sparke HELMORE LAWYERS

Half-Yearly

Cyber Wrap Up

JUN 2023 ISSUE 1

IN THIS ISSUE

Jehan Mata

Partner
Sparke Helmore

Welcome to our half-yearly cyber update, aimed at keeping you at the forefront of issues and legislative changes and impacts in the fast-paced world of cyber. In this update, we:

- undertake a review of the Australian cybersecurity reforms and landscape
- pose the question, is data security the next big class action trend; and
- explore the tort of privacy.

We hope you find this mid-year update informative and useful. If there are any topics you would like us to cover in future, please contact Jehan Mata.

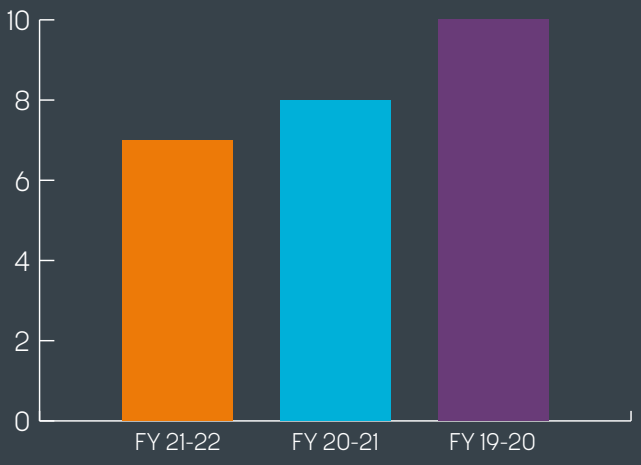
DATA ABOUT HANDLING DATA: A REVIEW OF THE AUSTRALIAN CYBERSECURITY REFORMS AND LANDSCAPE

Author: Partner Jehan Mata
Acknowledgment: Adem Murtic, Georgia Mineo and Georgie Aidonopoulos

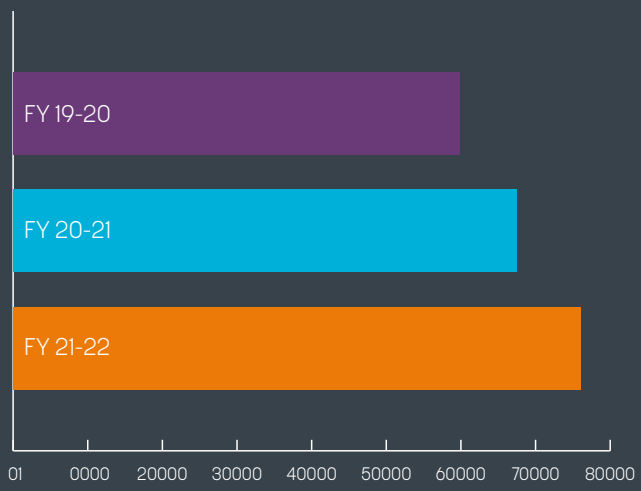
Falling victim to a cybercrime is becoming inevitable. This could be on a grand scale, (such as recent large-scale breaches of financial and health sector organisations where data has been compromised) or on a smaller scale (by clicking a malicious link in an email, which corrupts files on a computer), but everyone will experience a cybercrime in some capacity.

In 2021-22 year alone, one cybercrime was reported to the Australia Cyber Security Centre (**ACSC**) every seven minutes on average, compared to one report every 10 minutes in 2019-2020. Cybercrimes are becoming a daily occurrence and statistics published by the ACSC illustrate that the prevalence of cybercrimes is growing at a steady rate.

Cybercrime Reports - per minute



Cybercrime Reports - Number of reports



Clearly, the need for cyber security reforms is more crucial than ever. Australia has seen a range of reforms and proposals in the last few years in an attempt to tackle these issues.

Attorney General cyber security reforms

The reforms can be summarised into four main obligations.

1. **Review your reporting obligations:** SMEs should proactively familiarise themselves with reporting requirements, procedures and guidelines considering the likely removal of the SME exemption within the Act.

