W+K UPDATE

Navigating the high cost of data breaches in the new cyber legal landscape

DEC22

Authors: Kieran Doyle (Partner), Magdalena Blanch-de Wilt (Special Counsel)

wotton kearney

A founding member of LEGALIGN GLOBAL

At a glance

- Recent major cyber incidents and associated data breaches in Australia, particularly those involving Optus and Medibank, have increased community expectations around data and the management of cyber security.
- The Australian Government has taken swift legislative action to increase the consequences of data breaches by amending the *Privacy Act* 1988 (Cth), and has indicated there will be an array of further reforms.
- For cyber and privacy insurers, this changing regime is likely to mean the average cost of claims under a cyber or cyber and privacy breach policy will get higher.

In the current maelstrom of breach, policy and legislative developments, we take a moment to answer some key questions – where are we now in this post-Optus breach era, what can we expect next, and what does this all mean for cyber insurance?

Higher penalties for serious data breaches

In response to the Optus data breach, and those that followed, the Australian Government has passed the *Privacy Legislation Amendment (Enforcement and Other Measures) Act* 2022 (the Act). The Act has significantly increased penalties for serious data breaches arising from cyber incidents. The maximum penalty under the Privacy Act was $2.22 million.

The maximum penalty is now the greater of:

- $50 million
- 3 x the value of the benefit obtained, or
- if the court can't determine that value, 30% of the adjusted turnover over the period of the breach.

The maximum penalty for individuals is now $2.5 million.

> The Australian Government has taken swift legislative action to increase the consequences of data breaches … For cyber and privacy insurers, this changing regime is likely to mean the average cost of claims under a cyber or cyber and privacy breach policy will get higher.

More powers for the OAIC

The augmentation of the OAIC's investigative and enforcement powers has made for fewer headlines but it is arguably an even more significant shift in Australia's privacy regime than the sharply increased penalties – especially given the boost to the OAIC's funding in the March and October budgets. The OAIC has an acknowledged mandate to take a "stronger enforcement posture", said by the Attorney General to be "in line with increased privacy risks and the community's growing concerns over the protection of their data".

The Commissioner can now:

- **Compel entities to give information, documents and answers** about actual or suspected eligible data breaches or their compliance with the notifiable data breach scheme. In practical terms, compliance with similar provisions under parallel legislative regimes is often a lengthy and costly exercise.
- In certain circumstances, **compel entities to undertake external reviews** (i.e. involving an external third party expert) to improve their practices to reduce the likelihood of repeat breaches. In practice, this will increase the costs associated with privacy compliance where the OAIC forms the view that an external review should take place.
- Assess the ability of an entity to comply with the notifiable data breach scheme under Part III of the Privacy Act (i.e. the OAIC can now **investigate an organisation's capacity to manage data breaches**).
- **Require entities to make individual notifications or public statements** about privacy breaches, investigations, determinations and assessments. These powers will amplify the reputational impacts of weaker privacy and data practices even if a penalty won't ultimately be applied.
- **Share information with other enforcement agencies**, which will better enable the coordination of enforcement activity among regulators.

Finally, the **extra-territorial application of the Act has been expanded** to respond to data collection in a digital age by ensuring that foreign organisations doing business in Australia are caught, even if they do not obtain personal information directly from a source in Australia. This is a significant change to the law, however it has less practical impact as it now reflects how broadly the previous "collected" or "held" criteria was interpreted by the OAIC in practice.

Further Privacy Act amendments

That's not the end of the story for privacy law reform. The Attorney General has indicated that his Department will finish its comprehensive review of the Privacy Act this year. That review is expected to result in further reform to the Privacy Act, with canvassed amendments including:

- eliminating existing exemptions from the application of the Act
- stronger consent requirements
- an expanded definition of personal information more fit for the digital era, and
- the introduction of the right of individual enforcement of privacy (e.g. a statutory tort of privacy).

A further Privacy Act Amendment Bill is expected next year to implement any additional reforms.

And data law reform (as well as SOCI reform) has also been mooted …

In the media release announcing the privacy amendments, the Attorney General The Hon Mark Dreyfus KC MP stated that, as well as the increased penalties under the Act, "[w]e need better laws to regulate how companies manage the huge amount of data they collect".

There is no indication yet of what those data reform laws will be, or how they will fit within the complexity of existing data laws, including the rollout of the Consumer Data Right across industry sectors (banking and energy, followed by telecommunications).

The government has also mooted that reform of the SOCI Act and regulation of ransomware payments will be considered.

So, what does this all mean?

The penalty horse before the better legal standard cart?

There is no doubt that material Privacy Act breaches should incur consequences, and there's well-established merit to a policy argument that those consequences should be sufficiently serious to incentivise privacy and data compliance.

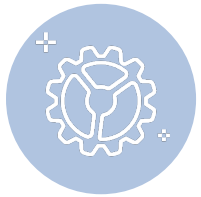
It's less clear that slogging Australian business with hefty penalties for 'serious and repeated' interference with privacy will improve overall privacy and data compliance in the current Australian regulatory context.

To incentivise the right behaviour, logically, we need to define what that is. While we now have the penalties in place, at this point in time, we don't have the 'better laws' the Attorney General has said are needed.

