JONES DAY | One Firm Worldwide℠

WHITE PAPER

May 2019

Data Breach Class Actions in Australia

Australia has started to observe a rise in the number of data breach class actions being investigated and filed, although there has not yet been a successful data breach class action there. A range of factors are at play which support the increasing prevalence of claims relating to data breaches, and conversely there are also issues which will likely pose obstacles for claimants bringing successful data breach class actions in Australia.

This Jones Day *White Paper* explores the potential for data breach claims to be commenced, and ultimately to succeed in Australia, in addition to recent developments and trends that will likely influence the prevalence and prospects of data breach class actions in Australia. It also discusses steps businesses might take in response to the increased risk of activity in the data breach class actions space in Australia.

TABLE OF CONTENTS

A rise in the mass collection and commercial use of personal data, along with the growing potential for such data to be easily extracted, disseminated and potentially misused via new technologies, has resulted in an increasing number of data breaches. Such events have the potential to affect millions of individuals in a similar way, and raise serious concerns around privacy and data security that are often heavily publicised. These developments have resulted in the emergence of a new breed of class action, where individuals affected by data breaches, such as customers, employees and shareholders, bring group proceedings seeking remedies against the business involved in the data breach.

So-called data breach class actions have been filed in various jurisdictions, including in the United States, the United Kingdom and Canada. These claims can have a number of legal bases, depending on the nature of the relationship between the claimants and the business and the jurisdiction in which proceedings are filed. A number of data breach class actions outside of Australia have resulted in the businesses targeted agreeing to pay significant financial settlements to claimants.

In Australia, we have started to observe a rise in the number of data breach class actions being investigated and filed. However, we have not yet seen a successful data breach class action in Australia. There are a range of factors at play which are supporting the increasing prevalence of claims relating to data breaches, and conversely there are also issues which will likely pose obstacles for claimants bringing successful data breach class actions in Australia.

This Jones Day *White Paper* explores the potential for data breach claims to be commenced, and ultimately to succeed in Australia, in addition to recent developments and trends that will likely influence the prevalence and prospects of data breach class actions in Australia. It also discusses steps businesses might take in response to the increased risk of activity in the data breach class actions space in Australia.

BACKGROUND

Advancements in technology have improved businesses' ability to collect, record, store, analyse and share personal data, and deploy that data for valuable commercial purposes. Almost everyone uses products and services which record personal data, and the vast majority of this data has been created in the last 10 years. Personal data now represents a significant information asset, but it also poses new risks for businesses. In particular, the widespread prevalence of personal data has resulted in increasing concerns over data security and privacy, compliance costs and the potential for data breach.

In addition to an increase in the volume of recorded personal data and concerns around individual privacy, two other factors are working to foster an environment where data breach class actions are likely to be brought in Australia, following precedent in other jurisdictions. First, we have seen a general increase in the number of class actions commenced in Australia, and this trend is likely to continue as initiatives have been proposed that will promote the funding of such actions. Secondly, a data breach notification regime has recently been implemented in Australia which may provide a source of information that plaintiff law firms and litigation funders may seek to interrogate to identify and investigate potential claims.

Conversely, there are a number of complexities that may pose obstacles for claimants seeking to pursue data breach class actions under Australian law. Australian courts have not yet definitely recognised a right to privacy and corresponding cause of action for breach of privacy, meaning the legal basis for such actions remains unclear. Even if a legal breach can be established, losses incurred by particular individuals as a result of data breaches may be difficult to prove and quantify. This difficulty is compounded by the relative infancy of methodologies used to value personal data. Additionally, to the extent that potential claimants have entered into arbitration agreements with potential defendants to data breach class actions, those agreements might prevent claimants from bringing group action in courts.

For businesses that might be targeted by claimants, a further issue arises in relation to insurance coverage for data breaches. Practices for quantifying and pricing the insurance of data breach risk are not yet well-established, meaning the extent of a business's coverage may be contentious.

These developments are discussed further below.

INCREASING PREVALENCE OF CLASS ACTIONS IN AUSTRALIA

In recent years, there has been a rise in the number of plaintiff law firms and litigation funders investigating and pursuing class actions in Australia, as the law and practice around class actions becomes more systematised and developed.[1]

Recent developments in litigation funding more generally in the class action space will likely provide great financial backing to incentivise the filing of such class actions.[2] This includes the Australian Law Reform Commission's recommendation of the legalisation of contingency fees for lawyers in class actions, subject to court approval and supervision (discussed in a previous Jones Day *White Paper*[3]). Other more specific developments include the Supreme Court of New South Wales relaxing requirements for the commencement of multi-defendant class actions, which we have discussed in a previous article.[4]

This expansion and commercialisation of class actions has encouraged plaintiffs to pursue class actions outside more traditional areas such as product liability, disaster and financial services claims. We will comment on some of these class actions in our Review of Class Actions in Australia for 2018. One such emerging area is class actions based on data breaches.

