Dude, Where's My Data? The Effectiveness of Laws Governing Data Breaches in Australia

Jack Hile
Macquarie University

Abstract: The increasing prevalence of large-scale data breaches prompted Australia to strengthen the Privacy Act by enacting the Privacy Amendment (Notifiable Data Breaches) Act to regulate the behaviour of entities entrusted with personal data. However, this paper argues that these legislative instruments are ineffective when dealing with data breaches and their associated problems. In supporting this conclusion, this paper first develops a criterion for effective data breach law, and then evaluates the Australian framework against this criterion to determine its operational effectiveness. In addition, this paper analyses practical developments in the area of data-breach law to garner insights as to how the Australian framework can be made more effective. Ultimately, this paper concludes that the Australian framework is ineffective when dealing with large-scale data breaches, and recommends future legislative amendment as a means of bolstering its effectiveness.

Introduction

The growing reliance on the Internet as a means of processing and storing personal data has presented a slew of issues for society as a whole, the most prominent being the unauthorised access to personal data by third parties, and the associated consequences arising from its misuse. As personal data rapidly becomes the 'life-blood of retail' (Aguirre *et al.*, 2015, p. 34), it has become increasingly common for online vendors to acquire personal data from customers under the assumption that this data will be securely stored (Morey *et al.*, 2015). However, in recent times, the threat of unauthorised access to personal data and the malicious consequences that may follow have increased as the frequency of large-scale data breaches has grown (Winder 2019).

This paper will employ the meaning of 'data breach' espoused by Geistfeld (2017, pp. 386-387), who defined a data breach as the theft or unauthorised access to one's confidential information that has been entrusted to another in a business transaction. The prominence of such breaches can be seen through recent examples such as the Microsoft Exchange

http://doi.org/10.18080/jtde.v9n2.381

vulnerability which affected tens of thousands of servers globally (Palmer 2021), and other megalithic examples, such as Sony, which had the financial records of 77 million user accounts compromised (Quinn & Arthur 2011), or Equifax, who were subject to a data breach that exposed the personal data of over 140 million customers (Swinhoe 2020). Australian entities have also been subject to major data breaches, with ServiceNSW, a provider of government services, being subject to a data breach in 2020 that exposed the personal data of 186,000 customers (Bungard 2020).

As an attempt to better regulate the conduct of parties who are entrusted with personal data, the *Privacy Amendment* (*Notifiable Data Breaches Act) 2017 (Cth)* ('**NDB Scheme**') was introduced to impose notification and reporting obligations on specified bodies to notify affected individuals in the event of an eligible data breach. However, while reporting obligations are imposed and a complaints system has been created, the NDB Scheme has two main faults. Specifically, individuals are unable to commence legal action on their own volition, and there is no scheme in place that prescribes compensation or damages for affected individuals (Smith & Bloch 2018).

Aim of research

The central aim of this study is to evaluate the effectiveness of the Australian legal and regulatory framework and analyse potential reforms in the event it is deemed ineffective. To achieve this central objective, the paper will: (1) develop a theoretical framework for determining what constitutes effective data breach law; (2) increase understanding of the effectiveness of Australian law regarding its ability to recognise and compensate data breaches**;** (3) consider academic, legislative, and judicial materials to create a roadmap for future domestic reform; and (4) develop options to guide future legislative reform in Australia.

The existing literature

There is a distinct lack of scholarly literature on the provision of compensation following a data breach in the Australian context. However, there have been some contextual studies into the operation of the Australian legislation regarding data breaches generally. Alazab, Hong & Ng (2021) maintain that the NDB Scheme gives entities responsible for data protection significant leeway while imposing responsibilities on data subjects who must shoulder the consequences of a data breach (2021, p. 28). Further, Daly (2018, p. 489) has noted that under the current framework, individuals are denied an equal access to the courts, while Selvadurai, Kisswani & Khalaileh (2017, p. 13) have opined that there is room for further initiatives in Australia. However, there is currently no academic discourse regarding the role of

http://doi.org/10.18080/jtde.v9n2.381

compensation in Australian data-breach law, and this paper will therefore fill a void in the Australian jurisprudential landscape.

While no literature expressly considers the Australian context, various theoretical frameworks with the potential to provide legal redress to individuals following a data breach have been developed. Most notably, Bergelson (2003, pp. 436-443) recommends the attachment of a bundle of rights and therefore a quantifiable monetary value to personal data, while Samuelson (2000, p. 1129) has maintained that copyright protection should be extended to personal data as a method of protection. Additionally, Lim (1999, p. 90) has proposed a contractual model for the regulation of breaches in data security. However, the abovementioned proposals all focus on the determination of liability in the event of a breach and do not consider the inherent difficulties that arise when providing compensation if liability is found. This paper, by focusing on the availability of compensation for individuals, will consider data-breach law from a novel theoretical standpoint and will provide new recommendations in a historically shunned area of discussion.

Finally, this paper will draw insights from the wider international context, most notably in the European Union ('**EU**') under the *General Data Protection Regulation* ('**GDPR**'). It is prudent to note, in line with Lynskey (2017, p. 285), that the EU data protection governance structure has not attracted much doctrinal attention. However, a distinct focus will be placed on the work of Chamberlain & Reichel (2019, pp. 8-9), who note that the compensation provisions of the GDPR are unclear and grant national courts significant flexibility. Further, this paper will assess the work of O'Dell (2017, p. 113), who maintains that the broad discretion placed on national courts undermines the consistent application of the GDPR, and Lynskey (2017, p. 261), who reiterates that the reliance on the discretion of national courts and supervisory authorities erodes the effectiveness of data protection rules generally.

Theoretical Framework for Determining What Constitutes Effective Data-Breach Law

Before the effectiveness of the Australian legislative framework can be critiqued it is prudent to first outline the criteria for effective data-breach law. This paper will consider effectiveness under three main categories, namely: the proper attribution of liability following a data breach, a direct right of action for individuals, and the existence of a consistent compensation mechanism (together '**the criteria for effective data-breach law**'). Each of the abovementioned categories will be considered separately.

http://doi.org/10.18080/jtde.v9n2.381

Attributing liability in data breach matters

The benefits of a defined liability model are espoused by Mitrakas (2011, p. 129), who notes that attributing liability in the information security context is a useful means of reducing social costs, and that the ability to apportion liability between information owners and information security service providers is desirable, as it contributes to a reduction in transaction costs.

