Cyber Update

SEPTEMBER 2019

wotton kearney

A founding member of LEGALIGN GLOBAL

Insurers face a double blow from cyber fines and claims in Australia

AT A GLANCE:

- With anticipated new laws and significant investigations underway, Australia appears set to further enhance its data protection regime with high penalties and serious potential for third party claims.
- Recent mega fines for data breaches handed down around the world may accelerate Australia's tougher regime, which is likely to affect businesses of all sizes.
- Increased enforcement, penalties and third party claims will create a rapid increase in exposure for insurers – and may put the question of whether cyber fines are insurable into the spotlight, as has happened in other jurisdictions around the world.

Huge mega-fines from UK and US regulators for data breaches have dominated recent cyber headlines, and it appears that the EU's General Data Protection Regulation (GDPR) fever is spreading worldwide.

With anticipated further enhancement to laws and significant representative actions and investigations underway, Australia appears to be edging its way into the fight to compete for the highest cyber penalties and the most deterrence. The response of companies like Facebook and Google to increased scrutiny by the OAIC and ACCC, combined with the growing public backlash about their market power, may influence the final position on Australia's laws and penalties.

Earlier this year, the Federal Government announced its plans to increase funding to the OAIC by $25 million over three years, as well as to substantially increase its powers – including a shift towards GDPR-esque turnover penalties. The draft legislation is expected to be considered by Parliament later this year. The increase in penalties is significant and designed to mirror the powers of the ACCC to issue penalties for breaches of the Australian Consumer Law.

The first year of the notifiable data breach scheme saw no penalties issued by the OAIC (as far as we are aware). However, while it's not yet waving the penalty stick, the OAIC appears to be shifting its stance from compliance to enforcement. The Commissioner has recently sought enforceable undertakings from companies, most notably the Commonwealth Bank and Wilson Asset Management – requiring each company to take specific steps to comply with the Privacy Act and destroy data not needed.

> **"The increase in penalties is significant and designed to mirror the powers of the ACCC to issue penalties for breaches of the ACL."**

This signals a shift towards stronger enforcement by the Commissioner. If the OAIC's budget and powers are boosted as anticipated, it will be more able to enforce tougher sanctioning, similar to what we have seen in the UK and Europe. This will put increasing pressure on companies to think about what data they collect and how it is used and protected.

RECENT MEGA-FINES

On 8 July 2019, the UK Information Commissioner (ICO) announced it intended to fine **British Airways** GBP183.39 million (about AUD329 million) following a data breach that affected around 500,000 customers. Sensitive information, including credit card data, was reportedly harvested through website cross-scripting.

Just a day later, the ICO announced it intended to issue another hefty fine – this time to **Marriott International Inc** for GBP99.2 million (about AUD180 million). Marriott acquired Starwood, a hotel chain, in 2016, whose systems are believed to have been compromised back in 2014. The breach wasn't discovered until 2018 – when it was notified to the ICO – and had affected a massive 339 million guest records globally over that time.

Not to be outdone, the US Federal Trade Commission (FTC) shortly afterwards issued a massive USD5 billion fine against **Facebook** for its data practices, including those arising from Cambridge Analytica.

£183.39m
FINE ISSUED

ARE WE FOCUSED ON THE WRONG REGULATOR?

The proposed legislative amendments will increase the OAIC's powers, which is a change that has been widely expected. Perhaps less anticipated are the recommendations made by the ACCC in its *Digital Platforms Inquiry Final Report*, which was published on 26 July 2019 – a report touted as a world first review into the market power of data titans such as Google and Facebook.

While largely competition and consumer focused, the recommendations adopt a number of key features of the GDPR that are absent in Australian privacy laws to date. Most notably they would create a direct statutory right of action for individuals, introduce a statutory tort of serious invasions of privacy and introduce strict liability fines for companies that breach the law. This has the potential to increase both regulator and claim activity at the same time.

Not unexpectedly, the Digital Industry Group Inc (DIGI), whose members include Facebook, Google and Twitter, has quickly hit back at the recommendations, accusing them of being "innovation-stifling red tape" and based on insufficient evidence. The data titans are not only concerned about the competition-focused merger recommendations, but also, they argue, the "detrimental effects on consumer choice" of stricter privacy laws.

As part of its preparations for the *Digital Platforms Inquiry Final Report*, the ACCC focused its investigations into the conduct of both Google and Facebook on suspected breaches of privacy and data collection laws. Although the specific conduct under investigation has not been disclosed, it has been suggested that it was quite broad – ranging from collecting location data without consent to placing consumers in a position where they are forced to consent to lengthy, complex privacy policies to access services.

ACCC Chair Rob Sims has confirmed these investigations are "very well advanced" and Australia is willing and able to "act alone" in pursuing these monolithic companies.

This is a provocative and clear statement to global regulators and a signal that Australia wants to be a serious player in the enforcement game. It is also a clear nod to companies that Australia is about to get tough.

In making this statement, the ACCC also clarified the protection of consumer data is not just the OAIC's problem as data protection crosses over into consumer protection more broadly. ACCC's focus on the individual's rights rather than the protection of information (the core basis of the Privacy Act) has long been anticipated.

While the ACCC's stance is good news for consumers, as there is more room for government resources to be allocated to make privacy a priority, it does put more pressure on companies to ensure data is handled appropriately. We have already seen this shift take place in the US, with the Federal Trade Commission (FTC) issuing a USD5 billion (about AUD7.1 billion) fine against Facebook for its data policies and practices.

