HERBERT SMITH FREEHILLS

# LITIGATION RISKS ARISING FROM CYBER ATTACKS/DATA BREACH INCIDENTS

15 March 2022 | Insight
Legal Briefings – By **Christine Wong, Georgia Roy and Tim Porter**

Now, more than ever, litigation risk related to data breach incidents is something that should be kept front of mind for businesses.

## THE LANDSCAPE

Over the 2020-2021 financial year, the Australian Cyber Security Centre received over 67,500 cybercrime reports, nearly 13% more than the 2019-2020 financial year: see here. The cost of these cyber incidents is not insignificant and is closely tied to compliance levels; IBM's *Cost of a Data Breach Report 2021* noted that, globally, organisations with a high level of compliance failures (resulting in fines, penalties and lawsuits) experienced an average cost of a data breach of $5.65 million, compared to $3.35 million at organisations with low levels of compliance failures, a difference of $2.3 million or 51.1%.

Two significant areas of litigation exposure for businesses arising out of cyber incidents are:

- group proceedings, including representative complaints under the *Privacy Act 1988* (Cth) (**Privacy Act**) and class actions; and
- data breach claims between commercial parties.

While there are obstacles to potential litigants (discussed further below), the consequences can be significant: for example, in *LB and Comcare (Privacy)* [2017] AICmr 28, Comcare was ordered to pay $23,000, comprising the non-economic loss and costs for ***one*** complainant.

# CLASS ACTION RISK

Victims of cyber incidents face significant difficulties in commencing class action proceedings. Unlike other jurisdictions such as the UK, there is no recognition in Australia of tortious interference with privacy.

This absence of a general cause of action for privacy breaches has meant that plaintiffs must rely on existing common law and statutory causes of action.

The difficulties with relying on these actions to date have included:

- challenges in recovering any compensation for mere injury to feelings or humiliation (breach of confidence, contract and misleading and deceptive conduct); and
- hurdles in establishing duty of care and actual damage for negligence claims.

An example of this difficulty is the decision approving the settlement in *Evans v Health Administration Corporation* [2019] NSWSC 1781, the first data breach class action in Australia. Our previous update on the case is here. This class action arose out of a contractor for Ambulance NSW unlawfully accessing and selling sensitive information of over 100 Ambulance NSW staff.

In approving the settlement, Ward CJ noted need for the plaintiffs to "establish [a] new ground", due to the lack of a recognised tort and the uncertainty surrounding whether an equitable cause of action for breach of confidence will sound in damages for mental distress falling short of psychiatric illness.

This decision highlights how this judicial uncertainty can pose risks to all parties to data breach class actions, and will continue to do so until revisited by a superior court.

Even in jurisdictions where privacy actions are more established, there remains difficulties with quantifying claims and establishing damage. For example, in the UK, a unanimous bench of the Supreme Court in *Lloyd v Google* (see our previous update here) recently overturned a Court of Appeal decision to find that each of the 4 million individuals in the class would need to show that Google made some unlawful use of personal data and that they suffered some damage as a result.

# OAIC REPRESENTATIVE COMPLAINT PROCESS

An alternative and more commonly used pathway available to victims of data breach incidents to seek redress is to make a representative complaint for breach of the Privacy Act to the Office of the Australian Information Commissioner (**OAIC**).

Once a complaint is made, the Commissioner will decide whether to investigate the conduct and must refer the parties to conciliation if she considers the conciliation would have reasonable prospects of success.

After investigating the complaint, the Commissioner may make a determination, which extends to loss of damage for humiliation or injury to the complainants' feelings. In a recent determination, Commissioner Falk set out five categories of non-economic loss, with compensation ranging from $500-$4000 for "general anxiousness, trepidation, concern or embarrassment" to over $20,000 for "extreme loss or damage". This is in addition to economic loss, which is to be paid on a case by case basis, to restore a complainant to the same position they would have been if they had not sustained the wrong.

However, the Commissioner's determination is not binding or conclusive between the parties and the complainants or the Commissioner, must commence proceedings in the Federal Court or Federal Circuit and Family Court of Australia for an order to enforce a determination.

## DATA BREACH CLAIMS BETWEEN COMMERCIAL PARTIES

Contractual considerations are increasingly relevant for commercial parties who wish to apportion/minimise their liability for loss arising from a data-breach.

In particular, contractual legal considerations may arise when there is a data breach for a company which has outsourced data / IT services to a third party who has then failed to protect the information. The types of contractual claims that may arise include warranty / representation claims between a customer and a business (such as to have minimum security controls), or an indemnity claim with a third party.

Parties should consider in their contractual arrangements their notification obligations (including under their outsourcing agreements).

The loss or damage that may arise may be significant, such as interruption to the business if it has to shut down for a period, reputational / other damage to the business and breach of contract with customers. Whether or not damages can be recovered for these losses will depend on the terms of the contract.