However, while legal effectiveness is in many ways defined by the ability to identify which party is legally at fault, care must be taken when creating a mechanism to attribute liability. Specifically, the level of care demanded by legislation must be carefully weighed against the practicality of feasible protection measures available to businesses. In this sense Raz (2010, p. 6), while discussing liability rules generally, correctly notes that, if the level of care demanded by the law is inappropriately high, it may invalidate the claim that the liability resulting from a data breach is legitimately tied to an act of negligence. As such, it is evident that a liability model must be balanced to accurately apportion blame, which has led Mitrakas to conclude that assessing the liability of a service provider is a complex task (Mitrakas, 2011, p. 131). However, despite this complexity, this paper accepts that the ability to attribute fault is an essential part of an effective legal system, and must exist in some form to guarantee the success of a data-breach law.

Academic discourse has supported a slew of workable frameworks that are capable of attributing liability in data breach matters, most notably the least cost avoider model ('**LCA**'), the law of contract, and the legislative model that regulates conduct through statute. These frameworks will be individually assessed to determine which is the most appropriate for data-breach matters.

The Least Cost Avoider Model

The LCA model operates on the premise that, when an accident could have been avoided if a party took care, the obvious approach is to place liability on the party who could have prevented the accident at the lowest cost (Dari-Mattiacci & Garoupa, 2007, p. 235). This approach assists in identifying who should be deemed liable for an incident, and has a positive external effect on the risk landscape as a whole. As parties understand their liabilities in the event care is not taken, entities generally exercise higher levels of care, which contributes to an overall increase in safe practice, and contributes to a decrease in the magnitude and frequency of risk-based activities overall (Carbonara *et al.*, 2016, pp. 173-175). Examples of this approach include, but are not limited to, cars slowing down to avoid a collision, manufacturers exercising a higher level of care to avoid faulty goods being provided to consumers (Dari-Mattiacci & Garoupa, 2007, p. 236), or data controllers investing more heavily in data security to avoid a data breach occurring.

http://doi.org/10.18080/jtde.v9n2.381

However, while the LCA model assists in mitigating the occurrence of accidents generally, the model has three main deficiencies. First, when attributing liability, the LCA model relies on information that, while available at the time of adjudication, may not have been available to the parties when they decided whether or not to exercise higher levels of care (Dari-Mattiacci & Garoupa, 2007, p. 237-238). As a result, parties may be deemed liable for a failure to take preventative action in circumstances where they were unaware they had an obligation to do so (Raz, 2010, p. 16). This approach to liability has been criticised by Meglio (2020, pp. 1225-1226) who, while discussing data breach law generally, warns against the imposition of unclear compliance obligations in circumstances where the risks to data subjects are poorly understood.

Secondly, the LCA model requires that liability be attributed entirely to the party with the lowest costs of care (Dari-Mattiacci & Garoupa, 2007, p. 245). As such, parties may forego taking preventative measures if they are confident that they are not the party with the lowest cost of care, thereby shouldering the burden to take preventative measures on a singular party. Thirdly, under the LCA model, parties will likely have an understanding of what fines will be issued if they are found to be liable for a data breach. Further, parties will understand the cost of implementing more stringent security measures. As such, parties may decide not to comply with the requirement to implement protective measures if they know the costs of care are higher than the fine that will be issued if they are found to be liable for a data breach (Dari-Mattiacci & Garoupa, 2007, p. 246). This allows parties to purposely breach their legal obligations on the understanding that compliance with the law costs more than non-compliance. As such, parties are able to selectively comply with their obligations, which undermines the effectiveness of the LCA model.

Contract law

One solution to the issue of liability in data-breach matters would be to allow parties to decide who is liable through the use of contractual provisions (Lim, 1999, p. 90). Kecsmar (2003, p. 280-283) correctly maintains that contractual clauses can establish clear rights and responsibilities that introduce legal certainty into the area of data-breach law. In addition, Massey (2010, p. 89) validly asserts that through contract parties can opt to circumvent the need for arbitration which may make the determination of cases more expedient. Further, Lim (1999, p. 90) affirms that contract law is already a widely accepted means of regulation that is international in scope and adaptable to changing social circumstances. Finally, Lindqvist (2017, pp. 59-60) has noted that the use of contracts is beneficial as it allows stakeholders to include broader forms of damage that can be specifically tailored to the data that is the subject of the contract. This allows individuals to determine what constitutes adequate damages in the event of a breach of contract, which facilitates a more balanced distribution of liability

http://doi.org/10.18080/jtde.v9n2.381

between data controllers and data subjects (Lindqvist, 2017, pp. 59-60). However, as will be discussed below, the effectiveness of contract law is limited by two key deficiencies that render it inoperable when dealing with data breaches and their associated consequences.

First, while contracts allow parties to establish their own liability and compensation provisions, an imbalance in bargaining power may allow data controllers to limit their own legal liability or restrict the rights of data subjects. As Lindqvist (2017, p. 62) notes, it is usually the data controller that decides the terms of a contract. Further, standard-form contracts are often written in a 'take it or leave it' form where, if an individual does not agree to the terms of the contract, they are precluded from using a product or service (Lindqvist, 2017, p. 62). This situation has led Prins (2006, p. 292) to conclude that, as a result of an imbalance in bargaining power, individuals faced with a standardised contract are likely to accept any contractual terms that data controllers offer them. The use of 'take it or leave it' terms under the threat of exclusion of use therefore allows data controllers to coerce individuals into contracts that they may ordinarily be reluctant to agree to (Prins, 2006, p. 292).

Secondly, the feasibility of contract law as a means of attributing liability is hindered by its lack of adaptability. The subject of a contract is fixed at the time it is drafted and can often only be altered through express agreement by the contracting parties. Personal data, however, when digitised, can rapidly change form and location, which makes it difficult to draft contracts involving personal data with precision. For example, the holder of personal data may transfer the data to a server in a different country or convert data into a different file type. In both of the above examples a contract would likely need to be amended each time the form of personal data changed, which has led Lindqvist to conclude that contracts relating to personal data are often difficult to draft, lead to confusion among stakeholders, and will likely cause problems in the future (Lindqvist, 2017, p. 62). As such, the inability of contracts to adapt to a fast-paced technological landscape limits their ability to consistently attribute liability in data breach matters.