DATA BREACHES IN AUSTRALIA

Recent data breaches involving Australian companies and companies based outside Australia have affected Australian citizens in various capacities, including as customers, users, employees and shareholders. As a result of such events, the Australian Government has introduced the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), which established a mandatory data breach notification scheme in Australia ("NDB Scheme"). The NDB Scheme was implemented in February 2018, and it has already resulted in hundreds of notifications involving significant data breaches. Further information regarding the NDB Scheme and its implications for businesses is available in our recent publication.[5]

The NDB Scheme requires agencies and organisations regulated by the *Privacy Act 1988* (Cth) to notify any affected individuals, and the Office of the Australian Information Commissioner ("OAIC"), when a data breach has occurred that is likely to result in serious harm to individuals whose personal information is involved in the breach.[6] Entities required to comply with the NBD Scheme include businesses and not-for-profit organisations with an annual turnover of $3 million or more.[7]

The OAIC publishes quarterly statistical reports about notifications received pursuant to the NDB Scheme. The most recent report relating to the period October to December 2018 was published by the OAIC on 31 December 2018.[8] The December 2018 report records that 262 data breaches involving personal information were notified during the last quarter of 2018, compared to 245 and 242 in the preceding two quarters.[9]

The leading cause of those breaches was malicious or criminal attack (168 notifications), followed by human error (85 notifications). Approximately 60 percent of notifications involved personal information of less than 100 individuals. The four industries that reported the greatest number of data breaches, in descending order, were the private health insurance sector, finance sector, legal, accounting and management services sector and private education sector.

Whilst the companies that have made notifications under the NDB Scheme are not specifically identified in the Government's quarterly reporting, we still expect that NDB Scheme may accelerate the development of data breach class actions. The NDB Scheme's requirement that affected individuals be notified of data breaches will provide a source of information that plaintiff law firms and litigation funders may seek to interrogate to identify and investigate potential claims.

General media interest in data breaches and individual privacy will likely have a similar effect in providing material for potential class actions. This year alone, Australian media reports have disclosed a significant number of potential data breaches involving entities such as Australia Post, retail provider Kathmandu, software company Citrix, Melbourne Hospital, online dating site Coffee Meets Bagel, property valuation firm LandMark White and hardware retailer Bunnings Warehouse. These recent data breaches involved a range of conduct, including recording of customers' credit card information, unauthorised downloading of personal medical data, accessing of personal identity documents, monitoring and

release of employee performance information and publication of personal contact information.

POTENTIAL LEGAL BASES FOR DATA BREACH CLASS ACTIONS IN AUSTRALIA

In Australia, there is currently no specific personal statutory right or cause of action for a claimant to make a claim in respect of a data breach. Rather, it is likely that claimants will rely upon a number of causes of action in Australian data breach class actions, depending on the nature of the claim and the character of the relationship between the claimants and the business targeted. This has been the case in the New South Wales Ambulance class action which is discussed further below, where the claimants are relying on four key causes of action.

An obvious choice for claimants lies in the common law tort for breach or invasion of privacy. However, the High Court of Australia in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* ("*Lenah*") declined to recognise a general right to privacy in Australia and corresponding tort for breach or invasion of privacy.[10] The High Court decided that an individual's privacy could be defended by reference to other laws, and that there was no reason to depart from the traditional position established by the High Court's 1937 decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* that there is no specific right to privacy in Australia.[11] This stands in contrast to other similar jurisdictions such as the United States and New Zealand, which do recognise a more general right to privacy.

However, the High Court in *Lenah* indicated that it may be receptive to arguments that a right to privacy should be recognised in the future, if such protection was limited to the privacy of a natural person (as opposed to a company). Indeed, a cause of action based on invasion of privacy has since been recognised by two lower Court decisions. In 2003, the District Court of Queensland in *Grosse v Purvis* allowed damages for breach of privacy.[12] Similarly, the Victorian County Court awarded damages for conduct that amounted to a breach of an individual's personal privacy in the 2007 decision of *Doe v Australian Broadcasting Corporation*.[13] Both cases settled before appeals could be heard, such that no appellate court has confirmed the existence of a tort for breach of privacy.

