AUSTRALIAN SOCIETY FOR COMPUTERS & LAW

Cybersecurity lawsuits

John Swinson [1]

9 November 2020

> "For many, the phrase 'data breach' provokes dread and invokes disquiet. Suddenly, a person's once private information roams untrammelled, and a degree of uncertainty as to its location and possessor now unexpectedly exists.
>
> Of course, for as long as individuals and companies have maintained documentary records and stored private information, data has been poached. Then, as even now, cabinets were jimmied, trashcans were rifled through, and manila envelopes were haphazardly left open, furtively glimpsed.
>
> Once companies committed to storing files on local machines, enterprise databases, and cloud servers, however, breaching a company's every bit of data required no more than gaining access to restricted networks. Soon enough, data breaches became inescapable features of a digitized world.
>
> This case grew from one such breach, its extent and depth still murky. …"
>
> *Blahous v. Sarrell Regional Dental Center for Public Health, Inc*., No. 2:2019cv00798 (M.D. Ala. 2020)

We can often look to the United States to see what is likely to come next in the field of technology law.

The tort of privacy developed in the United States in the early 1900s, before the tort of negligence. The impact of a new technology, the camera, propelled the common law development of this tort. After 120 years, this tort may soon arrive in Australia with Attorney-General's Department considering this tort as part of its current Privacy Act review and Justice Keane recently suggesting "it would not be surprising were the High Court now to accept a tort of invasion of privacy".

The tort of negligence was recognised in New York in 1928 by Justice Cardozo, then on the NY Court of Appeals, when he said: "[t]he risk reasonably to be perceived defines the duty to be obeyed…". The tort of negligence arrived in Australia within the next decade.

In the industrial revolution, efficient production techniques were advancing faster than safety issues, resulting in large numbers of workers suffering similar injuries. These individuals often lacked the resources to sue individually. In the United States, class action litigation was perceived as a great way to provide access to justice. In 1853, the United States Supreme Court reiterated that, for the sake of both justice and convenience, courts should allow a representative to sue or be sued on behalf of all those who were similarly situated, with the resulting judgment binding all members of the group. In 1938, in an effort to provide more uniformity in the conduct of these cases, the Supreme Court adopted Rule 23 of the Federal Rule of Civil Procedure to govern class action litigation. After much discussion in Australia, the first Australian class action regime was enacted in 1992 (though representative procedures themselves – which had not been given a liberal interpretation – were not new.)

Current cybersecurity lawsuits in the United States bring together privacy and negligence claims in massive class actions. Looking at what is happening in the courts in the United States over the past few years may be predictive of what is soon to come to Australian courts.

---

[1] Partner, King & Wood Mallesons; Professor of Law, The University of Queensland

Where there is a security breach at an IT service or cloud computing provider, there are a range of possible lawsuits. Consider, for example, a bank B using cloud provider X to store data about the bank's customers C. A security breach occurs at X. B could sue X, but X is often protected by contractual limitation of liability provisions. So what we are seeing in the United States today is C suing B and/or X in a class action lawsuit.[2]

An example is the recent Blackbaud lawsuit. Blackbaud is a cloud computing provider that manages servers for non-profits, education institutions, healthcare organisations and the like (including for organisations in Australia). Blackbaud was subject to a ransomware attack during February to May 2020. Sensitive and personal data from students, patients, donors, and other individual users who were "customers" of Blackbaud's customers was accessed by the attackers. Blackbaud paid the ransom, and then was sued by an individual whose data was accessed. The class action lawsuit was not brought by Blackbaud's customers, but by an individual whose data was stored in the Blackbaud system by a customer of Blackbaud. The lawsuit identified many failures by Blackbaud to safeguard personal information including:

- Failure to provide timely notice of the unauthorised access (Blackbaud notified users in July and August 2020)
- Failure to identify all the information that was accessed
- Failure to properly monitor their IT systems (and thus, finding out about the attack too late)

The causes of action relied upon included: (i) negligence, (ii) the tort of privacy – intrusion upon seclusion, (iii) breach of express contract, (iv) breach of implied contract, and (v) violations of state data breach statutes. The Plaintiff claims damages for the cost of ongoing credit monitoring and potential loss from future identity theft.[3]

Even without the tort of privacy in Australia and no private right of action for breach of the Privacy Act, it is not hard to imagine similar class action lawsuits soon being filed in Australia.