Legislation

While the LCA model and contract law have merit, commentators have noted that in general legislation can provide better incentives for compliance than ordinary liability rules (Dari-Mattiacci & Garoupa, 2007, p. 236). Further, research to date suggests that data-breach notification laws may have an overall positive effect on encouraging better data security practices (Daly, 2018, p. 480), which reduces the risk of a data breach generally. Additionally, Solove maintains that there must be a centralised system by which individuals can exercise their rights, which he states can be achieved through information regulation that prescribes a set of actions that must be followed (Solove, 2006, p. 370). This paper agrees with the above findings, and accepts that an enforceable legislative scheme is the most favourable model by

http://doi.org/10.18080/jtde.v9n2.381

which liability can be attributed effectively in data-breach matters. This is due to the fact that a codified negligence standard creates an environment where parties clearly understand their obligations when dealing with personal data (Dari-Mattiacci & Garoupa, 2007, p. 239).

This paper acknowledges the argument that legislation may disproportionately affect small and young firms by creating an anti-competitive market landscape (Campbell *et al.*, 2015, p. 67). That said, Solove (2006, p. 384) correctly notes that modern society is already heavily regulated, and the inclusion of a negligence standard in a domestic legal framework will not impede economic development in any significant manner. As such, this paper considers that legislation can effectively establish a liability standard capable of consistent application, thereby making it the most appropriate liability model for the purposes of the following discussion.

Conclusions on liability

While the LCA model and contract law both present a feasible method of attributing liability in the event of a data breach, this paper aligns with the view of Garoupa in maintaining that regulation generally provides better incentives than ordinary liability models (Dari-Mattiacci & Garoupa, 2007, p. 236). As such, the scope of the following discussion, when discussing liability, will be limited to statutory provisions that regulate the conduct of parties following a data breach.

A direct right of action for individuals

The second criterion of effective data breach law is the ability of individuals to directly enforce the law in court. As will be discussed below, this paper agrees that meaningful access to the courts is an essential feature of a functional legislative scheme, which Abel maintains can only be secured if a litigant can identify the central issues in a case and present evidence and arguments in a court regarding those issues (Abel, 2012, p. 808). This is of particular importance in respect of data-breach laws, as modern technology has created a range of new legal issues that warrant judicial determination (Dolbow, 2017, p. 1935).

That said, it is important to recognise that there are several reasons why a direct right of action may not be feasible, most notably the fact that it might strain judicial resources. For example, Jamison (2019, p. 35) has warned that a direct right of action may give rise to an increase in the number of nuisance suits, while Nieuwesteeg & Faure (2018, p. 1238) have argued that deferring jurisdiction away from supervisory bodies will detrimentally affect the efficiency of the courts. However, the risk of frivolous suits can be overcome with sufficient safeguards, and the introduction of a direct right of action will ensure that individuals are able to effectively assert their rights (Jamison, 2019, p. 35). As such, the increased workload placed on the courts is an unfortunate collateral impact that is required to ensure all affected individuals enjoy

http://doi.org/10.18080/jtde.v9n2.381

unequivocal access to justice in the event of a data breach. Ultimately, while a direct right of action will adversely affect judicial efficiency, it is arguable that this right would tailor the law specifically to the needs of data breach victims (Alazab *et al.*, 2021, p. 27). As a result, this paper accepts that a direct right of action is a necessary component of effective data breach law.

A consistent compensation mechanism

The final criterion of effective data-breach law is the ability of individuals to receive compensation in the event of a data breach. Timmel (2012, p. 48) has noted that the costs of data security incidents to data subjects are real and material, which supports the notion that individuals should be entitled to some form of compensation to remedy the consequences that flow from a data breach.

That said, the provision of compensation is challenging due to the fact that the damage suffered as a result of a data breach is often fluid and difficult to quantify. For example, if an individual's social media account is lost or stolen as a result of a data breach, it is likely that the individual will wish to be compensated for the loss of the account. However, studies have shown that the value of data (and by extension the damage suffered as a result of its loss) can fluctuate significantly (Glikman & Glady, 2015), which makes it difficult to determine whether compensation is appropriate and, if so, what damages would be adequate to compensate for the loss. As such, it is likely that a court, when attempting to compensate a plaintiff for the loss of personal data by a defendant, would have difficulties determining adequate compensation. This is especially so given that traditional valuation methods have been ineffective in data breach matters (Sidgman & Crompton, 2016, p. 172).

This paper recognises that compensating a plaintiff for loss suffered as a result of a data breach is a difficult task (Stewart, 2005, p. 21). However, this paper does not accept that this difficulty by itself justifies a legislative approach where courts are unable to compensate individuals. As will be discussed later in this paper, it is unimportant whether the compensation provided is in the form of material or non-material damages, it is only necessary that a legislative framework is able to compensate individuals in the event of a data breach.

The practical operation of the criteria

The aforementioned criteria for effective data-breach law operate in tandem to create a legislative model in which legal wrongdoing and its consequences are recognised and adequately compensated. The framework for attributing liability, a direct right of action to a court, and a consistent and clear compensation model all contribute to a well-rounded and

http://doi.org/10.18080/jtde.v9n2.381

effective legal model that is capable of adapting to emerging technological issues in the area of data-breach law.

The Effectiveness of the Present Australian Legal Framework

To assess the effectiveness of Australian law it is prudent to consider its operation in line with the criteria for effective data-breach law. However, this paper will first outline the provisions of the *Privacy Act 1988* (‘**PA**’) and the NDB Scheme that regulate the storage and use of personal data in Australia. It is noted that the PA and NDB scheme refer to ‘personal information’. However, for the purposes of consistency in terminology throughout this paper, the term ‘personal data’ will be used instead.

Australia’s legislative framework

The Privacy Act

The handling and use of personal data in the Australian context are governed by the PA. The PA contains the Australian Privacy Principles (‘**APPs**’), which impose obligations on Commonwealth agencies, private companies with an annual turnover of more than $3 million, and private health providers irrespective of their size (‘**APP Entities**’) (PA, 1988, s. 6). While the PA provides for thirteen APPs that govern the use and disclosure of data, for the purposes of this paper only Principles six and eleven are relevant, and the following discussion will be restricted as such. APP 6 maintains that, if an APP entity holds data about an individual that was collected for a specific purpose, the APP Entity must not use or disclose the data for another purpose unless the individual has consented to the secondary purpose (PA, 1988, sch. 1 pt 3 cl. 6.1-6.2(a)). APP 11, in complementing APP 6, states that, if an APP Entity holds personal data, the entity must take reasonable steps to protect the data from misuse, interference and loss (PA, 1988, sch. 1 pt 4 cl. 11.1(a)), as well as from unauthorised access, modification or disclosure (PA, 1988, sch. 1 pt 4 cl. 11.1(b)). In other words, APP 11 provides that APP Entities must take reasonable precautions to prevent data breaches in any circumstance, whether inadvertent, deliberate, or on account of external malicious sources. In the event of non-compliance, an individual must first make a complaint to the organisation that has allegedly breached an APP and, if the organisation does not respond satisfactorily, the individual may then make a complaint to the federal Privacy Commissioner (PA, 1988, s. 36). The abovementioned provisions set a baseline standard for personal data protection in Australia and create a complaints mechanism for individuals in the event their personal data is improperly disclosed by an APP Entity.