Further, other courts have shown greater caution in noting that the weight of authority is against the proposition that the tort is recognised at common law, or explaining that the position is at least unclear.[14] As such, the question of whether a common law action for breach of privacy exists in Australia remains open. Until the existence of a tort for breach or invasion of privacy in Australia is authoritatively ruled out, any class actions in Australia involving a data breach will likely include a claim for breach of privacy. This was the approach taken by the claimants in the *NSW Ambulance* class action.

There are at least two other potential common law causes of action that might be raised by claimants. First, an alleged breach of contract may arise if the conduct constituting the data breach could be interpreted as a breach of the terms of an agreement between the business involved in the data breach and the party that supplied personal data. Various class actions in the United States have involved claims for breach of contract, including those filed against Target. Secondly, claimants may also rely on negligence, if there is evidence to suggest that the company responsible for the data has not taken reasonable steps to protect it from being compromised. According to the Bryan Cave 2017 Data Breach Litigation Report, negligence is claimed in nearly 95 percent of all data breach class actions filed in United States district courts.[15]

In addition to common law causes of action, equitable causes of action available in Australia may prove a popular option for claimants. The most obvious choice here is breach of confidence, which involves three essential elements that are satisfied when the information has a necessary quality of confidence, information was imported in circumstances importing an obligation of confidence and there was unauthorised use of the information.[16] Claims for breach of confidence, being an equitable wrong, have an additional advantage for claimants, in that equitable gains-based remedies, such as an account of the defendant's profits, may be available.[17] In contrast, common law causes of action, and most statutory claims, give rise to compensatory damages based only on the loss suffered by the claimant.[18] In this way, equitable claims may pose a greater risk for defendants. If the company defending the class action has made a profit from the breach, for example by selling users' data, claimants might elect to recover those profits instead of compensation. That said, if the defendant has made no profit from the data breach, remedies for breach of confidence will likely involve equitable compensation, which will generally provide for no additional recovery beyond ordinary

common law damages. As such, the causes of action relied upon by claimants will likely depend on the circumstances surrounding the data breach.

Aside from general law bases, claims based on general statutory provisions may also provide a legal foundation for data breach class actions. This may include, for example, an allegation of misleading or deceptive conduct or breach of a company's continuous disclosure obligations. Such claims could arise, for example, in shareholder class actions based on the drop in share price caused by a major data breach involving the company, if there was evidence to suggest that the company misrepresented its ability to prevent and manage data breaches.

If a major data breach class action proceeds to judgment in Australia, claimants and potential defendants will have greater clarity regarding the causes of action upon which such claims might be based, and corresponding remedies available to claimants.

COMMENCEMENT AND INVESTIGATION OF DATA BREACH CLASS ACTIONS IN AUSTRALIA

At least three data breach class actions have been filed or investigated in Australia in the past five years.

In December 2017, a class action was filed against the New South Wales Ambulance service in the Supreme Court of New South Wales on behalf of ambulance employees and contractors whose sensitive health and personal information was the subject of a mass data breach in 2013. The data breach involved a NSW Ambulance contractor unlawfully accessing and selling the workers' compensation files of 130 former and current employees to personal injury law firms. The claimants have alleged that NSW Ambulance is liable for breach of confidence, breach of contract, misleading and deceptive conduct and invasion of privacy, as a result of its failure to adequately protect the personal records of its employees.[19] Solicitors acting for the class have suggested that damages could reach "millions of dollars", with class members seeking compensation for pain and suffering, psychological injuries and economic loss.[20]

NSW Ambulance filed a Defence to the action on 8 May 2018. Part of NSW Ambulance's Defence involves a denial that the claimants have any relevant right to privacy, or that a cause of action exists in respect of a tort of privacy.[21] Given the apparent disagreement as to whether such a tort exists, the NSW Ambulance class action, if it proceeds to judgment, may provide an opportunity for judicial consideration of whether Australian law recognises a general right to privacy.

The same firm representing the claimants in the *NSW Ambulance* class action is currently investigating a potential class action for breach of privacy in relation to the PageUp data breach that took place in May 2018.[22] PageUp is a software provider used by various organisations, including Australian companies, for managing job applications. Recently PageUp notified their customers that their software had been hacked and personal details of thousands of job applications may have been compromised. Proceedings against PageUp have not yet been filed.