However, it seems that even as regulators globally put their game face on, the financial incentive to make use of consumers' data, whether with consent or not, likely far exceeds the risk. While the Facebook FTC fine seems enormous, it really only represented about 9% of Facebook's annual revenue. That begs the question – do the penalties need to be higher or different? Perhaps a better deterrent would be public embarrassment, leading to reputational harm, given those companies rely on consumers for their existence.

TRICKLING DOWN TO SMES

The potential for the enactment of strict liability fines for companies as announced by the Government and recommended by the *Digital Platforms Inquiry Final Report* will likely have a significant impact on the state of play for cyber claims at all levels. This could put more pressure on the coverage for these fines under cyber policies, particularly given they don't require a finding on conduct.

The anticipated reforms are not targeted at any particular industry, kind of data collection or size of company – instead, they are expected to have a purposefully broad reach that will create risks for companies of all sizes and levels of operation.

ANTICIPATED AUSTRALIAN REFORMS

The new maximum penalties will be the higher of:

- **$10 million for serious or repeated breaches, or**
- **3 times the value of any benefit obtained through the breach and misuse of personal information, or**
- **10% of annual domestic turnover.**

New powers for OAIC for infringement notices for failure to cooperate with minor breaches up to:

- **$63,000 for entities, and**
- **$12,600 for individuals.**

The ACCC also recommended the introduction of:

- **a statutory tort of breach of privacy, and**
- **a direct statutory right of action for individuals.**

CASE STUDY:

OAIC REPRESENTATIVE ACTION AGAINST FACEBOOK

The OAIC launched its investigation into Facebook in April 2018 after the revelations arising from the Cambridge Analytica scandal, which affected more than 300,000 Australians. The investigation was launched off the back of a representative complaint to the OAIC seeking $10,000 on behalf of each individual.

The US experience suggests that, while the total value of class actions against companies might appear monolithic, the driver of the big numbers is the number of individuals affected, which can be into the millions. Once this number is whittled down to each individual, it paints a different picture.

An example that made this issue abundantly clear was the settlement of the Anthem data breach class action, arising from a breach of the health information of almost 79 million people. Although the settlement was worth USD115 million, it equated to about $50 for each individual or free credit monitoring services for up to four years, unless the individual was able to provide evidence of financial loss (such as out-of-pocket costs).

We expect to see the US experience reflected in Australia possibly as soon as the Facebook action. This will require individuals to prove their loss to receive any significant remedy, otherwise only minimal damages for hurt feelings are likely to be awarded. It is also worth noting that the OAIC's decisions are non-binding unless actively enforced by the Federal Court, so initially whether the individuals receive any remedy at all will be in Facebook's hands. A statutory right to claim, as recommended by the ACCC, would change this.

CLAIMS AND PENALTIES?

The Facebook representative action before the OAIC could already be a watershed moment for claims by individuals. However, a direct right of action as recommended in the *Digital Platforms Inquiry Final Report* in the near future wouldn't affect just the big end of town.

To date, the key risks facing companies have been only regulatory and the central focus has been on ensuring compliance rather than enforcement. However, having increased enforcement, penalties and third party claims could open the floodgates, hitting sections of cyber insurance policies that have been largely untouched to date in Australia.

While looming as a big double whammy for insurers increased enforcement and penalties may put the issue of insurability of fines and penalties back on the table. Are these mega penalties insurable? There is a growing sentiment that insurance cuts across the intended deterrence effect – which has been an issue that Australian courts have been considering in recent years in the consumer and WH&S realm.

A number of recent, well-publicised reports have suggested that privacy and data breach fines are only insurable in two out of 30 EU countries. Although there is no law preventing their insurability in Australia yet, it may be that the recent public, judicial and parliamentary backlash against the insurability of WH&S fines migrates to the proposed amendments to the Privacy Act when they come before Parliament later this year.

Whether privacy enforcement is insurable or not, the growing prevalence of attacks is a risk that all companies big and small must manage. Everyone from the data titans to the SMEs are equally at risk and need to be aware of their obligations and the looming enforcement agenda, or risk claims and penalties. No company wants to be the OAIC's test case to issue its first penalty, regardless of whether or not the penalty approaches the likes of the mega-fines storming through the US and Europe.

If you want to get on the front foot in managing these risks, contact us to see how we can help you prepare.

Need to know more?

For more information please contact our authors.

Kieran Doyle
Partner & Australian Cyber Leader
T: +61 2 8273 9828
E: kieran.doyle@wottonkearney.com.au

Jessica Chapman
Solicitor
T: +61 2 8273 9876
E: jessica.chapman@wottonkearney.com.au

Australian Offices

Sydney
Level 26, 85 Castlereagh Street
Sydney NSW 2000
T: + 61 2 8273 9900

Melbourne
Level 15, 600 Bourke Street
Melbourne VIC 3000
T: +61 3 9604 7900

Brisbane
Level 23, 111 Eagle Street
Brisbane QLD 4000
T: +61 7 3236 8700

Perth
L1/Suite 1, Brookfield Place Tower 2
123 St Georges Tce Perth WA 6000
T: +61 8 9222 6900

New Zealand Offices

Auckland
Level 18, Crombie Lockwood Tower
191 Queen Street, Auckland 1010
T: +64 9 377 1854

Wellington
Level 13, Harbour Tower
2 Hunter Street, Wellington 6011
T: +64 4 499 5589