http://doi.org/10.18080/jtde.v9n2.381

The Privacy Amendment (Notifiable Data Breaches) Act

In addition to the PA, the NDB Scheme was enacted to strengthen data protection legislation and better protect the rights of individuals as society progresses to a predominantly online realm (Australian Law Reform Commission, 2008, p. 61). The NBD Scheme is located under Part IIIC of the PA, and imposes an obligation on APP Entities to notify both the federal Privacy Commissioner and any affected individuals in the event an eligible data breach occurs (PA, 1988, ss 26WK(2), 26WL(2)). An eligible data breach is defined to be any unauthorised access to, or unauthorised disclosure of, personal data, where 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 data relates (PA, 1988, s. 26WE(2)(a)). In determining whether serious harm is likely to be suffered, regard is to be had to the kind and sensitivity of the data (PA, 1988, s. 26WG(c)-(d)), the persons who have obtained the data (PA, 1988, s. 26WG(g)), whether the data is protected (PA, 1988, s. 26WG(e)-(f)), the nature of the harm (PA, 1988, s. 26WG(i)), and any other relevant matters (PA, 1988, s. 26WG(J)).

The effectiveness of the Australian legal framework

This paper recognises that the Australian legal framework is successful in attributing liability in the event of a data breach. The PA expressly states which entities will be subject to its provisions (PA, 1988, s. 6), and what circumstances must be met for a data breach to be considered 'eligible' for notification (PA, 1988, s. 26WE(2)). In addition, the framework accounts for situations where multiple APP Entities jointly hold personal data that is subject to a data breach. For example, an eligible data breach of one entity will also be considered an eligible data breach of all entities that hold the same data (OAIC, 2019), and all entities are generally responsible for complying with the NDB scheme in relation to the affected data. As such, the Australian legal framework is capable of attributing liability to either a singular party or multiple parties in the event of a data breach.

Despite the ability of the Australian framework to attribute liability, this paper recognises that the framework has two main faults. First, the framework fails to provide individuals with a right of direct access to the courts. Secondly, there is no compensation model that can be relied on by individuals in the event of a data breach. For clarity, these issues will be discussed separately.

A direct right of action for individuals

Given the High Court has failed to recognise a general right to privacy or any corresponding tortious action for a breach of privacy (ABC v Lenah Game Meats, 2001; Smethurst v Commissioner of Police, 2020, para 48), individual complaints regarding a data breach must be directed through the Office of the Australian Information Commissioner ('**OAIC**'). The

http://doi.org/10.18080/jtde.v9n2.381

OAIC is entitled to investigate complaints, make determinations, and issue fines in circumstances where non-compliance is found (PA, 1988, ss 36A, 40, 52). However, there are concerns regarding the capacity of the OAIC to respond in data-breach matters. In this sense, Coyne (2015) has noted that insufficient funding has impacted the OAIC's ability to adequately carry out its investigative functions, while Daly (2018, p. 489) has maintained that the OAIC lacks the capacity to properly investigate each claim. These limitations are of particular importance when considering large-scale data breaches in which hundreds of thousands or even millions of individuals are affected (Quinn & Arthur, 2011), as the OAIC is unable to carry out its investigative function to an adequate standard when dealing with claims of this magnitude. Whilst representative complaints are possible under the PA (PA, 1988, s. 38), Timmel has noted that the absence of a clear statutory cause of action creates a significant hurdle for plaintiffs in privacy class actions (Timmel, 2012, p. 48). This hurdle limits the success of representative claims in Australia, and forces individuals to rely on the investigative power of the OAIC to seek legal redress. However, on account of its limited capacity, the OAIC is often unable to effectively pursue individual complaints (Daly, 2018, p. 489).

This reliance on the OAIC to investigate infractions has prompted Daly (2018, p. 492) to note that more stringent data-breach laws are necessary to facilitate the proper application of the NDB Scheme. Additionally, commentators have recently affirmed the need for individuals to have a proper avenue of redress where a notifiable data breach has occurred (Alazab *et al.*, 2021, p. 27). As such, the recommendation to include a direct right of action for individuals following a data breach is frequently proffered, most notably by the Australian Competition and Consumer Commission ('**ACCC**') in its Digital Platforms Inquiry. In its final report, the ACCC recommended granting individuals a direct right to bring actions against APP entities to seek compensation for an interference with their privacy (ACCC, 2019, p. 35). This recommendation garnered approval from the OAIC, which supported the implementation of a direct right of action for individuals (OAIC, 2019), and the Australian Government, who in principle endorsed the introduction of a direct right of action in Australian data-breach law (Australian Government, 2019, p. 18). Further, the Australian Law Reform Commission has previously advocated for the inclusion of a direct right of action (2014, p. 53), while academic discourse has criticised the Australian framework for failing to provide individuals with an avenue to sue for a breach of the APPs (Goggin *et al.*, 2019, p. 6).

However, it is arguable that allowing public access to the courts in data-breach matters will facilitate an increase in nuisance claims (Jamison, 2019, p. 35). Currently, investigative powers are centralised under the authority of the OAIC, which has jurisdiction to investigate a matter following a complaint (PA, 1988, s. 40(1)), or on its own initiative (PA, 1988, s. 40(2)). However, once a complaint has been received, the OAIC is under no obligation to undertake

http://doi.org/10.18080/jtde.v9n2.381

an investigation, and may decide not to investigate if it is satisfied that the act complained of is not an interference with the privacy of the individual (PA, 1988, s. 41(1)(a), or that the complaint is vexatious, misconceived, lacking in substance, or not made in good faith (PA, 1988, s. 41(1)(d)). Section 41 of the PA is effectively a screening mechanism that allows the OIAC to restrict its investigative resources to those claims with substantial merit, while culling those complaints that, in the Commissioner's opinion, have no reasonable chance of success. If a direct right of action were introduced, and complaints from individuals could be instigated directly, the courts would likely be forced to service an increased number of vexatious or misconceived claims, as there would be no authoritative body screening the matters beforehand. That said, the risk of frivolous suits can be overcome with sufficient safeguards (Jamison, 2019, p. 35), and as such an increased workload placed on the courts is not, by itself, a sufficient justification to exclude a direct right of action in data breach matters.