In 2018, litigation funder IMF Bentham and compensation law firm Shine Lawyers investigated a potential class action against a social media company in relation to breaches of the *Privacy Act 1988* (Cth), and lodged a representative complaint with the OAIC.[23] The alleged breaches related to unauthorised access to users' profiles and information by political consulting firm Cambridge Analytica when personal data was collected through a software application downloaded by social media users. After conducting the investigation, Shine Lawyers stated that they had formed the view that consumers would not benefit from the commencement of a class action, and so proceedings were not filed.[24] The company is currently facing a number of large-scale class actions outside of Australia, however, some of which are discussed further below.

PRECEDENT OUTSIDE AUSTRALIA

Unauthorised disclosure of personal data has given rise to successful data breach class actions in the United States, the United Kingdom and Canada. Claimants have included consumers whose personal information was the subject of the breach, and financial institutions and credit card providers that have incurred losses relating to the breach. Such losses have included the risk of identity theft and fraud, restitution for fraudulent transactions and costs associated with monitoring for potential fraud. As with most class actions, ordinarily such claims are resolved out of court and entail a significant financial settlement paid by the company associated with the data breach.

The success of claimants in bringing data breach class actions in other jurisdictions will likely prompt similar activity in Australia. That said, recognition of invasion of privacy as an actionable legal wrong is generally broader in the United States compared with Australia, and the right to privacy is protected by hundreds of state laws relating to particular types of information. As such, claimants in any Australian proceedings may experience greater difficulty in successfully establishing an entitlement to remedies as a result of a mass data breach.

United States

Some of the most significant data breach class actions in the United States have involved claims against Target, a company that provides web services, a consumer reporting agency company and a social media company.

Multiple class actions were filed in the United States against retail company Target by consumers, financial institutions and shareholders after a 2013 cyberattack resulted in the credit card and personal contact information of millions of customers being compromised. The class actions resulted in significant financial settlements of US$10 million with affected consumers, US$39 million with claims brought by banks, $67 million with Visa and $39 million with Mastercard.[25] The shareholder class action, in which the claimants alleged that Target's directors had breached their fiduciary duties, was eventually dismissed.[26]

A company that provides web services has been the subject of class actions relating to three data breaches that occurred between 2013 and 2016, which ultimately settled. The breaches were varied in nature but generally involved the hacking of users' account login details and contact information, some of which was eventually published on the internet, and led to the compromise of billions of user accounts. The company's shareholders brought derivative litigation against the company's directors and officers, alleging that the company had made false and misleading statements to the market about its policies to prevent data breaches. This action resulted in a settlement of US$29 million earlier this year that was approved by the Superior Court of California.

Class actions were also brought by consumers from a range of jurisdictions on numerous legal bases. The company originally attempted to settle the consumer class actions for approximately US$50 million. However, on a recent application for approval of the settlement, the judge criticised and ultimately rejected the settlement, stating that the terms were not "fundamentally fair, adequate, or reasonable". The company has since revised its settlement figure to US$117.5 million, which is still subject to judicial approval.

More than 200 lawsuits have been filed against a consumer reporting agency company as a result of a mass data breach involving cybercrime identify theft that took place in 2017, including by individuals, payment card issuers and small businesses. Those lawsuits have predominately been consolidated into one case that will be heard by the U.S. District Court for the Northern District of Georgia, where the company is based. Information accessed by the hackers included personal identity information and credit card information. One class action relating to the breach seeks US$70 billion in damages, which if successful would make it the largest class action in United States history. The claimants alleged that the company knew of severe deficiencies in their data security systems but failed to take reasonable measures to prevent a data breach.

A class action has been filed by various companies registered in the United States and the United Kingdom against the social media company referred to above in relation to the Cambridge Analytica breach.[27] The complaint alleges that various U.S.- and UK-based defendants are guilty of fraud, negligence and statutory violations in relation to the personal information of approximately 87 million social media users, 70.6 million of whom were in the United States and 1 million of whom were in the United Kingdom. It claims that the users' personal information was improperly accessed by a number of entities without users' knowledge, consent or authorisation. Such information included users' names, contact details, demographic information and political and religious affiliations.

Further, and separately from the Cambridge Analytica breach, a class action has been filed against the same social media company in the U.S. District Court for the Northern District of California in relation to the hacking of account credentials of millions of users in 2018.[28]

Other targets in the United States include, among many others: a fast food chain in relation to a 2015 and 2016 data breach that affected the company's point-of-sale systems, which was

also eventually settled; health insurance provider AvMed in relation to stolen data of more than one million customers; and a hotel chain in relation to a data breach which exposed the personal information of more than 300 million guests.

