
KING&WOOD
MALLESONS
金杜律师事务所
The Power of Together
2018-19
Privacy Law
Update

Contents

Michael Swinson
Partner
T +61 3 9643 4266
M +61 488 040 000
michael.swinson@au.kwm.com

Cheng Lim
Partner
T +61 3 9643 4193
M +61 419 357 172
cheng.lim@au.kwm.com

Patrick Gunning
Partner
T +61 2 9296 2170
M +61 418 297 018
patrick.gunning@au.kwm.com

Annabel Griffin
Partner
T +61 2 6217 6075
M +61 408 847 519
annabel.griffin@au.kwm.com

With thanks to Thomas Dysart, Kendra Fouracre, Stephanie Johnson, and Alana Humphris for their contributions to this publication and to Cal Samson for his significant editorial role.

Welcome

If 2018 sowed the seeds for the next wave of privacy law reform and enforcement activity, then so far 2019 has been the season of growth with more reforms proposed, more assertive regulators, more (in some cases very large) penalties being imposed, and more media attention.

This year, our annual wrap-up of privacy law developments touches on important regulatory reviews, controversial legislative changes, recent enforcement actions, and judicial consideration of some complex Australian privacy law issues. However, these developments should not be viewed in isolation. The increasingly global nature of the world economy and the extra-territorial reach of many national privacy regimes means that internationally-minded organisations now face the challenge of trying to reconcile and comply with many different and, in some cases, conflicting privacy rules. To address this, there is a growing push towards harmonising global privacy laws and growing collaboration between national privacy regulators. Notably, Australia's Angelene Falk was recently elected to the executive committee of the International Conference of Data Protection and Privacy Commissioners (the premier global forum for data protection authorities) and we expect that her approach to enforcing the law in Australia will be closely informed by the attitudes of her counterparts in other leading privacy jurisdictions.

Of course, a constant reference point in any discussion of global privacy standards has been the European General Data Protection Regulation (**GDPR**), which came into effect in May last year. While it is still settling in, and nuances are apparent in how it has been implemented and interpreted across relevant European jurisdictions, the GDPR is at the heart of any debate about harmonisation of international privacy laws and we have seen a number of international organisations use the GDPR as a de facto standard across their global operations. There is no doubt that comparisons to the GDPR will be drawn in relation to any future revision of privacy laws in Australia.

While there have been many significant developments in this area of law in recent times, there are still more to come. It will be especially fascinating to see how the government responds to the final report from the ACCC's Digital Platform Inquiry, which as we explain in our summary below contains a number of sweeping recommendations for privacy reform in Australia. In any event, we hope that this publication provides a useful overview of recent developments and gives you some insight as to what to expect for the future.

If you would like to understand how any of the issues discussed below may affect your organisation, please get in touch with one of KWM's privacy experts.

Wide ranging recommendations for reform from the ACCC

On 26 July 2019, the Federal Government released the Australian Competition and Consumer Commission's (**ACCC**) much-anticipated final report on the Digital Platforms Inquiry (the product of over 18 months of effort). Originally framed as an inquiry into the impact of digital platforms (including search engines, social media, and content aggregators) on the state of competition in the media and advertising services markets, the recommendations in the final report are much wider in scope and will directly affect many other sectors of the economy. Most relevantly for this publication, while reserving some specific recommendations for digital platform operators, the final report recommends broad-ranging changes to Australian privacy laws.

In justifying the broad reach of its recommendations, the ACCC asserts that the Australian privacy regime must "require a clear and consistent standard of data protection across different industries in the data-driven digital economy to consistently protect consumers and to achieve the economy-wide potential benefits of data." Certainly, if the ACCC's recommendations on privacy reform are implemented they will have a significant economy-wide impact. This will no doubt attract attention from a wide range of consumer-facing businesses that are heavy users of consumer data but may only have been keeping one eye on the Digital Platforms Inquiry, on the assumption that they would not be directly affected by its outcome.

The Government has not yet committed to implementing all of the ACCC's recommendations, though it has accepted that some degree of reform is required. The Government's formal response will be informed by a 12 week public consultation process, after which the Government will finalise its response by the end of 2019. Given the reach of the ACCC's recommendations, we expect a far broader level of engagement in this consultation process compared to the Digital Platforms Inquiry itself.

Key operational impacts

Key aspects of the ACCC's privacy-related recommendations that may have a material operational impact on any business that relies upon the collection and use of consumer data include:

- **Mandatory consent requirements** – the ACCC recommends that consent be required whenever a consumer's personal information is collected, used or disclosed except where necessary for the performance of a contract to which the consumer is a party (or as otherwise required under law or for an overriding public interest). Valid consents would have to be given by some clear affirmative act, with any data collection settings being defaulted to "off". If implemented, this recommendation will likely result in many organisations having to significantly increase their reliance upon consumer consent. In particular, consents may be required for any processing of personal information that goes beyond what is required to provide an organisation's core consumer-facing service (even extending, perhaps, to ancillary processing such as for security and fraud detection). While to some degree the ACCC's recommendations in this area align to the current "high water mark" of the GDPR, the ACCC has deliberately chosen to exclude the GDPR provision that permits processing of data for "legitimate interests" on the basis that this concept is too uncertain. This could lead to a stricter and more rigid regime in Australia, with the focus on consent potentially resulting in a more cumbersome, confusing and unsatisfactory user experience for consumers.
- **Enhanced notice requirements** – the ACCC recommends that existing obligations for organisations to notify consumers about the collection, use and disclosure of their personal information be strengthened. Notices should be designed to be concise, transparent, intelligible and easily accessible using clear and plain language. The ACCC is also critical of privacy policies that are long, complex, difficult to navigate, and potentially ambiguous or unclear in their use of language. The ACCC recommends that privacy policies be redesigned to adopt a multi-layered

format, with essential information on key points covered in a concise initial layer, with consumers then able to access more detail in subsequent layers (potentially right down to very specific details, such as the name and contact information for every third party with whom personal information may be shared). This may require many businesses to revisit their current notification practices, and to update their privacy policies to align with the ACCC's design recommendations. It may also present some significant challenges, as there is an inherent tension between the objectives of (i) developing clear, concise and easily intelligible documents and (ii) providing comprehensive information about often complex data management practices. The ACCC suggests that some of these challenges may be overcome using standardised language or icons with pre-defined meanings. However, the extent to which it would be practical to do this across a wide range of different businesses that all may have unique data management practices, remains to be seen.

