach of privacy as there is no tort of privacy in Australia. The issue of the emerging tort of privacy in Australia had gained much interest today as the advancement in digital technology had created an impact on one's privacy rights.

While there is currently no tort of privacy in Australia, the judges in the case of *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* have left open the possibility of the development of a tort of privacy in future. Furthermore, Callinan J compared Australian law to the laws of other countries which already have privacy rights and stated:

> 'It seems to me that, having regard to current conditions in this country, and developments of the

> law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made' (208 CLR 199, 328).

The legal development in cases such as *Grosse v Purvis* seems to encourage an attempt to establish a free-standing tort of privacy. However, this case has limited interstate applicability as it was decided by the District Court in Queensland. American jurisprudence was followed in *Grosse v Purvis* as William Prosser and his academic theory was highlighted by Judge Skoein. In *Kalaba v Commonwealth of Australia,* Heeray J saw that there is a possibility that the tort of privacy can develop in common law. Heeray J's judgment also illustrated the difficulties that the courts face as their hands are bound by the doctrine of judicial precedent. While judicial activism can be exercised where appropriate, the courts will exercise it cautiously. Other cases where the judicial attitude seems just as encouraging while maintaining that the position is unclear are *Gee v Burger, Doe v Commonwealth Securities Ltd, Maynes v Casey, Saad v Chubb Security Australia Pty Ltd., Chan v Sellwood; Chan v Calvert* and *Doe v Yahoo! 7 Pty Ltd.*

The case of *Doe v Australian Broadcasting Corporation* saw the acceptance of the tort of privacy by Hampel J. This case was appealed, but it was settled on 4 March 2008. Hampel J stated:

> 'this is an appropriate case to respond, although cautiously, to the invitation held out by the High Court in Lenah Game Meats and to hold that the invasion, or breach of privacy alleged here is an actionable wrong which gives rise to a right to recover damages according to the ordinary principles governing damages in tort' ([2007] VCC 281, at [157])

In the report, *For Our Information, Australian Privacy Law and Practice*, the Australian Law Reform Commission (ALRC) recommended the introduction of a statutory cause of action for serious invasions of privacy [16]. In 2014, the ALRC in the report, *Serious Invasions of Privacy in the Digital Era*, proposed a statutory cause of action which would enable Australians to litigate for privacy [17]. The proposed privacy tort is an adaptation of the jurisprudence in the US and UK. The ALRC′s proposed privacy tort is a step forward as there appears to be a gap in Australian common law. It will also complement the limited protection for personal information provided by the *Privacy Act 1988 (Cth)*.

The ALRC recommended that to establish an action under the Tort of Serious Invasions of Privacy, a plaintiff must prove that their privacy was invaded by intrusion upon seclusion or misuse of private information, there must have been an intentional or reckless invasion of privacy and, there need not be an actual damage (and hence, one could claim for damages for emotional distress) [17]. The proposed action is subject to the conditions that:

> ‘A person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances ... The court must consider that the invasion of privacy was ‘serious′, in all the circumstances, having regard to, among other things, whether the invasion was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff ... The court must be satisfied that the plaintiff’s interest in privacy outweighs the defendant′s interest in freedom of expression and any broader public interest in the defendant′s conduct.′ [18]

These conditions were then laid out as part of the elements in establishing an action of breach of privacy under the proposed tort [17]. However, the recommendations of the ALRC have not been adopted. Hence, in the absence of a privacy tort, victims can make complaints to the Office of the Australian Information Commissioner under section 38 of the Privacy Act 1988 (Cth). However, in practice, there appears to be a stumbling block in such class actions and several class actions that have been attempted were not very successful. Privacy class actions will need a cause of action, and typically, the cause of action for such class actions are based on arguments on breach of confidence, breach of contract, negligence or misleading and deceptive conduct. They can also result in court actions.

3.2. Class actions and privacy issues

Unlike the UK and US, the current Australian regime does not provide individuals with a specific statutory right to make a claim for breach of privacy. However, individuals can make a representative complaint to the Office of the Australian Information Commissioner for such data breaches pursuant to section 38 of the *Privacy Act 1988 (Cth)*. This avenue of redress has been in existence even prior to the enactment of the NDB scheme and continues to apply after its enactment.