Ultimately, while the inclusion of a direct right of action for individuals may adversely impact the efficiency of the courts, this paper accepts that the effectiveness of the Australian legal framework would be bolstered should a direct right of action be introduced, as doing so would ensure that the merit of each claim would be properly assessed by a competent judicial body.

Individual compensation in the event of a data breach

The PA and NDB Scheme both fail to provide compensation to individuals whose data has been compromised in a data breach. This paper recognises that assessing the value of harm to intangible property such as personal data is difficult (Brooks, 1998, p. 384). Further, Stewart (2005, p. 21) is correct to maintain that calculating economic damages following a data breach is no simple task. Nevertheless, it is unacceptable for a legislative scheme to find a party liable for a data breach yet offer no compensatory damages to those individuals who have been affected by the conduct.

Ultimately, the implementation of a compensation mechanism into the PA would bolster its effectiveness by allowing courts to compensate individuals following a data breach. That said, this paper does not recommend the creation of an arbitrary compensation model for data breaches. Instead, as will be discussed later, this paper recommends granting courts the ability to award non-material damages in data-breach cases on broad grounds such as breach of privacy or distress. This approach has already garnered approval under the GDPR, with Tâbušca, Garais & Enâceanu (2018, p. 78) noting that damages of this type have created an effective policy framework that is capable of consistently compensating individuals following a data breach.

http://doi.org/10.18080/jtde.v9n2.381

Conclusions on the effectiveness of the Australian legal framework

The above discussion highlights that the Australian data breach regime has several flaws. First, Daly (2018, p. 489) accurately asserts that concentrating the power to initiate legal proceedings on the OAIC deprives individuals of the ability to seek legal redress on their own accord. Secondly, Dolbow (2017, p. 1935) and Abel (2017, p. 808) correctly maintain that precluding individual access to the courts denies claimants a meaningful access to justice. Finally, the NDB Scheme fails to provide victims of a data breach with a right to compensation. Ultimately, these deficiencies support the conclusion of Daly (2018, p. 492) that the current data-breach notification laws are merely a weak, retroactive response to corporate non-compliance. However, this paper echoes the views of Selvadurai, Kisswani & Khalaileh (2017, p. 13) in maintaining that these fundamental flaws have the potential to be remedied through further initiatives, the potential success of which will be evaluated below.

Insights from the European Union

The success of the GDPR will be assessed in line with the criteria for effective data-breach law. However, this paper will first outline the provisions of the GDPR that regulate the storage and use of personal data. The regulations of the EU have general application, are binding in their entirety, and are directly applicable in all member states of the EU (TFEU. 2012, art. 288). As a result, the following discussion will be confined to an analysis of the GDPR itself and will not consider any domestic legislation that has been enacted in response by member states.

The legislative framework of the GDPR

The GDPR imposes two broad obligations on data controllers (those entities that determine the purposes and means of processing data (GDPR, 2016, art. 4(7)), and third parties that process data on behalf of another entity (GDPR, 2016, art. 4(8))). First, in the case of a personal data breach, the data controller must notify the supervisory authority that a breach has occurred within 72 hours unless the breach is unlikely to result in any risk to the rights and freedoms of those affected (GDPR, 2016, art. 33(1)). Secondly, when a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller must communicate the personal data breach to the data subject without undue delay (GDPR, 2016, art. 34(1)). These notification obligations are analogous to the requirements of the NDB Scheme; however, the GDPR is divergent in the way it establishes a direct right of action and a scheme of compensation for individuals who are affected by a data breach. Article 82 of the GDPR is relevant in this respect, which provides that a data controller can be held liable to pay compensation for any damage (either material or non-material) caused by an infringement of the GDPR (GDPR, 2016, art. 82(1)). The Article also provides that affected

http://doi.org/10.18080/jtde.v9n2.381

individuals are entitled to bring such claims for compensation before their national court or the courts of the member state where the data controller has an establishment (GDPR, 2016, art. 82(6)). Article 82 therefore establishes a direct right of action in the event of a data breach, as well as a model of compensation that is able to compensate individuals for both material and non-material damage.

In addition to Article 82, Recital 146 is of relevance when considering an individual's entitlement to damages. The Recital maintains that a data controller should compensate any damage suffered as a result of an act that infringes the GDPR (2016, recital 146). The Recital maintains that damage is to be interpreted broadly, and that affected individuals should receive full and effective compensation for the damage they have suffered (GDPR, 2016, recital 146). In addition, in instances where multiple data controllers are involved in the same negligent processing, they will be held jointly liable for the entire damage (GDPR, 2016, recital 146). This approach effectively regulates multi-party data breaches, bypasses the complex task of apportioning liability between various data controllers, and gives the framework a character of transparency (Chamberlain & Reichel, 2019, p. 7).

The effectiveness of the GDPR in regulating data breaches

This paper will now assess the effectiveness of the GDPR against the criteria for effective data-breach law. Specifically, the GDPR will be considered exclusively in relation to the deficiencies of the Australian legal framework. If the GDPR is effective where the Australian framework is deficient, it is reasonable to assert that it would be beneficial to incorporate those successful aspects of the GDPR into Australian law to bolster its effectiveness.

A direct right of action for individuals

The effective results of the GDPR can be seen most prominently through the implementation of a direct right of action in data breach matters. Szydło (2017, pp. 370-376) notes that, prior to the enactment of the GDPR, complaints for data-breach violations were administered independently by the national supervisory authority of each member state. These bodies possessed a wide range of powers, with Lynskey (2017, p. 255) noting their role as negotiators, law enforcers, and policy advisors among a slew of other responsibilities. In addition, Lynskey (2017, p. 261) reiterates that these bodies, as the sole investigator of data breach violations, were permitted a broad level of discretion in determining what violations to pursue and what remedies to award to affected individuals. Supervisory authorities were therefore able to use their discretionary power to reject individual and small-group complaints on the grounds of pragmatism to pursue more strategic issues (Lynskey, 2017, p. 262). This situation is analogous to Australia, where the OAIC holds dominion over the instigation of judicial proceedings for data-breach violations. This framework denies complainants an effective

http://doi.org/10.18080/jtde.v9n2.381

avenue to seek legal redress, and ultimately inhibits an individual's access to justice in the event of a data breach.