Commercial parties may attempt to apportion liability for loss between parties for data breaches by seeking indemnities from third parties, limiting consequential damages and incorporating exclusion clauses into their commercial agreements.

Data breach indemnities are increasingly common. Often they are drafted regardless of the outsourced supplier's level of access to data. For a data breach indemnity to apply to a supplier who is not in the business of data security, it is likely an explicit mention of data breaches would be required to ensure it is not considered too broad / ambiguous.

Given the increasing frequency and magnitude of cyber-attacks and data breaches, there is growing demand for cyber security insurance and insurers are emerging as an important participant in cyber security litigation. Insurers also benefit from a right of subrogation. In other jurisdictions such as the UK and the US where the market for cyber insurance is more developed, insurance has played an important role in meeting defence costs and awards of damages and there have also been cases of insurers meeting ransom payments.

## BIG-TECH TAKING ACTION AGAINST MALWARE

Big-tech companies have started taking proactive action against entities using malware to surveillance and target their users. For example, a leading hardware and software company and a leading platform company have commenced separate claims against a technology firm alleged to have sent malware to their customers. Both companies have sued for an injunction, restraining the firm from using their platforms. Part of these claims were grounded on breach of contract, relying on restrictions in their product's terms and conditions. In November 2021, a US appeals court upheld one of the plaintiff's right to pursue a private action, rejecting the defendant's claim of immunity as a foreign sovereign.

Also in November 2021, a search engine company commenced a proceeding for computer fraud and abuse, trademark infringement, and other claims against the operators of a botnet, which targets Windows devices and defends itself using blockchain. In a blog post the company said:

"Botnets are a real threat to Internet users, and require the efforts of industry and law enforcement to deter them. As part of our ongoing work to protect people who use Google services via Windows and other IoT devices, our Threat Analysis Group took steps to detect and track Glupteba's malicious activity over time. Our research and understanding of this botnet's operations puts us in a unique position to disrupt it and safeguard Internet users around the world."[1]

While in December 2021, another big tech company filed a claim against actors who impersonated its subsidiaries in phishing attacks to deceive users to share their login credentials.

These claims are examples of a growing trend of large tech companies taking proactive action against cyber-crime, often in instances where the government is failing to take appropriate action.

## EYE ON THE HORIZON: POTENTIAL REFORM

Not only do businesses need to be mindful of litigation risk arising from law as it stands, but they should be keeping an eye to future reforms.

As discussed in our insight "Online Privacy Bill and Privacy Act Discussion Paper: Increased Enforcement Risk and Regulatory Change" (access here), potential reforms to privacy laws could lead to:

- a direct right of action; and
- a statutory tort of privacy.

The regulatory landscape is rapidly changing. We note the following has taken place since our earlier posts on Cyber-Ransoms and Regulatory Enforcement:

- The introduction of the *Ransomware Payments Bill 2021 (No.2)* into the Senate: this Bill seeks to establish a mandatory reporting requirement to the Australian Cyber Security Centre for Commonwealth, state or territory entities, corporations and partnerships to report ransomware payments paid in response to a ransomware attack. This Bill was introduced to the Senate on 12 August 2021. The *Ransomware Payments Bill 2021* that we previously commented on (here) is not proceeding.
- The commencement of the *Security Legislation Amendment (Critical Infrastructure) Act 2021*: this imposes a notification regime on owners of key infrastructure assets across many industries, where there has been a critical cyber security incident. The Act also gives the Government the power to make a range of directions in the case of a serious cyber security incident.

Remedying internal systems and processes to mitigate the risk of a cyber-attack or data breach incident is not something that can happen overnight. For instance, in 2021 it took an average of 212 days to identify a breach and an average of 75 days to contain a single data breach.[2] This litigation risk arising from increased future regulation is an area of risk that businesses should be proactively responding to.

---

1. See https://blog.google/technology/safety-security/new-action-combat-cyber-c...
2. See page 22 of the IBM *Cost of a Data Breach Report 2021*

## SHARE

Share to Facebook Share to Twitter Share to LinkedIn Email Print

Show Share Links

## RELATED TOPICS

Data and privacy

Class Actions

## FEATURED INSIGHTS

# FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

## RELATED ARTICLES

Tax in M&A in the UK and Europe – What you need to know

Crypto winter is here – what does it mean for insolvency practitioners?

Deal or no deal? Bring disputes lawyers in early to close that deal

# KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.


**CHRISTINE WONG**
PARTNER, SYDNEY

+61 2 9225 5475
Christine.Wong@hsf.com



**PETER JONES**
PARTNER, SYDNEY

+61 2 9225 5588
peter.jones@hsf.com



**JULIAN LINCOLN**
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com



**TANIA GRAY**
PARTNER, SYDNEY

+61 2 9322 4733
Tania.Gray@hsf.com



**KAMAN TSOI**
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com



**MARINE GIRAL**
SOLICITOR, MELBOURNE
+61 3 9288 1496
marine.giral@hsf.com