To take some examples:

- Under the Australian Privacy Principles, entities are required to destroy or de-identify records when they're no longer needed. However, there is little real legislative guidance on how long data can be retained if it's required to be collected (to take the example of identity information, can a business keep customer identity data just until the task of identifying the customer is complete, or for future verification as well?).

- Entities are also required to take reasonable steps to protect personal information. However, there's no mandatory cyber security standard (and existing guidance is principles-based). This leaves significant uncertainty about whether existing protections are enough.



The leading cause of data breaches in Australia is ransomware attacks. However, there is no centrally mandated or precisely prescriptive cyber security standard in Australia. Neither are there any 'safe harbour' provisions to protect diligent organisations. For these reasons, the majority of Australian organisations suffering a significant cyber-related data breach will be vulnerable to an active regulator forming the view that a 'serious interference with privacy' has occurred. There will always be an argument that there was something more an organisation could have done to prevent or reduce the impact of a data breach.

While the lack of clear standards does leave organisations vulnerable to a wide scope for penalties, it would also be misleading to suggest that a penalty would necessarily apply to future cyber incidents that were the same as those grabbing headlines in the past few months.

This is because:

- the increased penalties apply to "serious or repeated" interferences with privacy, so not all cyber incidents or data breaches are caught – most will not be as their scale, the type of information affected, and the nature of the conduct will not meet the test

- the threshold of what constitutes "serious" interference with privacy is not defined in the Privacy Act and there is limited guidance on how this applies to cyber-related data breaches

- to be caught, a cyber-related data breach will effectively need to involve some type of wrongdoing by the breaching organisation regarding personal information – in the majority of cyber incidents, there will be arguments each way about whether or not adequate protections were in place, and

- ultimately, we expect that in the coming months and years the question of how serious a data breach has to be to constitute a "serious or repeated interference with privacy" is likely to be the subject of robust argument between organisations and the OAIC, and ultimately, litigation.

Regulatory investigation costs will increase

In the longer-term, the increased powers of the OAIC and higher penalties can be expected to correspond with an aggregate increased cost of privacy investigations and data breaches. Experience with other Australian regulators suggests that the OAIC's increased investigative powers (e.g. the power to request documents) may result in prolonged and complex regulatory investigations and information requests, ahead of managing the notifiable data breach process or defending an allegation of serious or repeated interference with privacy. Taken together, we can expect that the average cost of settling a breach response claim from an insured under a cyber or cyber and privacy breach policy will get higher.

Pressure on cyber policy economics

Cyber insurance policies in Australia have traditionally covered the cost of fines and penalties for breaches of privacy. Standard cyber policies apply limits to these penalties, which previously would have covered a typical or even maximum fine for a serious or repeated interference with privacy. Now that the increased penalties apply, this may not be the case. This may place pressure on cyber policy economics and create demand from insureds for changes to sub-limits.

With business interruption and incident response costs increasing and already resulting in large claims, we expect that in the near-term, insureds will need to carry larger limits overall. That will come at a cost and is likely to put further upward pressure on premiums.

In the longer-term, we will need to see whether the market's response to materially increased regulatory penalties will be an exclusion, increased retentions for these types of penalties, increased premiums to offset the likely higher payouts, or breaking up the cyber policy into first and third party covers.

Good cyber defences will be critical

The Privacy Act amendments are substantive. They're designed, in the government's view, to deter data breaches and to take them out of the realm of being a routine 'cost of doing business'. The OAIC, with its expanded powers, will also become the equal of traditionally more litigious Australian regulators.

Organisations experiencing serious data breaches arising from cyber incidents in Australia now have to run a tricky gauntlet between unhappy customers and shareholders (who may choose to take their business elsewhere), tougher regulatory investigations, significantly steeper penalties, and a cyber policy that may not meet total losses.

Regulatory sanctions are not, however, a foregone conclusion. Good cyber defences that adhere to reputable standards and robust privacy and data practices and policies, together with well-established processes for managing cyber and data incidents, will give an organisation sound protection from cyber-related data breaches and the best chance of containing them when they occur.

Australian offices

Adelaide
Hub Adelaide, 89 Pirie Street
Adelaide, SA 5000
T: +61 8 8473 8000

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

Canberra
Suite 4.01, 17 Moore Street
Canberra, ACT 2601
T: +61 2 5114 2300

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

Melbourne – Health
Level 36, Central Tower
360 Elizabeth Street, Melbourne, VIC 3000
T: +61 3 9604 7900

Perth
Level 49, 108 St Georges Terrace
Perth, WA 6000
T: +61 8 9222 6900

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

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

www.wottonkearney.com.au

wotton kearney

Need to know more?

For more information, contact our authors, **Cyber, Privacy + Data Security** specialists.

Kieran Doyle
Partner, Head of Cyber + Technology, Sydney
T: +61 2 8273 9828
kieran.doyle
@wottonkearney.com.au

Magdalena Blanch-de Wilt
Special Counsel, Melbourne
T: +61 3 9116 7843
magdalena.blanch-dewilt
@wottonkearney.com.au

Get in touch with our specialists

To learn more about our expertise, click here.