2. **Know your data:** All entities, regardless of size, need to be managing data, having robust systems and procedures in place to protect data; and be constantly reviewing and deleting any unnecessary or outdated data. The change to the net-profit cap means that all entities, regardless of size or the sophistication of the data management processes, are subject to increased risk and scrutiny when considering data breaches.

3. **Plan and prepare:** All entities should be proactive, adopting a "when, not if" approach to cyber breaches. After all, if the past year has shown us anything, it is that entities both big and small are at risk of cyber breaches. Current data shows that insufficient planning and preparedness is still the single biggest barrier to cyber resilience today. We strongly encourage entities to implement and frequently test their response procedures. Systems should also consider the risk of indirect data compromise and having systems or policies in place to respond in the event their data is compromised while being held with another company.

4. **Prepare for Incident response and Disaster recovery:** Entities should also be looking forward to the steps they need to take following a cyber-attack. This includes knowing reporting requirements and having appropriate safeguards, which includes proper cyber insurance.

Australia's Cyber Security Strategy (**ACSS**) has highlighted its key expectations of businesses and their responsibility to increase security against cyber threats. These expectations are summarised below.

Improving baseline security for critical infrastructure

The responsibility of entities to improve their security for critical infrastructure is not only a significant undertaking, but a failure to do so can be catastrophic. In practice, this reform creates an obligation for enhanced security operations for a critical service provider, and a potentially enforceable action should they fail to do so. For further information about these reforms, please refer to our previous articles discussing the *Security of Critical Infrastructure Act* 2018.

Providing secure products and services

The increasing number of 'connected devices' has been identified by the ACSS as a significant risk factor in the cyber sphere. Beyond releasing a Voluntary Code of Practice on the provision of secure products and services, the ACSS has indicated its intention to design supply chain principles for decision makers and suppliers. The aim of undertaking this is to improve integrity, transparency, security and procurement practices throughout the supply chain process. For further information regarding supply chains, please refer to our previous article.

Upskilling the workforce

This initiative aims to provide a larger pool of cyber-savvy professionals to be available for the broader Australian workforce, from SMEs to large entities and agencies. In doing this, policymakers seek to ensure the Australian workforce is empowered to implement the aims of the broader reforms. The initiative includes education programs for future members of the Australian workforce, as well as delivery of programs and training to upskill those already in it.

Uplifting the cyber security of SMEs

While it is typically telecommunication entities and financial institutions that have made headlines for cyber-attacks, SMEs are particularly vulnerable targets in this space due to their comparative lack of resources and the consumer's notion that SMEs 'fly under the radar' compared to large Australian businesses.

Having identified this vulnerability, the ACSS has committed to a cyber program to assist these SMEs, as well as online training and a 24/7 helpdesk for SMEs requiring cyber security advice and assistance. This support provides SMEs with the opportunity to report

and seek advice on cyber risks in real-time. In 2021-22 there were over 25,000 calls to the Cyber Security Hotline an average of 69 per day, and an increase of 15 per cent from the previous financial year. The goal is to take proactive steps to block malicious activity not only at a large scale, but also for smaller security risks evident in the operations of SMEs.

Furthermore, there have been amendments proposed in relation to SMEs under the *Privacy Act* (1988) (the **Act**). The proposed reforms to the Act are discussed in our previous article here. Currently, businesses or agencies with a turnover of $3 million or less per year are excluded under the Act, subject to some carve outs. The reforms recommend that the small business exemption of the Act is removed once the following have been put in place:

- an impact analysis, development of appropriate support
- an appropriate way for small business to meet obligations proportionate to risk is developed, and
- small businesses are in a position to comply with the obligations.

The report states that the main reason behind this reform is that when the exemption was carved out in 2000, SMEs were thought to pose little to no risk to the privacy of individuals. This is no longer the case.