However, little success existed in making such complaints as it required that the victims prove that 'harm' had been caused, rather than the fact that the victims had experienced embarrassment, anger or unhappiness. This was illustrated in class actions such as the *Cbus class action.* It has also been commented that class actions are a very difficult and cumbersome process. [19]

Furthermore, Facebook's Cambridge Analytica privacy issues also attracted a possible

class action in Australia as 53 Australians had provided their data through the "thisisyourdigitallife" app on Facebook, while 300,000 Australians 'may have' shared their data with Cambridge Analytica [19]. However, the result of an investigation by Australian lawyers from Shine lawyers and the Australian funder of the potential litigation, IMF Bentham, revealed that consumers would not benefit from the class action. Hence, Shine lawyers did not continue to file proceedings against Facebook. This showed that even in such cases of apparent, egregious privacy violations, class actions may not be viable.

3.2.1. Cbus class action

In the *Cbus* class action in 2017, 328 employees of a building sub-contractor made claims based on the disclosure of their superannuation details, which were wrongly disclosed to Cbus, the head contractor. The class action was based on the argument that the breach had caused them to be 'unhappy', 'angry', 'upset', 'disappointed' or 'uncomfortable' and argued that they were entitled to AUD 2,000-AUD 3,000 in general damages and between AUD 3,000 and AUD 4,000 in aggravated damages per class member. Furthermore, the complainants also claimed legal costs. The Commissioner was of the opinion that a public apology and a review of procedures would suffice, and thus, no financial compensation was awarded.

The *Cbus* class action illustrates that the class action claims on data breaches will not result in financial compensation where the breach had merely caused the claimants to be 'unhappy', 'angry', 'upset', 'disappointed' or 'uncomfortable.' There needs to be some evidence of actual loss or damage for such claims could be awarded financial compensation.

3.2.2. NSW Ambulance class action

Class actions can also result in court actions. The first class action to result in a court action is the *NSW Ambulance class action*, which later reached a settlement.

In 2017, the NSW Ambulance Service brought a class action on behalf of 130 of its employees. In this class action, the employees′ medical records were illegally obtained by a NSW Ambulance contractor (named Waqar Malik), who then sold it to personal injury lawyers. This class action was brought after the NSW Ambulance contractor had been convicted of unlawfully disclosing the information in June 2015. Claims were made for pain and suffering, humiliation, psychological injuries, and economic loss. These claims were made based on the argument that there was a breach of confidence, breach of contract, misleading and deceptive conduct, and invasion of privacy because NSW Health Administration Corporation (HAC) had not adequately protected the employees′ personal records. HAC filed a defence which argued that the claimants did not have any relevant right of privacy or that a cause of action under the tort of privacy existed. HAC denied that it did not have the authority to give the confidential information to Waqar Malik or that it was vicariously liable for the Waqar Malik‘s actions. It also denied that it was liable for breach of confidence. In November 2019, the parties to the class action reached a settlement and agreed to a payout of AUD275,000. The barrister for the class stated that the agreement reached in the settlement was “fair and reasonable” largely due to the risks involved in proceeding with the claim as well as the fact that there was “very limited disclosure of material and very limited distribution” as only one law firm had purchased the confidential information from Waqar Malik [20]. Hence, it would appear that while there is a privacy breach which had clearly caused distress amongst the employees of NSW Ambulance, it would be difficult to prove the element of ‘harm′ as only one law firm had purchased the confidential information.

According to the solicitor for the lead plaintiff, Adjunct Professor George Newhouse, "This is the first privacy class action in Australia - it's the first to go to court and it's the first to settle in this way," [21]. However, he also stated that, "... it was a long and difficult road to travel. Our politicians need to intervene urgently and provide individuals with a satisfactory remedy for breaches of privacy and data breaches. If those who held our data were able to be held accountable for its misuse, then perhaps they would be more careful." [22]

3.3 The Australian Information Commissioner takes Facebook to the courts: Australian Information Commissioner v *Facebook Inc. & Anor*

As discussed above, the Cambridge Analytica privacy breach illustrated that class actions may not be viable even in cases of apparent, egregious privacy violations. However, while it was not feasible to bring a class action in the Cambridge Analytica privacy breach, there seems to be a way forward in the Cambridge Analytica legal saga as the Australian Information Commissioner had brought an action against Facebook. The case was brought in the Federal Court because Facebook had breached Australian Privacy Principle 6 (APP 6) and Australian Privacy Principle 11 (APP 11). It was argued that Facebook's platform was designed in a way where users will not be able to choose and control how their personal information was disclosed. Furthermore, its default settings allow for the disclosure of personal information, which infringes one's privacy. It was claimed that Facebook had exposed about 311,127 of its users' data to be sold and used for other purposes which were outside their expectations, and this included the purpose of political profiling. This was in contravention of APP 6 as the 'entity must not use or disclose the information for another purpose (the secondary purpose) ...'

