wotton kearney

Client Update

Shaping the future of insurance law

An Australian first – privacy regulator commences action against Facebook

30 APRIL 2020

AT A GLANCE

- The Australian Information and Privacy Commissioner has commenced Federal Court action against Facebook for 'serious and/or repeated' breaches of the Privacy Act, in an action that is the first of its kind in the Australian legal landscape.
- The case marks the turning point where the Australian regulator signals more of an enforcement approach to applying privacy laws in Australia.
- The ultimate findings could have a long-lasting impact on companies operating in Australia, potentially creating a landscape for privacy litigation and class actions in Australia.
- Despite the action being a novel claim in Australia, we do not expect that a finding against Facebook will open the floodgates in the short-term to a significant increase in privacy claims in Australia.
- Insurers should be mindful that litigation funders will carefully assess the case to see whether it offers any guidance on privacy class actions for data breaches following cyber-attacks.

On 9 March 2020, the Office of the Australian Information Commissioner (OAIC) lodged Federal Court proceedings against Facebook for 'serious and/or repeated' violations of the Privacy Act 1988 (Cth) (the Act). The case has the potential to impact the privacy obligations of all companies operating in Australia and may give litigation funders guidance on privacy class actions for the misuse of data or data breaches following cyber-attacks.

Facebook officials are reported to have said that they had been "actively engaged with the OAIC over the past two years as part of their investigation… We've made major changes to our platforms, in consultation with international regulators, to restrict the information available to app developers, implement new governance protocols and build industry-leading controls to help people protect and manage their data".[1]

BACKGROUND TO THE CASE

The OAIC alleges that during the period of March 2014 to May 2015, Facebook disclosed the personal information of approximately 311,127 Australian Facebook users (Affected Users) to a third-party personality quiz application, This is Your Digital Life (the App), in breach of the Act.

The basis of the OAIC's case is that Facebook allegedly supplied the App with the personal data of the Facebook users who installed and used the App, as

[1] https://www.afr.com/technology/australian-watchdog-sues-facebook-for-repeated-privacy-breaches-20200309-p548c0

well as the Facebook friends of people who had used the App. The personal information collected by the App was then sold to Cambridge Analytica, the controversial political data firm that harvested and analysed personal information for political profiling and targeting. Cambridge Analytica was alleged to have influenced the 2016 US presidential race in favour of Donald Trump and the Leave campaign in the Brexit vote.[2]

PRIVACY ISSUES

The Act sets out 13 key Australian Privacy Principles that govern the way all entities covered by the Act are required to comply with the Act. In the case against Facebook, the OAIC alleges that Facebook breached:

1. Australian Privacy Principle 6 – Use or disclosure of personal information, and
2. Australian Privacy Principle 11 – Security of personal information.

Australian Privacy Principle 6

Australian Privacy Principle 6 outlines when an organisation may disclose personal information it collects. In particular, this principle provides that an organisation must not use or disclose personal information for any purpose other than what it was collected for, unless the individual has consented to its use or disclosure (or an exception applies, such as when it is required as part of a criminal investigation).

In the case against Facebook, the OAIC considers that the disclosure of the Affected Users' personal information to the App was "well outside users' expectations" because the Affected Users did not have any control over the way their individual data was used. Of particular concern will be the friends of Facebook users who were not provided with an opportunity to consider consent and had their information provided to a third party without their knowledge.

Australian Privacy Principle 11

Australian Privacy Principle 11 requires an entity to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as from unauthorised access, modification or disclosure.

It also obliges an entity to destroy or de-identify personal information in certain circumstances.

In the case against Facebook, the OAIC also alleges that Facebook failed to take reasonable steps to protect the personal information belonging to the Affected Users from unauthorised disclosure. To comply with Australian Privacy Principle, the OAIC considers that Facebook should have robust protective measures and procedures in place to ensure that the personal information of their users is safeguarded. This did not happen in the case of the App and the sale of personal information about the Affected Users to Cambridge Analytica.

PENALTIES SOUGHT

In Australia, the action brought by the OAIC against Facebook procedurally will go through the Court process and the OAIC is required to apply to the Federal Court under s13G of the Act for a civil penalty. As this is the OAIC's first claim of this type, the proceeding may be pivotal in deciphering what constitutes a 'serious and/or repeated' breach of the Act – a previously untested definition in Australian law.

Based on the applicable maximum penalties when the conduct occurred in 2014-15, if the Court considers the breach as a collective single breach, the Court may issue a fine of up to AUD1.7million – an amount not likely to concern a company the size of Facebook. However, if the Court decides to treat each of the Affected Users as a separate breach of the Act, Facebook could theoretically be fined into the many millions or possibly billions of dollars. While sums of this magnitude are unlikely, the approach taken by the Court in assessing and calculating penalties will be of great interest and could have long-lasting consequences for future breach of privacy claims in Australia.