We are of the opinion that the removal of the exemption will increase transparency and accountability for customers whose data is stored with SMEs. The reforms will also assist SMEs recover quickly from cyber breaches as the increased regulatory framework will ensure that they are cognisant of the data they manage. This will likely have flow on impacts relating to supply chain attacks as SMEs have notoriously been regarded as the 'weakest link' and the 'soft underbelly' in supply chains. Through increasing the regulatory framework, this should limit the amount of successful supply chain attacks.

As a signification portion of the market will now be captured under the Act, this means insurers and insureds will need to be vigilant with their data management practices in a way they were not required to before. Insurers should also be reviewing policies offered to SMEs to ensure that if they wish to exclude third party losses incurred through contractual liabilities and/or reputational costs, that they make requisite changes now.

The reform also aligns with the shift in how storing data has been viewed. Historically, storing data was seen as control and useful to an entity's interests. Considering the ever-growing list of entities that have fallen victim to a cyber-attack, this mentality is shifting, and businesses are beginning to see the benefit of knowing the data they hold and only keeping what is necessary for as long as necessary.

A major risk with storing so much data is that entities are unlikely to know the particulars of all the data they store, meaning that when a cyber breach occurs, most of the time in the incident response phase is spent attempting to figure out what data was held. In such circumstances, it takes longer for IT teams to discover what data has been compromised, which may result in missing key notification deadlines. This is relevant to SMEs as even local coffee shops hold customer data and payroll information and this recommendation will require SMEs to take stock of what data they have and what data they can delete.

Regardless, it cannot be overlooked that if these proposals are adopted, this will drastically increase compliance costs and add to the complexity of the cyber security patchwork of legislation. This means that for business owners to adhere to their new privacy obligations, they will need to be across the proposed changes.

The management of data is now more important than ever for SMEs in all industries across Australia. As always, the biggest take-away for SMEs is that prevention is better than a cure. Please refer to our previous Cyber Update – Issue 1 for further tips on what actions SMEs can take to limit the risk of cyber breaches.

A further reform to the Act we think warrants discussion is the tort of privacy. The conversation around the need for a "right" to privacy is not new. In 2014 and 2019, the Australian Law Reform Commission (**ALRC**) and Australian Competition and Consumer Commission (**ACCC**) both called for the introduction of a statutory right to privacy, however this was never implemented. As we have seen with the recent data breaches on telecommunication companies and financial institutions, cybercrimes are increasing in frequency and severity and Australian consumers, regulators and legislatures are eager to hold businesses accountable.

This proposal recommends the introduction of a statutory tort for serious invasions of privacy that are *intentional* or *reckless*. Importantly, the invasion does not need to cause *actual* damage and individuals may claim damages for emotional distress. In addition to this, it is also suggested that the Office of the Australian Information Commissioner (**OAIC**) should be able to appear as an impartial adviser to the court and intervene in proceedings with leave of the court for both the direct right of action under the Act and the tort for invasion of privacy.

If this proposal passes, individuals will have greater success in bringing cyber relation claims within Australian courts. To date, redress available to victims within Australia has been limited to the powers available to the OAIC due to the absence of a right to privacy.

As it stands, an individual or class of people who want to initiate proceedings for a cyber breach within an Australian court faces two significant hurdles – an absence of a clear cause of action and difficulties in quantifying their loss. This proposal would remove both of those hurdles.

As we forewarned in February, if the tort of privacy is introduced, the right to privacy has the potential to open the floodgates for class actions. If this does happen, it could have costly impacts on not only a business' pocket but their reputation, too.

What this means for the market

The market needs to familiarise itself with how compliance and enforcement procedures have changed in the cyber space. The market also needs to be cognisant of what level of cyber preparedness is required to comply with the increased obligations. Insurers and brokers specifically will also need to familiarise themselves with these issues and expectations to ensure they are adequately educated and providing the most up to date coverage advice to policyholders or would-be policyholders. A failure to do so could lead to claims made against them based on their financial advice to policyholders (and any perceived loss suffered as a result). It is likely we will start to see an increased plaintiff appetite as an avenue to pursue when there are questions surrounding coverage in the broader insurance space.