The GDPR has remedied the issue facing the Australian legal framework by granting individuals access to national courts for data-breach violations. This both remedies the complaints of Szydło (2017, pp. 370-376) and Lynskey (2017, p. 261) by effectively curtailing the discretionary power of investigative bodies, while simultaneously alleviating the workload of historically resource-starved institutions that Daly (2018, p. 489) and Coyne (2015) have noted are not capable of operating at an adequate standard when tasked with investigating large-scale data breaches. Also, without the consistent stream of individual complaints, these investigative bodies can devote more time to larger investigations and the development of better preventative practices to mitigate the occurrence of data breaches in the future.

Individual compensation in the event of a data breach

Tâbušca, Garais & Enâceanu (2018, p. 78) have noted that the GDPR, through Article 82 and Recital 146, has created an effective statutory framework that regulates the processing of personal data and damages in the event of a data breach. However, the framework is not without its faults, with O'Dell (2017, p. 111) noting that the provision of damages is not qualified by any method of calculation, and at present there has been no guidance provided as to the proper interpretation of Article 82 or Recital 146. In this sense, when courts are required to determine what damages are appropriate, the only assistance provided by the GDPR is that a person who has suffered damage is entitled to compensation (GDPR, 2016, art. 82), which should be full and effective (GDPR, 2016, recital 146). The drafting of these provisions, as Chamberlain and Reichel (2019, pp. 8-9) have concluded, has created a somewhat vague legal framework in which member states are granted significant discretion to determine what is compensable damage and effective compensation on a case-by-case basis. This framework has promoted the emergence of conflicting determinations on what non-material damage is worthy of compensation, which has led Lynskey to note that the best way to remedy violations under the GDPR remains contested (Lynskey, 2017, p. 261).

The inconsistent application of the GDPR's compensation provisions can be seen through conflicting determinations on what degree of harm is required to justify the provision of non-material damage. For example, in a matter involving the improper disclosure of personal data to an unauthorised third party, the Darmstadt Regional Court held that the violation of the protection of personal data, by itself, poses a sufficient risk to justify the provision of non-material damages (Darmstadt Regional Court, 2020, paragraph 70). While not considering data breaches per se, the Düsseldorf Labor Court made a similar decision regarding the threshold for damages under Article 82 by determining that a data controller, by failing to respond to a request for information made by a data subject, had committed an offence that

http://doi.org/10.18080/jtde.v9n2.381

entitled the data subject to non-material damage under Article 82 (Labor Court of Düsseldorf, 2020, Section I, paragraph 4(dd)). The Court in this matter noted that the severity of immaterial damage is irrelevant for the establishment of liability, and that the concept of damage is to be interpreted broadly (Labor Court of Düsseldorf, 2020, Section I, paragraph 4(dd)). These matters highlight that the threshold test for the provision of non-material damage under the GDPR is low, and that the mere occurrence of a data breach will be sufficient to entitle a data subject to compensation.

Conversely, the District Court of Frankfurt found differently in a matter involving a data breach. In this instance, the customer data of a hotel had been made available to third parties in error, which the plaintiff discovered through a media release relating to the incident (District Court of Frankfurt, 2020, paragraph 3-5). The Court in this matter found that serious impairment is required for a claim for non-material damage under Article 82, and that in the event of a data breach mere discomfort or a minor violation of a data subject's rights is not sufficient to justify a claim for damages (District Court of Frankfurt, 2020, paragraph 2). Ultimately, the court found that causal damage in the form of pain and suffering is required to create objectively understandable and detectable damage, and that individually perceived discomfort without serious impairment to an individual's self-image or reputation is insufficient to create an injury worthy of non-material damage (District Court of Frankfurt, 2020, paragraph 27-30).

This paper recognises that the above matters are somewhat distinct. That said, in light of the above it is evident that the discretion provided to courts has created a legal landscape in which conflicting threshold tests are being applied regarding what constitutes compensable damage under Article 82 of the GDPR. On one hand, the Courts of Darmstadt and Düsseldorf accept that the severity of the immaterial damage is irrelevant when considering whether compensation is available, and that the mere violation of personal data held by a data controller is sufficient to create a harm worthy of compensation. However, the stance employed by the District Court of Frankfurt is at odds with the approach of other EU courts, and severely restricts the circumstances in which a court is able to compensate individuals in the event of a data breach. As a result, O'Dell (2017, p. 113) is correct to assert that the application of the GDPR is contingent on further discretionary steps by the national courts of member states which, as Chamberlain and Reichel (2019, pp. 8-9) have noted, leaves member states grappling with the question of how far national flexibility is expected to stretch in the data protection area. The effectiveness of Article 82 and Recital 146 is therefore limited by the lack of clarity on the circumstances in which non-material damage can be provided in the event of a data breach.

http://doi.org/10.18080/jtde.v9n2.381

That said, Article 82 and Recital 146 allow courts to compensate individuals who have been impacted by a data breach. As such, it is likely that imputing a similar provision to Article 82 or Recital 146 into Australian law would bolster its ability to provide redress to individuals. However, it is not disputed that these provisions would need to be amended before being implemented into Australian law. Specifically, it would be necessary to include a threshold test of damage that must be met before non-material damage could be awarded, as this would curb judicial discretion and ensure consistency in the outcomes of data-breach matters. In doing so, the Australian landscape would be able to effectively compensate individuals in a diverse range of data-breach matters, and would satisfy the criteria for effective data-breach law.

Conclusions on the effectiveness of the GDPR

Ultimately, the GDPR, despite its shortcomings, has successfully remedied several issues that continue to plague the Australian scheme. First, in line with the findings of Szydło (2017, pp. 370-376) and Lynskey (2017, p. 261), the empowerment of individuals to instigate their own complaint has curtailed the unchecked discretion of independent investigative bodies, thereby promoting a more meaningful access to justice. Secondly, irrespective of the findings of Chamberlain and Reichel (2019, pp. 8-9), the provision of a scheme of damages has been successful in providing redress to affected individuals following a data breach. Finally, while this paper accepted the finding of O'Dell (2017, pp. 111-112) that the GDPR fails to consistently compensate plaintiffs in data-breach matters, this flaw in and of itself is not sufficient to detract from the success of the GDPR in providing non-material damage to individuals. Ultimately, the GDPR satisfies the criteria for effective data-breach law, and provides a feasible remedy to the issues faced by the Australian legal framework. As such, it would be sensible to introduce similar measures into the Australian jurisdiction, albeit with a number of modifications.