FACEBOOK'S RESPONSE

While not much has been said by Facebook regarding the OAIC proceedings against them, the tech giant's comments on the Cambridge Analytica scandal in general may prove to be detrimental to its prospects of defending the claim. Facebook's approach has focused on apologising and brand rebuilding with its Australia's managing director apologising for failing to admit user expectations in relation to protection of data.[3]

[2] https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory;

[3] https://mumbrella.com.au/facebooks-will-easton-apologises-australian-marketers-brands-507672

With the filing of a defence by Facebook being the next procedural step in the case, it will be particularly interesting to see whether Facebook admits or denies that its conduct amounts to a breach of the Australian Privacy Principles, what it says about damages and how these issues impact the progress of the case.

In our view, it will be difficult for Facebook to deny it has breached the Australian Privacy Principles as the managing director's apology more than likely constitutes an admission that it handled user data in a way that was outside of the real of user's expectations and that it failed to take reasonable steps to protect personal information from misuse.

With the prospects of Facebook successfully defending the case appearing reasonably low, it may be that its focus is on plea bargaining with the OAIC. Although, that strategic approach may be challenging for Facebook if the OAIC is determined to make an example out of them, particularly as this is the first case of its kind.

Insight from W+K:

In 2018, the maximum civil penalty for serious and repeated breaches of the Privacy Act was increased from AUD1.7 million to AUD2.1 million.

In 2019, the Commonwealth Government announced that it was seeking to increase the OAIC's powers and increase penalties. However, it is likely that new legislation will be delayed due to COVID-19.

We expect that during the next 12-24 months, the maximum penalty for serious and repeated breaches of the Act will be significantly increased to align more similarly with the maximum penalties available under GDPR.

This will include the penalty being measured by reference to a percentage of revenue rather than a fixed amount to bring it in line with the Corporations Act and consumer law.

THE GLOBAL DATA PROTECTION FRAMEWORK

In recent years, there has been an international trend towards penalising companies that are considered to not collect and handle their customers' personal information in an acceptable manner. This attitude is reflected in the series of mega-fines handed down by UK and US regulators against big data companies for data breaches.

For example, in 2019 the US Federal Trade Commission issued a USD5 billion fine against Facebook for its data policies and practices, including those in place during the Cambridge Analytica scandal.[4] This was the largest penalty for a privacy or data security violation in global history. The Federal Trade Commission emphasised that privacy obligations are to be taken seriously and used Facebook as the scapegoat to deter other companies from engaging in sub-standard privacy practices.

A similar regulatory approach has been taken in Europe with the introduction of the European Union General Data Protection Regulation (GDPR) in May 2018. Under the GDPR, fines may be issued in proportion to the severity of the data protection contravention. Most notably, in 2019, the UK Information Commissioner (ICO) issued two landmark fines for personal breaches—GBP183.39 million against British Airways and GBP99.2 million against Marriott International Inc, respectively.

Under the Data Protection Act 2018 the ICO is empowered to issue fines to companies that fail to protect personal information of individuals.[5] In contrast, the OAIC has not yet been empowered by legislation to issue fines against companies for infringements of privacy and is required to take action through the Federal Court system.

More recently, as highlighted in our article in late 2019, the Australian Government has embraced the idea of severe sanctioning for breaches of privacy that more closely match the regimes in the UK, Europe and the US. This is demonstrated by the release of the *Government Response and Implementation Roadmap for the Digital Platforms Inquiry Report* and an announcement earlier in 2019, in which the Commonwealth Government proposed increasing the maximum penalty available

[4] https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[5] *Data Protection Act 2018* (UK) section 115(9); Articles 58(2)(i) and 83 of the *General Data Protection Regulation* (EU) 2016/679 (GDPR).

for 'serious and/or repeated' breaches of the Act to the greater of:

1. AUD10 million
2. three times the value of any benefit that was gained by the company through misusing the personal information, or
3. 10% of a company's annual domestic turnover.

The proposed amendments to the Act also contemplated providing the OAIC with the power to issue infringement notices of up to AUD63,000 to corporates that fail to cooperate with the OAIC to resolve minor breaches. This would allow the OAIC to levy out fines expeditiously without the need to engage the court process.

We expect that the strengthening of privacy protection laws in Australia and increases in the OAIC's enforcement powers will be delayed as a result of COVID-19, as the government's primary focus is on the health of its citizens and the economic fallout impacting a significant portion of the population.