Now is the time for Australian businesses to strengthen their cyber security defences and build cyber resilience given the increasing appetite for litigation and the increasing regulatory requirements. We understand this can be difficult terrain to navigate. We encourage all entities to reach out and seek assistance where necessary to ensure they are as prepared and protected as possible. The last few months have illustrated that no company or person is safe from threat actors. Therefore, these reforms could not come at a more important time. We will continue to provide updates as the situation is evolving.

LIGHTS. CAMERA. CLASS ACTION! IS DATA SECURITY THE NEXT BIG CLASS ACTION TREND?

Author: Partner Jehan Mata
Acknowledgment: Georgia Mineo and Georgie Aidonopoulos

In Australia we have seen a 26% increase since the second half of 2022 in large scale data breaches, with millions of Australian and foreign consumers impacted. Understandably, the Australian Government, regulators and victims are eager to hold businesses accountable. To date, redress available to victims within Australia has been limited to the powers available to the Office of the Australian Information Commissioner (OAIC). Recent proceedings suggest that this could all be about to change.

Specialist privacy lawyers have forewarned in recent years that Australian businesses should prepare for the costly impact of cyber breach class actions. In recent years, cyber breach class actions have been seen in foreign jurisdictions, such as the US and UK. It is now a question of when, not if, similar actions will be seen here. For example, five class actions have been filed in response to the Medibank data breach of 2022, where 9.7 million current and former customers had their personal information leaked onto the dark web. A further class action has been recently filed in the Federal Court against Optus.

Historically, Australia has not had any class actions relating to data breaches, as collective actions for data breaches have been commenced via the OIAC with a plaintiff law firm making a representative complaint. This requires the OAIC to then investigate and the complaints made to date have been slow to be finalised. Therefore, the announcement of the Medibank class action filed in the Federal Court by Baker McKenzie is significant as it centres around the organisation's alleged failure to protect customer privacy.

In order to succeed in a class action, claimants must satisfy the necessary threshold requirements of the Federal Court of Australia regime:

- seven or more people have claims against the same person(s)
- the claims are in respect of, or arise out of, the same, similar, or related circumstances, and
- the claims give rise to at least one substantial common issue of law or fact.

It is that last limb that has to date been a significant hurdle in relation to class actions following large scale data breaches.

Further issues remain about the basis for compensating for such a breach. One issue that remains unresolved under Australian law is whether damages for a data breach are payable for non-economic loss and the basis for such a loss. The key question regarding the viability of data breach class actions will be whether victims are entitled to enough damages to make collective action economically viable for the plaintiff lawyers and litigation funders prepared to take on these cases. The uncertainty regarding the availability of damages is probably the reason for the decision of other plaintiff law firms to make a representative complaint to the OAIC, as the OAIC does have the power to award damages for non-economic loss for hurt and humiliation caused by a data breach.[1]

In the Medicare class actions, the claimants are seeking damages for distress, frustration, and disappointment. Recently in *Moore v Scenic Tours Pty Ltd* [2020] HCA 17, the High Court confirmed that damages for disappointment and distress are available to consumers for breaches of consumer guarantees for travel and recreational contracts. The High Court held that damages for disappointment are not damages for personal injury and are an exception to the rule that damages for emotional harm require a psychiatric injury to be suffered. However, the principle of disappointment damages has yet to be confirmed as available in the circumstances of a data breach and it remains uncertain whether such damages are available outside the particular context of the travel industry.

There are limited common law precedents for the availability of damages for hurt and humiliation. England's *Court of Appeal in Google v Vidal-Hall* [2015] EWCA Civ 311 determined that claimants could claim damages for distress without having to prove pecuniary loss. However, a subsequent appealed to the Supreme Court was withdrawn before the matter was heard and determined. Recently in *Reed, Michael v Bellingham, Alex (Attorney-General, intervener)* [2022] SGCA 60 Singapore's Court of Appeal held that emotional distress directly suffered as a result of a contravention of the *Personal Data Protection Act 2012* may constitute "*loss or damage*" in a private action. However, both these decisions rely upon an interpretation of each country's privacy statutes and therefore may be of limited assistance to Australian courts.