United Kingdom

Companies in the United Kingdom, like Australia, are subject to a mandatory data breach notification regime. Article 33 the EU General Protection Regulation 2016/679 ("GDPR") imposes an obligation on companies to notify supervisory authorities of any personal data breach without undue delay. It also includes rights which may make it easier for claimants to bring compensation claims and provides sanctions for non-compliance including revenue-based fines. Article 82(1) of the GDPR provides: "Any person who has suffered material or non-material damage as a result of an infringement of this regulation shall have the right to receive compensation from the controller or processor for the damage suffered". It is generally thought that the implementation of the GDPR, and particularly the express right to compensation in Article 82, will increase the likelihood of successful data breach class actions in the United Kingdom.

The Court of Appeal upheld the United Kingdom's first successful data breach class action in October 2018.[29] Supermarket chain Morrisons was found vicariously liable to more than 5,000 current and former Morrisons employees for the actions of a disgruntled employee, who published over 100,000 employees' bank account details and personal contact information on the internet. The Court of Appeal refused Morrisons permission to appeal to the Supreme Court, stating that the solution to such class actions resulting from "data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment" was to "insure against such catastrophes".[30]

Conversely, the High Court has refused to grant leave to serve a claim on a technology company outside of the English jurisdiction in relation to alleged use of cookie technology on an internet browser to obtain information about the internet activity of users.[31] The High Court found that the claim did not have reasonable prospects of success, as the claimants had not established that they suffered relevant damage. Alternatively, the court held that the claim could not continue as a representative action because members of the class did not have the same interest, within the meaning of English civil procedure requirements.

In terms of class actions being currently investigated, there have been reports that a UK-based class action is being investigated in relation to the Cambridge Analytica breach.[32]

Plaintiff law firm SPG Law has announced two potential class actions against airlines. The first is a £500 million class action against British Airways which may be brought under Article 82 of the GDPR.[33] The action is in relation to a data breach that compromised British Airways' security systems and led to the personal data of more than 380,000 customers being leaked, including contact details and credit card numbers The second is a proposed class action against airline Cathay Pacific in relation to a similar data breach, though allegedly involving an even more extensive compromise of personal data.[34]

Canada

In Canada, a class action lawsuit was brought against a home improvement retail company in relation to a 2014 data breach that resulted in the retailer's self-checkout systems being compromised, resulting in unauthorised access to over 50 million customers' credit card details. Damages were sought under a wide range of causes of action including those involving breach of confidence, breach of fiduciary duty, breach of privacy, breach of contract and negligence. The damage was said to result from an increased risk of credit card fraud and the inconvenience of monitoring for such fraud. In settlement of the proceedings, the company has agreed to establish a C$13 million settlement fund to compensate affected individuals.

Other Canadian class actions that have resulted in significant settlements include the *Human Resources and Skills Development Canada* class action, in which a C$17.5 million settlement was paid in relation to a data breach involving loss of an external hard drive containing personal information of student loan borrowers.[35]

POTENTIAL IMPACT OF ARBITRATION AGREEMENTS FOR DATA BREACH CLASS ACTIONS

As discussed above, mass data breaches are likely to affect individuals in their interactions with companies, including employees and consumers. These individuals will likely have individual contracts with the company, and such contracts

commonly include agreements to arbitrate disputes between the individual and the company. In the United States, such arbitration agreements have created obstacles for individuals seeking to bring class actions against companies. This is because exclusive arbitration agreements exclude the jurisdiction of courts and compel private arbitration, which normally does not involve group action. Further, some arbitration clauses include specific "class action waivers", which expressly provide that claimants can engage in only individual arbitrations with the company.