This was mainly due to the fact that the users did not install the 'thisisyourdigitallife' app, and their personal information was disclosed through their friends who had used the app. It was also argued that Facebook had failed to 'take such steps as are reasonable in the circumstances, to protect the information from ... unauthorised access, modification or disclosure,' as set out in APP 11.

3.4 Where does that leave class actions?

The court action that was lodged against Facebook by the Australian Information Commissioner was a welcome move, especially for those who had found it difficult to bring a class action against Facebook. However, it begs the question of the usefulness of class actions.

Class actions are efficient avenues of redress where there are large groups of injured parties as the cases would not need to be heard individually. They also provide a means where the plaintiffs can afford the high cost of litigation as the cost can be shared between the plaintiffs. However, the examples of previous class actions on data breaches have shown that the main problems in class actions are that they are hardly successful and are too difficult a process.

Furthermore, it may not always be possible to rely on the Australian Information Commissioner to lodge a proceeding in the way that it did against Facebook, as it all depends on whether the Australian Information Commissioner is able to do so. It may also take a long time for the Australian Information Commissioner to lodge proceedings. Shine Lawyers and IMF Bentham lodged a representative complaint with the OAIC and investigated whether there could be a class action against Facebook for breaches of the Privacy Act 1988 (Cth) in 2018. However, the Australian Information Commissioner only lodge proceedings against Facebook two years later in 2020.

There remains a need for a better legal avenue which does not entail waiting for the Australian Information Commissioner (which could be as long as two years) and allows people to bring an action in court for privacy infringements. Hence, reforms to improve the law by introducing a statutory cause of action for serious invasions of privacy remain critical.

4. Is NDB a safeguard for individual privacy?

The NDB scheme itself does not impose entities a duty to take remedial steps for a data breach. Instead, the notification requirements render individuals to take remedial steps. This means that the responsibility to protect personal information is eventually on each individual rather than entities that hold personal information. In contrast, those entities are granted with leeway to inform the regulator only when they have been exposed publicly (or the leaked information pertains to Federal or state government agencies). Thus, when an entity has been determined to have a data leak, they would be given 30 days to prove that they are taking relevant action into investigating the threat and determining the best method of notifying individuals who have had their information leaked. The Information Commissioner has the discretion to extend the 30 days by a time frame which is "practicable" if requested by the compromised entity. The NDB scheme aims at rectifying information asymmetry between firms and individuals. But it gives much leeway to entities, which should be responsible for data protection while holding individuals, who can be the only victims of the data breach, much responsibility to deal with the consequences.

4.1 The lack of a more specific avenue of redress

As discussed so far, the Australian NDB scheme places a duty on entities holding personal information to ensure they are aware of data breaches and to act on them promptly. It would suffice that such entities notify the regulator only after any breach has been recognised. The scheme does not ask those entities to be equipped with measures that would prevent personal information from being compromised. In other words, the focus of the legislation is on getting individuals informed of their personal information breach. Individuals, rather than entities holding breached information, are required to act on dealing with the harm which comes as a consequence of personal information compromise. The Australian NDB scheme is likely to leave large room for error and exposure to unwitting Australians and residents.

This may be inevitable as consequences of a data breach cannot be entirely controlled by entities holding personal data. For example, entities are not authorised to change passwords for individual account holders' login profile when individual account information is compromised. They can only notify holders of such accounts to act on such compromise, by guiding them, for example, to change passwords to more sophisticated ones simply. What entities could do when facing credit card information leak by a cyber-attack would be similar: notifying holders of credit cards to monitor malicious misuse of those cards and close off the card if necessary. It is also up to individuals, upon receiving such information and guidance, that they take action to cease business with those entities.

The class actions above illustrate the need for there to be a proper avenue of redress specifically where it involves the mandatory notification of data breaches as it would act as a deterrent from the negligent mishandling of the private information of individuals or the lack of preventive measures which then results in the data breach. The problem of proving 'harm' in

privacy issues appears to be a stumbling block in the class actions as victims usually experience embarrassment or anger, rather than actual harm. Interestingly, the ALRC's proposed privacy tort is a more suitable avenue of redress as it caters for issues such as privacy breach which result in embarrassment or anger, and would not require the victim to prove the element of 'harm'.