The risk of a data breach class action is not the only class action risk faced by publicly listed companies that are alleged to have failed to manage data security incidents. In addition to the Federal Court proceedings, Medibank has also been named in Supreme Court of Victoria proceedings in a shareholder class action. This is the first time an American based firm has filed such proceedings in the Supreme Court of Victoria. Quinn Emanuel Urquhart & Sullivan has brought the proceedings on behalf of persons who acquired an interest in Medibank shares during 1 July 2021 to 19 October 2022. The action alleges that the organisation breached its disclosure obligations by not disclosing to the market the alleged deficiencies in its cyber security systems. Not only will this action give a taste at what financial compensation could look like for these actions, it will also show businesses what the courts expect from an organisation in terms of disclosure and may discuss what are considered to be deficient cyber security systems.

Shareholder class actions arising from data security incidents have had a mixed history in the US and the overall record of successful claims is not great. While there are significant and important differences in the US and Australian class action regimes that make direct comparisons difficult, the mixed success of these actions in the US means that Australian directors and their insurers should remain cautiously optimistic that this will not result in an inevitable securities class action off the back of a large data breach.

[1] 'WP' and the Secretary to the Department of Home Affaris (Privacy) [2021] AICmr2 (11 January 2021).

These class actions should be on all business' radar, as they will set a blueprint for how similar breaches will be dealt with in the future and also the impact on appetite for class actions in this space in Australia. We have had discussions with colleagues at the Victorian Bar and there is uncertainty regarding whether class actions following data breaches will be the next big trend. Specifically, we spoke with Joel Harris of Counsel who stated that:

> "The issue of whether Privacy claims will become the next trend in class actions is still being determined. The claims have significant potential quantum if they succeed, which is undoubtedly an attraction to law firms and litigation funders. However, the claims themselves are complex. One only needs to look at the decision of several plaintiff law firms to make representative complaints to the OIAC rather than file proceedings in the Federal Court as an indication of the challenges faced by group members in this space.
>
> Looking into the future, the success of these types of claims will likely depend upon there reforms to the *Privacy Act*. Without a specific statutory cause of action, the success of Privacy class actions will be based on a variety of common law and statutory grounds that are not exactly fit for purpose. Further, for group members to realise their claims, there must be enough damages to make such claims economically viable for litigation funders to consider funding. The basis for damages remains an unsettled area of the law and will undoubtedly be the subject of intense debate as these cases progress."

In the meantime, we strongly encourage all organisations to be proactive in protecting themselves from potential actions. Some of the ways they can do this are by obtaining cyber insurance; investing in harm reduction technologies; factoring in potential financial exposure to your case plan; assessing data retention schemes and considering what is truly necessary; enhancing staff training; keeping up to date with the latest updates and news surrounding cyber breaches and government responses; and finally seek external advice where necessary.

TORT OF PRIVACY: THE ROAD SO FAR

Author: Partner Jehan Mata
Acknowledgment: Georgia Mineo and Georgie Aidonopoulos

A "right to privacy" within Australia has once again become a hot topic considering the recent health and telecommunication data breaches.

To date, no such tort has been formally codified in Australian law. However, considering the recent class actions lodged for cyber breaches and the Government's keenness in clamping down on cyber security and providing avenues for redress for victims, whether a tort of privacy should exist is again being considered.

Discussion regarding a tort of privacy is not a new phenomenon. It was first raised in 1979 by the Australian Law Reform Commission (**ALRC**). Since then, it has been discussed in various cases, however no one has affirmatively concluded whether such a right does or should exist:

- In 2001 in *Australian Broadcasting Corp v Lenah Game Meats Pty Ltd*, the High Court held that a court could find that there is a tort (or legal cause of action) of unjustified invasion of privacy if the facts allowed for it.
- In 2003 in *Grosse v Purvis* the Plaintiff received damages for unlawful stalking, which was found to involve an invasion of the privacy of the victim. While the award was made for the unlawful stalking, this case re-enlivened the need for a tort of privacy.