There was a very small class action brought by Ambulance officers in NSW in November 2017 where a contractor was allowed access to their sensitive personal information. About 100 or so workers successfully settled for what may be considered to be a small amount. This was a traditional privacy breach not a cybersecurity breach.[4]

One solicitor's firm is reporting that it has started a class action against Facebook as a result of the Cambridge Analytica issues, but it does not appear to have been started as a class action.[5]

A review of recent US lawsuits involving cybersecurity incidents is illuminating:

- Where there is a cybersecurity breach impacting a number of people or businesses, a class action is common.
- There are many class actions resulting from ransomware incidents.[6]
- Where an IT service provider is the cause of cyberbreach, the limitation of liability provision in the contract is carefully reviewed, even though in many instances such a provision was not specifically drafted with a cybersecurity incident in mind. For example, is loss of data regarded as a loss of property?[7]

---

[2] For example, *Hoskinson-Short v. Capital One Finance Corp. and AWS, US Dist Ct,* Western District of Washington No 2:19-cv-1218, Filed 5 August 2019.
[3] *Allen v. Blackbaud Inc.*, US District Court for the District of South Carolina, No. 2:20-cv-2930-RMG, Filed 8 January 2021.
[4] See https://www.centenniallawyers.com.au/nsw-ambulance-class-action/
[5] See https://jws.com.au/en/services/expertise/class-actions
[6] An example is *Stoll et al. v. Musculoskeletal Institute, Chartered.*, Circuit Court of the Thirteenth Judicial Circuit in and for Hillsborough County, Florida Civil Division, No. 109606945, Filed 30 June 2020). Pleadings at: https://www.classaction.org/media/stoll-et-al-v-musculoskeletal-institute-chartered.pdf
[7] *Princeton Community Hospital Association Inc. v. Nuance Communications, Inc.*, United States District Court, Southern District of West Virginia, No 1:19-00265, Filed 7 April 2020

- Where the IT service provider has a complex corporate structure, as is often the case, it is important to identify the actual entity that was the cause of the harm.[8]
- Many claims are for potential, uncalculated losses, for possible future harm. No-one knows who has the data now and what harm may arise in the future due to the cybersecurity breach. A recent class action by consumers against the IT provider for a health centre are seeking damages for 7 years of credit monitoring.[9]
- However, in the absence of an actuality or a likelihood, the mere possibility that the plaintiffs' personal information may have been gathered and disseminated and that their credit may suffer if the hackers opt to sell or release this information to those able and willing to exploit it, is generally not sufficient to found a damages claim. Similarly, where the risk of identity theft is too speculative to constitute an injury in fact, the alleged injury of mitigation efforts to minimise that risk is likewise typically found to be non-cognisable.[10]
- Where there is a settlement, most class action lawsuits have a global cap on damages, but this is not always the case.[11]
- Sometimes during the incident, a cybersecurity expert is brought in to find and close the vulnerability, and if unsuccessful, is then sued.[12]
- Directors are being sued by shareholders for cyber-breaches.[13]
- Regulators are also bringing lawsuits against large companies who have been the subject of a cyberbreach, for example for unfair practices or misleading statements about security or privacy.[14] This trend has already arrived in Australia.
- It is rare to go after the hacker. They are hard to locate and are often in unfriendly jurisdiction. On a few occasions, pre-action discovery is sought against an ISP to try to find out the identity of the hacker.[15]

When such class actions arrive in Australia, it will be interesting to see how Australian judges determine the standard of care. As absolute security is impossible, and a hacking attack is more than likely, what are reasonable steps a business should take to prevent a security breach? In many United States cases, it would appear that the standard expected is high if not absolute. Or as Cardozo said in 1928: "The risk reasonably to be perceived defines the duty to be obeyed."

[8] *Surfside Non-Surgical Orthopedics P.A. v. Allscripts Healthcare Solutions, Inc.*, United States District Court, Northern District of Illinois, No. 18 C 566, Decision 4 June 2019
[9] See Larry Rulison, 'BST Sued by Community Care Customers over Cyber Attack', *Times Union* (Web Page, 10 June 2020) https://www.timesunion.com/business/article/BST-sued-by-Community-Care-customers-over-cyber-15330030.php
[10] *Blahous v. Sarrell Regional Dental Center for Public Health, Inc.*, US District Court, Middle District of Alabama Northern Division, No. 2:2019cv00798, Decision 16 July 2020, – Document 35.
[11] Marianne Kolbasuk, 'Data Breach Settlement Has an Unusual Provision', *Healthcare Info Security* (Web Page, 29 June 2020) https://www.healthcareinfosecurity.com/data-breach-settlement-has-unusual-provision-a-14523
[12] *Affinity Gaming v. Trustwave Holdings Inc.*., United States District Court, District of Nevada, No. 2:2015cv02464, Filed 30 September 2016.
[13] *Eugenio v. Directors of Laboratory Corporate of America Holdings*, Court of Chancery, Delaware, No. 2020-0305-PAF,Filed 28 April 2020. The pleadings are located at: https://www.dandodiary.com/wp-content/uploads/sites/893/2020/05/LabCorp-derivative-shareholder-suit.pdf
[14] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)
[15] *GWA, LLC v. Cox Communications, Inc. and John Doe*, 2010 WL 1957864 (D.Conn. May 17, 2010)