A further argument for more specific avenues for redress for data breaches is the fact breaches of other less private types of information will soon have proper avenues of redress under the Consumer Data Right. The *Treasury Laws Amendment (Consumer Data Right) Bill 2018* seeks to amend the *Competition and Consumer Act 2010* and the *Privacy Act 1988.* This was followed by the *Treasury Laws Amendment (Consumer Data Right) Act 2019,* which was passed on 1 August 2019 and the first stage will come into effect in February 2020. The legislation introduces data portability in the form of a new "Consumer Data Right" (CDR).

According to the rules on Consumer Data Right, the OAIC will be the first point of contact available as an initial contact point for consumers and small to medium businesses (under $3m annual turnover) with complaints regarding breaches of the CDR. They will then refer the complainants to the most appropriate body which could deal with the complaint – which could be the OAIC itself or another dispute resolution body. The 'no wrong door approach' will ensure that the complainant will be able to address their grievances efficiently without being passed around from one party to the other [23]. The ACCC has an enforcement role in relation to serious breaches or habitual offenders. Consumers can also lodge a legal suit directly when there is a breach of their CDR. The complainants who are successful in their complaint under the CDR will have a range of remedies available to them, and they include injunctions, orders to delete data, infringement notices, civil penalties, compensation orders, enforceable undertakings and de-accreditation of data recipients (or suspensions or imposition of conditions). Hence, it would

only be proportionate if a data breach of our private information has a proper and designated avenue of redress in the same way that a breach of a Consumer Data Right has a proper avenue of redress.

4.2 Louder bark ... still no bite!

As the Amendment makes it mandatory for a regulated entity to inform the OAIC and the affected individuals of a 'serious data breach', it would have the effect of a watchdog with a louder bark than its predecessor. Indeed, affected individuals had been duly informed when their personal information had been compromised. However, this dog still does not bite!

Victims of privacy breaches would still have difficulties with class actions as the rules in s.38 *Privacy Act 1988 (Cth)* would continue to apply for those who intend to bring a class action in a representative complaint to the Office of the Australian Information Commissioner. Hence, the problem remains in that the class action would fail when the element of 'harm' is not evident in such cases.

It also remains difficult for the victims of data breaches to establish a successful cause of action in court largely due to the lack of a specific cause of action under Australian law that would allow a person to bring an action for a breach of privacy or the loss of data. There is no statutory right for a claim for a breach of privacy, and there is yet to be a recognised right for a breach of the tort of privacy. The ALRC's proposal for a tort of privacy is useful to the victims of data breaches as it would cater more specifically to their issues of a data breach where the breach had caused embarrassment and distress, although the element of 'harm' was not present. Under the ALRC's proposed tort of privacy, the element of 'harm' need not be proven and hence, the proposed privacy tort is the right fit for issues of data breaches where the victims of data

breaches have suffered from embarrassment and distress, although there is no specific harm that had been caused. Therefore, it is suggested that the ALRC's proposal for a tort of privacy should be revisited.

4.3 Regulatory governance for the data protection

Although it is arguable that the Australian NDB scheme may or may not guarantee Australian entities to be responsible for data protection, it does contribute to more secure data protection regime at least indirectly by providing a way of enhancing entities' concerns on the data breach. In a broader context of the Australian privacy regime, all entities holding personal information must take reasonable steps to ensure the observance of the Australian Privacy Principles (APPs) set out in the Privacy Act. The practice indicates that entities are required to take proactive steps to comply with the APPs by placing, for example, staff training and privacy management plans in place. Although the NDB scheme does not itself require entities to be equipped with such proactive steps, the Australian privacy regime asks entities to have a data breach response plan which enhances the entities' awareness, detection, and solution of the data breach.

In this sense, the NDB scheme becomes a means of protecting personal data only when combined with the implementation of APPs. And the Australian privacy regime needs a more systematic approach to ensure compliance with the APPs. APPs provides broad principles rather than a prescriptive list of obligations. The absence of such prescriptive list of what entities must do or must not do means that the regulation of APPs may not be carried out in the way of checking compliance line by line. It should be rather practised in a way that the regulator works with the regulated, discussing what kinds of measures can best meet the regulatory outcomes set out in the APPs. This is a central characteristic of principles-based regulation [24-26]. Black et

al. [25] define principles-based regulation as "moving away from reliance on detailed, prescriptive rules and relying more on high-level, broadly stated rules or Principles to set the standards by which regulated firms must conduct business." Unlike rules-based regulation, which aims at securing regulatory compliance with prescriptive rules, principles-based regulation strives to elicit compliance with the regulatory objectives [24, 26, 27]. Principles here do not proscribe what entities can do or cannot do. Any method can be endorsed in principles-based regulation as long as the method can meet the regulatory objectives set out in the principles. This is to comply with the spirit of the law as opposed to with the letter of the law [28].