Conclusions

This paper argued that the Australian legal framework fails to provide an avenue for individuals to instigate a claim or receive compensation following a data breach. Further, this paper accepted that the NDB Scheme, while attempting to respond to the pressing need for privacy protection, has provided APP Entities with significant leeway while imposing the responsibility to deal with the consequences of a data breach on affected individuals (Alazab *et al.*, 2021, p 28). As such, it is evident that the PA and NDB Scheme are unable to satisfy the criteria for effective data-breach law, and are therefore in need of legislative amendment.

Secondly, this paper evaluated the success and limitations of the GDPR. This paper, whilst identifying issues regarding the clarity of the GDPR's compensation provisions, did not

http://doi.org/10.18080/jtde.v9n2.381

consider that the shortfalls identified by O'Dell (2017, p. 113) are sufficient to entirely diminish the effectiveness of the GDPR. Ultimately, the GDPR satisfied the criteria for effective data-breach law, and showcased its potential in being able to remedy the deficiencies suffered by the Australian jurisdiction. Consequently, this paper recommends that, in the case of future domestic reform, the Australian legislature consider the successful aspects of the GDPR and its capacity to bolster the effectiveness of Australian law. Specifically, this paper recommends that Australia take steps to implement a right to non-material damage for a breach of the NDB Scheme similar to Article 82 and Recital 146 of the GDPR. Doing so would recognise a cause of action following a data breach, facilitate a direct right of action for privacy matters, and allow courts to grant compensation on broad grounds such as breach of privacy or distress.

Acknowledgements

I would firstly like to thank Niloufer Selvadurai, without whom this paper would not have been possible. Further, I would like to thank my sister, Ellen, my brother-in-law, Sean, and my parents, Maree and Gregory, who have spent longer than they should have reading countless drafts of this work. In addition, I would like to thank my partner, Amelia, whose consistent moral support helped me make the final push to get this paper over the line. Finally, I would like to thank the many friends who gave their time to read this paper: your constructive criticism and encouragement meant more than you'll ever know.

References

Abel, L. (2012). Turner v Rogers and the Right of Meaningful Access to the Courts. *Denver University Law Review*, *89*(4), 805-823.

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, *91*(1), 34-49. http://dx.doi.org/10.1016/j.jretai.2014.09.005

Alazab, M., Hong, S., & Ng, J. (2021). Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Future Generation Computer Systems*, *116*, 22-29. https://doi.org/10.1016/j.future.2020.10.017

Australian Broadcasting Corporation v Lenah Game Meats (2001) 208 CLR 199.

Australian Competition and Consumer Commission. (2019). *Digital platforms inquiry - final report*. Canberra: Commonwealth of Australia. Available at https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

Australian Government. (2019). *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry*. Available at https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf

Australian Law Reform Commission. (2008). *For your information: Australian privacy law and practice* (108). Available at https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

Australian Law Reform Commission. (2014). *Serious invasions of privacy in the digital era* (123). Available at https://www.alrc.gov.au/wp-content/uploads/2019/08/final_report_123_whole_report.pdf

Bergelson, V. (2003). It's Personal But Is It Mine? Toward Property Rights in Personal Information. *University of California Davis Law Review*, *37*(2), 379-452.

Brooks, R. (1998). Deterring the Spread of Viruses Online: Can Tort Law Tighten the Net. *Review of Litigation*, *17*(2), 343-392.

Bungard, M. (2020, September 7). Service NSW cyber attack: Data of 186,000 customers leaked. *The Sydney Morning Herald*. Available at https://www.smh.com.au/national/nsw/data-of-186-000-customers-leaked-in-service-nsw-cyber-attack-20200907-p55t7g.html

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy Regulation and Market Structure. *Journal Of Economics & Management Strategy*, *24*(1), 47-73. https://doi.org/10.1111/jems.12079

Carbonara, E., Guerra, A., & Parisi, F. (2016). Sharing Residual Liability: The Cheapest Cost Avoider Revisited. *The Journal Of Legal Studies*, *45*(1), 173-201. https://doi.org/10.1086/685498

Christiani, T. A. (2016). Normative and empirical research methods: Their usefulness and relevance in the study of law as an object. *Procedia - Social and Behavioural Sciences*, *219*, 201-207. https://doi.org/10.1016/j.sbspro.2016.05.006

Coyne, A. (2015, July 17). Starved of funding, resources, OAIC is left to shrivel. *IT News*. Available at https://www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273

Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, *34*(3), 477-495. https://doi.org/10.1016/j.clsr.2018.01.005

Dari-Mattiacci, G., & Garoupa, N. (2007). Least-Cost Avoidance: The Tragedy of Common Safety. *Journal Of Law, Economics, And Organization*, *25*(1), 235-261. https://doi.org/10.1093/jleo/ewm052

Darmstadt Regional Court, 13 O 244/19, 26 May 2020

Dolbow, L. (2017). Introduction: The Power of New Data and Technology. *Vanderbilt Law Review*, *70*(6), 1935-1938.

Düsseldorf Labor Court, 9 Ca 6557/18, 5 March 2020.

Frankfurt District Court, 385 C 155/19, 10 July 2020.

Geistfeld, M. (2017). Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability. *Depaul Law Review*, *66*(2), 385-412. https://via.library.depaul.edu/law-review/vol66/iss2/4

Glickman, P., Glady, N. (2015, October 14). What's the value of your data? *TechCrunch*. Available at https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

Goggin, G., Vromen, A., Weatherall, K., Martin, F., & Sunman, L. (2019). Data and digital rights: recent Australian developments. *Internet Policy Review*, *8*(1). https://doi.org/10.14763/2019.1.1390

Jamison, S. (2019). Creating a National Data Privacy Law for the United States. *Cybaris, An Intellectual Property Law Review*, *10*(2), 1-40. https://open.mitchellhamline.edu/cybaris/vol10/iss1/2.

Kecsmar, K. (2003). Contractual Solutions to the Transfer of Personal Data from Europe to Third Countries Without Providing an Adequate Level of Protection: Inventory. *International Business Law Journal*, *3*, 269-284.