In the recent decision of *Lamps Plus, Inc. v. Varela*, the United States Supreme Court decided that an arbitration clause barred a class action, and that it was unlawful to require class arbitration where the arbitration agreement did not directly address the availability of a group action.[36] In *Lamps Plus*, this meant that employees who had been victims of a data breach involving the disclosure and misuse of their tax filings were required to arbitrate their claims individually. This follows the Supreme Court's 2011 finding in *AT&T Mobility LLC v. Concepcion* that consumers who had entered into an arbitration agreement that contained a class action waiver upon purchase of a mobile phone were barred from bringing a class action regarding tax payable in respect of that purchase.[37] Class action waivers have also been upheld in Canada.[38]

In Australia, we have not yet seen litigation around the impact of arbitration agreements for class actions, and the issue of whether group arbitration can be ordered remains unclear. Further, the inclusion of specific class action waivers in arbitration clauses is not yet common practice in Australia. Based on the current position in the United States, arbitration agreements may be used by defendants as a shield to require claims around data breaches to be heard as private arbitral proceedings, as opposed to public data breach class actions heard in a court setting. As in other jurisdictions, agreements to arbitrate disputes are generally recognised by Australian courts as legitimate and enforceable under ordinary principles of freedom of contract.

However, arbitration agreements being deployed to limit group action following data breaches may be challenged on various bases. Australian courts would assess the enforceability of arbitration agreements in this context in accordance with the usual rules around the validity of contracts. In this way, challenges will likely be made on the basis of unconscionability, including under section 23 of the Australian Consumer Law, which provides that "unfair" terms in consumer contracts are void. Australian law also renders certain arbitration agreements void, including compulsory arbitration agreements in insurance contracts entered into before a dispute arises.[39]

QUANTIFICATION OF LOSS IN DATA BREACH CLASS ACTIONS

A critical issue in many data breach class actions will be the quantification and proof of losses allegedly suffered by the plaintiffs and group members. This may include calculation of the losses flowing from unauthorised access or disclosure of personal data, and consideration of the potential value of that data. In some cases, such as when identity theft leads to direct financial losses from an individual's bank account, or when a data breach has resulted in a measurable decline in share price, quantification of loss may be relatively straightforward. However, in other cases, such as where an individual's sensitive personal details are disclosed, it may be more difficult to measure potential future losses or non-financial forms of harm—for example, damages associated with harm to an individual's reputation.

As an intangible asset, data may be difficult to value compared with other traditional assets which are subject to more established and conventional accounting practices. However, growing recognition of the many ways in which businesses can leverage data as a valuable asset has led to progress being made to develop techniques for the valuation of data from an accounting perspective. Such approaches include, for example, adopting accounting practices that are analogous to other assets that embody future economic benefits, such as intellectual property and goodwill. Specific valuation measures that have been proposed for valuing data include a consumption-based approach;[40] a three-prong approach considering the asset value, activity value and expected future value;[41] and income-based valuations.[42] The development and approval of accounting principles for valuing data will likely assist claimants in quantifying losses, including by reference to the financial statements of defendants that specify an asset value for data.

In addition to calculation issues, other general limits on the availability of compensation may create hurdles for recovery in data breach class actions. In the United States, courts

have drawn a distinction between existing and ongoing damage or loss and the mere risk of future harm, which has been found to be too speculative and not a concrete and immediate injury sufficient to confer standing to bring proceedings.[43] The general position on the availability of damages is similar in Australia, in that compensable damage cannot be established by reference to a potential loss that may or may not occur in the future.[44] If arguments of this kind are used in the Australian courts, this may limit the losses that can be claimed in data breach class actions and discourage their pursuit in Australia.

RISK AND INSURANCE ISSUES

Given the number of technical variables involved, quantification and prediction of the risks associated with the storage and use of data, and the probability of a data breach, is not straightforward. As with other aspects of cybersecurity quantification, techniques to quantify data breach risks within businesses are currently being developed and refined. One such method is known as Factor Analysis of Information Risk ("FAIR"). The FAIR model provides a framework for considering the factors that contribute to risk and how they affect each other, in order to predict the potential frequency and magnitude of data security events.[45]

As these frameworks develop, companies will be internally documenting data security risks. These documents may become key evidence for plaintiffs in class actions. For example, they may be used to suggest that a company has not followed industry practice in monitoring and protecting data security, that the company recognised mass data breach risks and failed to address them or that the company underestimated the risk of a data breach and as a result dedicated insufficient resources to minimising such risk. As such, companies should be mindful of the use to which data security policies and related documents might be put in litigation.

Related to issues around quantifying and forecasting security risks is the immaturity of the insurance market in Australia for cybersecurity. As a consequence of rapid change in the area, insurers are finding it difficult to price against the risk of cybersecurity incidents, including data breaches. As noted above in relation to the *Morrisons* case, the English Court of Appeal has expressed its view that the "solution" to the increased risk of data breaches is to insure against such events. This position will likely be mirrored in other common law jurisdictions. However, companies may also encounter difficulties in assessing whether they are adequately insured for the potential losses that may result from a data breach. As such, litigation around data breaches will likely involve complex issues regarding the types of incidents that are covered by a company's insurance, and the extent of any such coverage.