The duty of notification both to the regulator and affected individuals stands that the NDB scheme aims at ensuring entities' accountability *ex-post* [29, 30]. The NDB scheme alone does not impose a direct duty on Australian private and public organisations to retain a secure data protection regime. It uses notification duties as a means of making entities' data protection efforts accountable to those who are affected. Compliance with the APPs is rather an *ex-ante* measure holding entities responsible for data protection. Entities are free to choose what measures they put in place to protect the personal data they hold as long as they prove such measures are sufficient to observe the APPs. This, in turn, imposes a duty to the regulator that it has to ensure the entities' measures meet the APPs. Therefore, the regulator needs to work closely with entities, have frequent dialogues to understand the entities' innovative approaches and adopt the best means to ensure entities' regulatory compliance. It is one characteristic of the NDB scheme that it is intended to strengthen entities' responsibility and integrity in protecting personal data they hold, by asking them to account for what has been compromised in the course of their conduct in this task. Ensuring compliance with the Australian data protection regime,

composed of the NDB and APPs, suffices when both the regulator and entities carry out the monitoring, detecting, and as required, reporting duties. In order to meet the expectations of the Australian data protection regime, private and public organisations need to establish internal governance that ensures personal data protection. The regulator is also required to supervise the private governance works appropriately.

5. Conclusion

In this paper, we have provided a brief analysis of the Australian mandatory data breach notification legislation. It may be too early to undertake a full-scale analysis of its effects and consequences. Its effects and consequences should be mostly dependent on how the legislation is implemented and enforced by the regulator. It is undeniable that assessment of this new legislation should be carefully taken and any assessment of the current stage cannot but be limited. However, the debates on this legislation has been the concerns of many stakeholders for more than five years in Australia. The Australian NDB scheme is a response to the pressing needs for privacy protection in the Internet age. So it is essential to see whether the Australian scheme is designed to address such challenges the society encounters.

This paper is intended in this context to provide a better understanding of the Australian NDB scheme. We have pointed out that the NDB gives entities who should be responsible for data protection much leeway while individuals who can be the only victims of the data breach are given much responsibility to deal with the consequences. This has been problematic as redressing the harm caused by a data breach was difficult in the Australian context. As shown in

the cases of unsuccessful class actions, the problem of proving 'harm' in privacy issues appeared to be a stumbling block as victims usually experience embarrassment or anger, rather than actual harm. Moreover, the lack of a tort of privacy in Australia made it difficult for victims of a data breach to bring an action for a breach of privacy or the loss of data. We suggest that the real effect of the NDB scheme should be understood in a broader context of Australian Privacy Principles (APPs). The NDB scheme itself does not impose a duty on entities to come up with proactive measures to enhance their data protection system. Implemented in a broader APPs context, however, the scheme could become a part of the privacy protection regime that requires public agencies and businesses to have better accountability and responsibility mechanisms.

Hiding the hack is more damaging than the hack itself: notification can potentially help affected individuals and businesses mitigate the risks. Implementing the mandatory reporting requirements would raise the awareness of those that do not understand the cyber threat through the external regulation and incentives, and therefore the benefits of strong cybersecurity. In January 2016, the Australian Cybercrime Online Reporting Network (ACORN) stated that it received 39,000 reports of cybercrime in 2015, and half related to online fraud and scams. For example, where an individual's identity details have been stolen, once notified, the individual can take steps to regain control of their information. This could be through cancelling credit cards, changing passwords or requesting new identifiers. Mandatory notification may assist entities with their response to serious data breaches. There may be benefits for entities that notify affected individuals that a serious data breach has occurred. Proactive and timely notification of a serious data breach helps the entity rebuild public trust, demonstrates that the entity is working to protect affected individuals from the harm that could result from the data breach.