Kugler, L. (2018). The war over the value of personal data. *Communications of the Association of Computing Machinery*, *61*(2), 17-19. https://doi.org/10.1145/3171580

Lim, L. (1999). Approaches to Liability for Breaches in Data Security. *Macarthur Law Review*, *3*, 81-97. http://www.austlii.edu.au/au/journals/MacarthurLawRw/1999/8.html

Lindqvist, J. (2017). New challenges to personal data processing agreements: Is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of things?. *International Journal of Law and Information Technology*, *26*(1), 45-63. https://doi.org/10.1093/ijlit/eax024

Lynskey, O. (2017). The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, *19*, 252-286. https://doi.org/10.1017/cel.2016.15

Massey, R. (2010). Outsourcing – New Standard Contractual Clauses for the Transfer of Personal Data Outside the EU. *Computer and Telecommunications Law Journal*, *16*(4), 88-89.

Meglio, M. (2020). Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation. *Boston College Law Review*, 61(3), 1223-1269. Available at https://lawdigitalcommons.bc.edu/bclr/vol61/iss3/9

Mitrakas, A. (2011). Assessing liability arising from information security breaches in data privacy. *International Data Privacy Law*, *1*(2), 129-136. https://doi.org/10.1093/idpl/ipr001

Morey, T., Forbath, T., & Schoop, A. (2015, May). Customer data: Designing for transparency and trust. *Harvard Business Review*. Available at https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

Naldi, M., Flamini, M., & D'Acquisto, G. (2013). Liability for data breaches: A proposal for a revenue-based sanctioning approach. *Network and System Security*, 264-277. https://doi.org/10.1007/978-3-642-38631-2_20

Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law and Security Review*, *34*(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026

Office of the Australian Information Commissioner. (2019, July 13). Part 4: Notifiable Data Breach (NBD) Scheme. *OAIC*. Available at https://www.oaic.gov.au/privacy

/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/

Office of the Australian Information Commissioner. (2019, September 23). Digital Platforms Inquiry final report — submission to the Australian Government. *OAIC*. Available at https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-final-report-submission-to-the-australian-government/

O'Dell, E. (2017). Compensation for breach of the General Data Protection Regulation. *Dublin University Law Journal*, *40*(1), 97-164. https://doi.org/10.2139/ssrn.2992351

Palmer, D. (2021, March 22). Microsoft Exchange Server attacks: 'They're being hacked faster than we can count', says security company. *ZDNet*. https://www.zdnet.com/article/microsoft-exchange-server-attacks-theyre-being-hacked-faster-than-we-can-count-says-security-company/

Prins, C. (2006). When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?. *SCRIPT-ed*, *3*(4), 270-303. https://doi.org/10.2966/scrip.030406.270

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

Purtova, N. (2010). Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights. *Netherlands Quarterly of Human Rights*, *28*(2), 179-198. https://doi.org/10.1177/016934411002800203

Quinn, B., & Arthur, C. (2011, April 27). PlayStation network hackers access data of 77 million users. *The Guardian*. https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

Raz, J. (2010). Responsibility and the negligence standard. *Oxford Journal of Legal Studies*, *30*(1), 1-18. https://doi.org/10.1093/ojls/gqq002

Regulation (EU) 2016/679 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 (General Data Protection Regulation) [2016] OJ L 119/1.

Reichel, J., & Chamberlain, J. (2019). The relationship between damages and administrative fines in the EU General Data Protection Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3447854

Ritter, J., & Mayer, A. (2018). Regulating data as property: A new construct for moving forward. *Duke Law and Technology Review*, *16*(1), 220-277. Available at https://scholarship.law.duke.edu/dltr/vol16/iss1/7

Samuelson, P. (2000). Privacy as intellectual property?. *Stanford Law Review*, *52*(5), 1125-1173. https://doi.org/10.2307/1229511

Selvadurai, N., Kisswani, N., & Khalaileh, Y. (2017). Strengthening data privacy: The obligation of organisations to notify affected individuals of data breaches. *International Review of Law, Computers & Technology*, *33*(3), 271-284. https://doi.org/10.1080/13600869.2017.1379368

Sidgman, J., & Crompton, M. (2016). Valuing personal data to foster privacy: A thought experiment and opportunities for research. *Journal of Information Systems*, *30*(2), 169-181. https://doi.org/10.2308/isys-51429

Smith, G., & Bloch, V. (2018, October 17). Where are all the data breach class actions in Australia? *Allens Linklaters*. Available at https://www.allens.com.au/insights-news/insights/2018/10/pulse-where-are-all-the-data-breach-class-actions-in/

Smethurst v Commissioner of Police [2020] HCA 14.

Smyth, S. (2013). Does Australia really need mandatory data breach notification laws – And if so, what kind. *Journal of Law Information and Science*, *22*(2), 159-182. Available at http://www.austlii.edu.au/au/journals/JlLawInfoSci/2013/8.html

Solove, D., & Hoofnagle, C. (2006). A Model Regime of Privacy Protection. *University of Illinois Law Review*, *2*, 357-404. Available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2080&context=faculty_publications

Spiekermann, S., & Korunovska, J. (2017). Towards a value theory for personal data. *Journal of Information Technology*, *32*(1), 62-84. https://doi.org/10.1057/jit.2016.4

Steppe, R. (2017). Online price discrimination and personal data: A General Data Protection Regulation perspective. *Computer Law & Security Review*, *33*(6), 768-785. https://doi.org/10.1016/j.clsr.2017.05.008

Stewart, A. (2001). Damages for mental distress following breaches of confidence: Preventing or compensating tears. *European Intellectual Property Review*, *23*(6), 302-304.

Stewart, M. (2005). Calculating economic damages in intellectual property disputes: The role of market definition. *The Computer and Internet Lawyer*, *22*(8), 21-28.

Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. *CSO Online*. Available at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Szydło, M. (2017). The independence of data protection authorities in EU law: Between the safeguarding of fundamental rights and ensuring the integrity of the internal market. *European Law Review*, *42*(3), 369-387.

Tâbušca, A., Tâbušca, S. M., Garais, G. E., & Enâceanu, A. E. (2018). Mobile apps and GDPR issues. *Journal of Information Systems and Operations Management*, *12*(1), 77-88.

The Privacy Act 1988 (Cth).

Timmel, S. (2012). Privacy liability and new world risks. *Franchising World*, *44*(12), 47-50.

Treaty on the Functioning of the European Union, opened for signature 7 February 1992, [2012] OJ C 326/47 (entered into force 1 November 1993).

Winder, D. (2019, August 20). Data breaches expose 4.1 billion records in first six months of 2019. *Forbes*. Available at https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=42806975bd54

Witzleb, N. (2009). Justifying gain-based remedies for invasions of privacy. *Oxford Journal of Legal Studies*, *29*(2), 325-363. https://doi.org/10.1093/ojls/gqp005