Given the increasing prevalence of shareholder class actions, and that class actions outside Australia have involved claims against directors for breach of duty arising from data breaches (as in the class actions against Target and the web services company discussed above), other complexities may arise in relation to directors and officers liability insurance for claims arising from data breaches.

IMPLICATIONS FOR AUSTRALIAN BUSINESSES

- Australian businesses should take appropriate preventative measures to prevent data breaches where possible.
- It is important to be conscious of the types of data breaches that may give rise to the type of public concern that may instigate a class action, and to ensure that adequate systems are in place to minimise the prospects of such breaches occurring.
- It will be important to have clear data security policies and response plans in place, and to ensure that such procedures are followed. This will assist in defending against an argument that a business has not taken reasonable steps to prevent and manage data breaches, or has not followed industry practice in relation to data security.
- In the event that a data breach does occur, businesses should take immediate steps, where possible, to contain and investigate the breach, and to notify affected individuals in accordance with the NDB Scheme. Given the potential for steps taken following the breach to be discoverable in any subsequent class action or other litigation, it will be important to consider how those steps are taken and whether the investigations should be undertaken by external legal advisors for the purposes of taking legal advice about the business's obligations and potential exposure.

- Given the difficulties with insurance coverage discussed above, businesses might consider conducting a review of their current insurance policies in light of the potential types and magnitude of data breach class actions to assess whether their level of coverage is adequate.

FIVE KEY TAKEAWAYS

1. As the number of class actions in Australia continue to rise, and the breadth of claims that are the subject of class actions expand, we expect that further class actions based on data breach will be filed in Australian courts, following the trend in overseas jurisdictions.
2. The recent introduction in Australia of a statutory data breach notification scheme may accelerate the development of data breach class actions.
3. The legal bases for Australian data breach class actions have not yet been considered by the Australian courts. Data breach class actions can potentially be based on a broad range of causes of action, providing claimants with an opportunity to seek a variety of remedies.
4. One obstacle to the potential for class actions to yield meaningful remedies for claimants is the critical question of the loss caused to an individual whose data is disclosed by reason of a breach. Even if claimants meet the requirements of a particular cause of action, as with ordinary claims for compensation, individuals will need to proffer evidence of direct loss suffered as a result of the data breach, which may be difficult to quantify.
5. Companies should be mindful of the potential increase in activity in the data breach claims space and should consider taking preparatory steps, including by establishing detailed procedures for responding to data breaches and reviewing their current insurance arrangements.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

John Emmerig
Sydney
+61.2.8272.0506
jemmerig@jonesday.com

Michael Legg
Sydney
+61.2.8272.0720
mlegg@jonesday.com

Adam Salter
Perth
+61.8.6214.5720
asalter@jonesday.com

Daniel Moloney
Melbourne
+61.3.9101.6828
dmoloney@jonesday.com

Stephanie Crosbie
Sydney
+61.2.8272.0707
scrosbie@jonesday.com

ENDNOTES

1 *See*, for example, Marsh Report, "Shareholder class actions shaping the future of Australia's D&O insurance landscape" (August 2017); Australian Institute of Company Directors, "The growing impact of rising shareholder class actions" (27 September 2018).

2 Australian Law Reform Commission, *Inquiry into Class Action Proceedings and Third-Party Litigation Funders* (Discussion Paper no 85, 24 May 2018).

3 Jones Day, "Australian Law Reform Commission Releases Class Action and Litigation Funding Report" (March 2019).

4 Jones Day, "Supreme Court of New South Wales Relaxes Requirements for Class Actions" (April 2019).

5 Jones Day, "Key Lessons from Australia's Notifiable Data Breach Scheme" (April 2019).

6 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) sections 26WE, 26WL.

7 *Privacy Act 1988* (Cth) sections 6C, 6D.

8 Office of the Australian Information Commissioner, *Notifiable Data Breaches Quarterly Statistics Report: 1 October–31 December 2018* (7 February 2019).

9 Office of the Australian Information Commissioner, *Notifiable Data Breaches Quarterly Statistics Report: 1 July–30 September 2018* (30 October 2018); Office of the Australian Information Commissioner, *Notifiable Data Breaches Quarterly Statistics Report: 1 April – 30 June 2018* (31 July 2018).