IMPACT OF THE ACTION AGAINST FACEBOOK

Insight from W+K:

Since the introduction of the Notifiable Data Breach Scheme in Australia, the OAIC has generally taken a compliance rather than enforcement approach to data breaches.

The enforcement action taken against Facebook is a turning point where the OAIC takes a more aggressive approach to enforcement, similar to that seen in other jurisdictions, particularly the UK, Europe and the US.

Instigating proceedings against Facebook may be a bold statement that the OAIC intends to get tough by cracking down on privacy and data breaches in line with what has been seen in other jurisdictions.

A question it raises is the extent to which an action against Facebook impacts other companies operating in Australia, particularly in the SME market, and whether such an action would likely lead to a significant increase in privacy related proceedings or class actions.

SME market impact

While it is conceivable that the Federal Court will levy a significant penalty against Facebook, SMEs in the Australian market will unlikely rush to tidy up privacy compliance given the lack of relatability to a company like Facebook which is both big tech and a significant foreign entity.

Until enforcement action is taken against a company that Australian entities can relate to in terms of its operations and size, it is unlikely that action against big tech companies will cause a significant shift in the behaviour of Australian SMEs.

Are the floodgates open for privacy third party claims?

For many years now, and particularly since the introduction of the Notifiable Data Breach Scheme, there has been concern about a potential flood of data breach or breach of privacy class actions in Australia. This concern is always considered in the context of the class action 'friendly' landscape Australia offers. However, more than two years has passed since mandatory reporting was enacted and the privacy class action space in Australia has been reasonably quiet.

The OAIC's action against Facebook presents a new issue. The Court's guidance on what amounts to a 'serious and/or repeated' interference with privacy may give individuals whose privacy rights are breached some guidance on whether that interference is something that can be pursued for damages in court. Plaintiff firms and litigation funders will be watching this closely as they look for new avenues and types of claims to bring in the names of those affected by data breaches.

The court's decision may also create or assist in creating the long-awaited tort of privacy, which has been almost 20 years in the making. A statutory right to bring a claim has also been proposed by the ACCC and is under review by the government. In the meantime, however, we do not expect a significant increase in the number of privacy related court proceedings, particularly against companies in the SME market in Australia.

Facebook litigation-funded privacy class action

There is also the issue of what to do with the current class action filed with the OAIC via its representative complaint framework. We understand this action was largely put on ice while the OAIC completed its own investigation.

The filing of the OAIC's own proceedings may be a signal for how the OAIC will decide this filed complaint.

While it seems a foregone conclusion that the OAIC will decide in the class' favour, to obtain any significant award of compensation from the OAIC it is not enough to simply prove that a privacy breach occurred—loss and/or damage resulting from Facebook's unauthorised disclosure of personal information must be substantiated in each instance.[6] Otherwise, it is unlikely that the OAIC would meet the class' AUD10,000 per individual demand and would instead award minimal damages for hurt feelings and/or humiliation suffered by the complainants.[7]

KEY TAKEAWAYS FOR INSURERS

Cyber insurers should pay particular attention to how the Facebook case proceeds for a variety of reasons.

Firstly, the action represents a shift in the OAIC's approach from compliance to enforcement. This is a significant step made by the Australian regulator and brings it into alignment with the approach of other global privacy regulators that have aggressively pursued big fines against big tech companies. The Facebook case may represent the beginning of a period in which we can expect an increase in regulatory investigations, potentially penalties levied by the OAIC and third-party claims for data breaches.

Secondly, cyber policies generally cover investigations by privacy regulators and third party actions brought for breach of privacy. If the Facebook case leads to a precedent for what amounts to 'serious and/or repeated' interferences with privacy or the Court decides that penalties should be awarded for each breach for Affected Users, as opposed to for a single breach, it could have a significant and long-lasting impact on the scope of cover. A Court decision could also provide a roadmap for plaintiffs and class action firms seeking to commence actions against companies that are impacted by a cyber-attack.

Thirdly, a significant award of penalties against Facebook may also bring into the spotlight once again the question of the insurability of fines. As we discussed in our article in September 2019, it is conceivable that there may be backlash from various stakeholders if privacy fines are insurable on the basis that the insurance cuts across the intended deterrence effect.

We will provide updates on the Facebook case as it develops.

Wotton + Kearney can help you manage these risks and advise on appropriate data protection mechanisms. Contact us for more information.

[6] https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-4-determinations/#legislative-framework
[7] Ibid.

Need to know more?

For more information please contact us.

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

Eden Winokur
Special Counsel, Sydney
T: +61 2 8273 9942
E: eden.winokur@wottonkearney.com.au

Kaila Hart
Graduate, Sydney
T: +61 2 8273 9838
E: kaila.hart@wottonkearney.com.au