In two Victorian courts privacy issues arose, however due to the non-existence of an actual tort of privacy, parties were able to circumvent this obstacle by pleading their cases as an equitable breach of confidence:

- In 2004, *Giller v Procopets* the Victorian Supreme Court awarded damages for the publication of an intimate video. While the action regarded a breach of privacy, due to the non-existence of such a tort, the Plaintiff received damages for emotional distress by pleading the case as an equitable claim for breach of confidence.
- In 2007 in *Jane Doe v Australian Broadcasting Corporation* the Victorian County Court decided to follow suit and award a plaintiff damages for breach of confidence regarding conduct that amounted to a breach of an individual's personal privacy. The breach involved the ABC reporting on a recent sentence handed down against Jane Doe's estranged husband. In this report the ABC named Jane Doe, the suburb where her home was located, revealed the offences, and noted that she was the victim of the crime.

While none of the cases firmly established the right to privacy, they fuelled the debate.

After the most recent data breaches, the Attorney General in the *Privacy Act* reform report (as discussed in our previous article here) has again raised the possibility of introducing the tort of privacy. If this were to eventuate, we could see an increase in claims relating to cyber breaches as there would be a more accessible tort available to people.

Turning to the United Kingdom, the recent decision by the England and Wales High Court (King's Bench Division) in *Andrew Prismall v Google UK Limited and Deepmind Technologies Limited* concerned a claim for damages in the tort of misuse of private information on behalf of 1.6 million people. As the claim was rejected, this decision has only furthered the uncertainty regarding a potential tort of privacy and reinforces that other jurisdictions, similar to Australia, are grappling with the existence of this tort.

Takeaways

We are of the opinion that the cyber landscape has created the 'perfect storm' for the introduction of the tort of privacy. The existence of this tort will likely become a central question in most of the class actions following data breaches and there will likely be a resolution once and for all as to if this tort exists. We will continue to keep everyone updated.

Why Sparke Helmore?

Sparke Helmore's national cyber practice, led by Partners Jehan Mata, Mark Doepel and Dalvin Chien, offers comprehensive cyber expertise across both individual and company risk. Our extensive experience includes advising on privacy notifications and notifiable data breach issues, cyber policy drafting, acting as coverage and monitoring counsel, and managing recovery efforts, including asset tracing and subrogated claims.

Our clients benefit from our experience across the full spectrum of cyber breach matters. We manage claims efficiently and provide strategic advice on legal and regulatory exposures. We engage in risk mitigation with both insureds and insurers on "Lifecycle Issues" (through training, incident response triage, third-party contract reviews, and coordinating service provider support during times of breach). In addition to providing advice, we help educate our clients on emerging cyber trends and topics. Our team has presented extensively on cyber insurance and contributed significantly to thought leadership in this space.

As a full-service firm, Sparke Helmore leverages the expertise of our technology law and advisory specialists along with our panel of third-party vendors to support our clients on their end-to-end cyber lifecycle needs. We have a thorough knowledge of the cyber solutions, platforms and providers in the market and can provide insights into innovative cyber risk solutions. Given the potential for a cyber claim to have wide-reaching international regulatory exposure, we can assist with any offshore cyber-related matters, leveraging our affiliated members through our Global Insurance Law Connect network.

Contact details

To find out about the ways that we can help you, please contact a member of our team:

Jehan Mata
Partner
t: +61 3 9291 2374 | e: jehan.mata@sparke.com.au

Mark Doepel
Partner
t: +61 2 9260 2445 | e: mark.doepel@sparke.com.au

Dalvin Chien
Partner
t: +61 2 9260 2537 | e: dalvin.chien@sparke.com.au

sparke HELMORE LAWYERS

www.sparke.com.au

adelaide | brisbane | canberra | darwin | melbourne | newcastle | perth | sydney | upper hunter