10 (2001) 208 CLR 199.

11 (1937) 58 CLR 479.

12 *Grosse v Purvis* [2003] QDC 151.

13 *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

14 *Kalaba v Commonwealth of Australia* [2004] FCA 763 (8 June 2004) 6; *Chan v Sellwood; Chan v Calvert* [2009] NSWSC 1335 (9 December 2009) [34]; *Sands v State of South Australia* [2013] SASC 44 (5 April 2013) [614]; *Doe v Yahoo!7 Pty Ltd* [2013] QDC 181 (9 August 2013) [310]–[311].

15 Bryan Cave, *2017 Data Breach Litigation Report*.

16 *Coco v A N Clark (Engineers) Ltd* [1968] F.S.R. 415, 419; *Commonwealth of Australia v John Fairfax & Sons* (1980) 147 CLR 39, 51.

17 *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB) (2008); *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109; *Douglas v Hello! Ltd* [2005] EWCA Civ 595 (18 May 2005). The Australian Law Reform Commission has also recommended that courts be empowered to award an account of profits, at least for serious invasions of privacy, to "deter defendants who are commercially motivated to invade the privacy of another for profit": see Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Discussion Paper no 80, 31 March 2014).

18 *See*, for example, *Robinson v Harman* (1848) 1 Ex Rep 850; *Livingstone v Rawyards Coal Co* (1880) 5 App Cas 25.

19 See Amended Statement of Claim filed on 27 March 2018.

20 *Sydney Morning Herald*, "Paramedics launch class action over the sale of their medical records to personal injury solicitors" (18 November 2017).

21 See Defence filed on 8 May 2018.

22 Centennial Lawyers, "PageUp Data Breach".

23 IMF Bentham, "IMF Bentham launches representative action against Facebook for privacy breaches" (10 July 2018).

24 Shine Lawyers, "Facebook Class Action".

25 *In re: Target Corporation Customer Data Security Breach Litigation*, U.S. District Court, District of Minnesota, No. 14-md-02522.

26 *In re: Target Data Security Breach Litigation,* No. 14-cv-203, decision of Judge Magnuson on various Motions to Dismiss (7 July 2016).

27 *See* case filed by plaintiffs Ben Redmond, Lindsay Rathert, Salvador Ramirez, Gerry Galipault, Kyle Westendorf, Robert Woods and Jordan Hunstone on 10 April 2018 against Facebook, Inc., Cambridge Analytica LLC and others (U.S District Court, District of Delaware).

28 *See* case filed by plaintiffs Carla Echavarria and Derrick Walker on 28 September 2018 against Facebook, Inc., Case 5:18-cv-05982 (U.S. District Court, Northern District of California).

29 *WM Morrisons Supermarkets Plc v Various Claimants* [2018] EWCA Civ 2339.

30 *WM Morrisons Supermarkets Plc v Various Claimants* [2018] EWCA Civ 2339, at [78] (per Sir Terence Etherton MR, Lord Justice Bean and Lord Justice Flaux).

31 *Lloyd v Google LLC* [2018] EWHC 2599 (QB).

32 *See*, for example, "Facebook's Cambridge Analytica woes continue with UK lawsuits"; "UK Group Threatens To Sue Facebook Over Cambridge Analytica".

33 SPG Law, "Our Cases".

34 SPG Law, "Our Cases".

35 Canada Student Loans Privacy Breach Class Action—Notice of Settlement Approval.

36 *Lamps Plus, Inc., et al. v. Varela* 587 U.S. ____ (2019).

37 *AT&T Mobility LLC v. Concepcion* 563 U.S. ____ (2011).

38 *Insurance Contracts Act* 1984 (Cth) section 43.

39 *Murphy v Amway Canada Corporation* 2013 FCA 38.

40 Reply company, "The Valuation of Data as an Asset: A Consumption-Based Approach".

41 *MIT Sloan Management Review*, "What's Your Data Worth?" (3 March 2017).

42 Chloe Mawer (Silicon Valley Data Science), "Valuing Data is Hard" (10 November 2015).

43 *See Reilly v Ceridian* 664 F.3d 38, 43 (3rd Circ. 2011)); *Whalen v. Michael Stores Inc*., 689 Fed.Appx. 89 (2d Cir. 2017); *In re SuperValu, Inc. Customer Data Breach Litig*., 870 F.3d 763 (8th Cir. 2017).

44 See *Tabet v Gett* (2010) 240 CLR 537.

45 FAIR Institute.