Acknowledgements

An earlier version of this paper was presented at the Korea Legislation Research Institute (KLRI), 2017 Legal Scholar Roundtable, How Law Operates in the Wired Society, 21-22 Sep 2017, Seoul, Korea. We thank the Department of Corporate and Information Services, NTG for the support. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

1. Broadhurst, R., et al., *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime.* International Journal of Cyber Criminology, 2014. **8**(1): p. 1-20.
2. Grabosky, P., *The Evolution of Cybercrime, 2006–2016*, in *Cybercrime through an Interdisciplinary Lens*, T. Holt, Editor. 2017, Routledge: New York. p. 29-50.
3. Broadhurst, R., *Cybercrime: Thieves, Swindlers, Bandits and Privateers in Cyberspace.* 2017.
4. Alazab, M. and R. Broadhurst, *Spam and criminal activity.* Trends and Issues in Crime and Criminal Justice (Australian Institute of Criminology), 2016(52).
5. Alazab, M., et al., *Cybercrime: the case of obfuscated malware*, in *Global security, safety and sustainability & e-Democracy*. 2011, Springer. p. 204-211.
6. Karyda, M. and L. Mitrou. *Data Breach Notification: Issues and Challenges for Security Management*. in *MCIS*. 2016.
7. Burdon, M., B. Lane, and P. Von Nessen, *Data breach notification law in the EU and Australia–Where to now?* Computer Law & Security Review, 2012. **28**(3): p. 296-307.

8. Joerling, J., *Data breach notification laws: An argument for a comprehensive federal law to protect consumer data*. Washington University Journal of Law & Policy 2010. **32**: p. 467-488.
9. Picanso, K.E., *Protecting information security under a uniform data breach notification law*. Fordham Law Review, 2006. **75**: p. 355.
10. Romanosky, S., R. Telang, and A. Acquisti, *Do data breach disclosure laws reduce identity theft?* Journal of Policy Analysis and Management, 2011. **30**(2): p. 256-286.
11. Rancourt, S.J., *Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information.* Tex. Wesleyan L. Rev., 2011. **18**: p. 183.
12. Wallbank, P., *Privacy Act Revisions: Little bark, no bite*, in *The Australian*. 2014.
13. Ponemon, *2019 Cost of Data Breach Study*. 2019, IBM Security.
14. Juniper Research, *Cybercrime & The Internet of Threats 2018*. 2019.
15. Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-month Insights Report*. 2020.
16. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice; Report*. 2008: Law Reform Commission.
17. Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era (ALRC Report 123)*, in *ALRC, Commonwealth Government*. 2014, Australian Law Reform Commission: Brisbane.
18. Australian Law Reform Commission, *Serious Invations of Privacy in the Digital Era (ALRC Report 80)*, in *ALRC, Commonwealth Government*. 2014, Australian Law Reform Commission: Brisbane.

19. Slezak, M., *Facebook data breach: Aussies find out if they were affected by Cambridge Analytica access*, in *ABC News*. 2018.
20. Bolza, M., *Settlement reached in NSW ambulance privacy class action*, in *Lawyerly*. 2019.
21. McCubbing, G., *NSW ambos win $275,000 class action payout after major data breach*, in *The Sydney Morning Herald*. 2019.
22. Dolor, S., *Court accepts settlement in pioneering privacy class action in Australia over data breach*, in *Australasian Lawyer*. 2019.
23. The Treasury, *Consumer Data Right*. 2018, Commonwealth of Australia: Canberra and The Treasury, *Consumer Data Right Overview*. 2019, Commonwealth of Australia: Canberra.

24. Black, J., *Forms and paradoxes of principles-based regulation.* Capital Markets Law Journal, 2008. **3**(4): p. 425-457.
25. Black, J., M. Hopper, and C. Band, *Making a success of principles-based regulation.* Law and financial markets review, 2007. **1**(3): p. 191-206.
26. Ford, C., *Principles-based securities regulation in the wake of the global financial crisis.* McGill Law Journal, 2010. **55**(2): p. 257-307.
27. Braithwaite, J., *Rules and principles: A theory of legal certainty.* Australian Journal of Legal Philosophy, 2002. **27**: p. 47-82.
28. Canales, R., *Rule bending, sociological citizenship, and organizational contestation in microfinance.* Regulation & Governance, 2011. **5**(1): p. 90-117.
29. Hong, S.H. and J.s. You, *Limits of regulatory responsiveness: Democratic credentials of*

responsive regulation. Regulation & Governance, 2018. **12**(3): p. 413-427.

30. Bovens, M., *Analysing and Assessing Accountability: A Conceptual Framework.* European Law Journal, 2007. **13**(4): p. 447-468.