Other wide-ranging recommendations

Other important recommendations by the ACCC in this area include:

- expanding the scope of "personal information" to specifically capture technical data (e.g. IP addresses, device identifiers and location data) that may be used to identify an individual;
- introducing a new right for consumers to be able to require the deletion of their personal information (equivalent to the "right to be forgotten" under the GDPR);

- introducing a new direct right for individual consumers to bring actions for breaches of the Privacy Act (where currently they must generally rely upon the Commissioner to take action on their behalf);
- increasing the civil penalties available under the Privacy Act to align with those available for breaches of the Australian Consumer Law (consistent with changes that the Federal Government signalled back in March 2019 that it would be proposing, namely a maximum penalty of $10 million or three times the value of any benefit obtained through the misuse of information or 10 per cent of a company's annual domestic turnover – whichever is the greater); and
- introducing a new statutory tort for serious invasions of privacy (aligning with recommendations made by the ALRC and others over a series of previous privacy-related reviews in recent years).

The ACCC's final report also includes some more targeted recommendations that apply only for digital platform operators – including that a new enforceable privacy code of practice be developed for digital platforms – and that will not directly impact on other businesses.

Besides the specific recommendations mentioned above, the ACCC's final report also recommends a broader review of Australian privacy law be undertaken to consider whether other changes may be necessary or appropriate to further protect consumer interests. While the report does not provide much detail on what further reforms may be required, it does recommend that any broader review should consider current Privacy Act exemptions, regulation of inferred information, and standards for de-identification of personal information.

Finally, the ACCC also recommends considering updating the Privacy Act to more closely align with the GDPR (as things stand Australia is not recognised by the European Commission as a jurisdiction that provides an "adequate level" of data protection, in large part because of exemptions that currently apply under the Privacy Act that do not apply under the GDPR) so as to facilitate freer flow of information between Europe and Australia.

Key takeaways

- If implemented, the ACCC's recommendations would require substantial changes to an area of law that was reviewed in-depth only a short time ago (with the last major revision of the Privacy Act coming into effect in 2014).
- The pace of technological change, and recent significant developments in this area of law overseas (most notably through the introduction of the GDPR in Europe), means that global businesses are facing mounting challenges in having to comply with similar but different local regulatory regimes. As such, any push to seek a degree of harmony on key points will likely attract some support from these businesses.

GDPR fines are big … and getting bigger

Now that the GDPR has been in effect for more than 12 months, national data protection authorities across Europe are beginning to flex their new regulatory muscles. There have been a number of high-profile enforcement actions this year that have culminated in major fines for some large companies who have been found to be in breach.

By way of setting the scene, one of the headline features of the GDPR is the very significant fines that it allows data protection authorities to issue. Maximum fines are capped at the greater of €20 million or 4% of the offending entity's worldwide annual turnover in the preceding financial year. Compared to the previous maximum fines that could be issued – for example, before the GDPR came into effect the maximum fine that the Information Commissioner's Office (**ICO**) in the UK could issue was just £500,000! – this represents a massive increase. The size of fines that are now being issued has given even the most well-resourced users of personal information cause to sit up and take notice.

CNIL v Google

The first significant fine under the GDPR was issued in January 2019, when the French data protection authority, the National Commission on Informatics and Liberty (**CNIL**), handed down a fine of €50 million to Google.

The action taken by the CNIL was in response to complaints by a number of privacy advocacy groups including noyb (or 'none of your business') and French NGO La Quadrature du Net. After completing its investigation, the CNIL found evidence of two types of breach by Google:

- violations of obligations of transparency and information; and
- violations of the obligation to have a legal basis for advertisement personalisation processing.

In relation to the first category of violations, the CNIL concluded that information regarding Google's data processing purposes, data storage periods and what type of personal information was used for ad personalisation was not easily available to users through Google's privacy policies. In making this finding, the CNIL noted that relevant information was only available after passing through several steps, sometimes taking as many as five or six actions / clicks from the user. The CNIL also considered that the information, once found, was not clearly set out in a comprehensive way and that users would struggle to understand the complexity of the processing operations undertaken by Google. These conclusions are interesting in light of the recommendations made by the ACCC in the Digital Platforms Inquiry about the need to improve and simplify privacy notifications, including through the use of multi-layered policies that lead off with the information most likely to be important to users.

In relation to the second category of violations, the CNIL concluded that Google's methods of obtaining user consent for the processing of data for purposes of ad personalisation were not adequate. According to the CNIL, the consents that Google purported to collect were not sufficiently informed because users were not properly notified about the extent of Google's processing activities. Furthermore, in the CNIL's view the purported consents were not "specific" nor "unambiguous" because the user had to take steps to modify their personal settings in order not to have consented. In other words, ad personalisation permissions were pre-selected by default. Consent under the GDPR requires the user to take unambiguous affirmative action (for example, by ticking a non-ticked box) to consent. Acceptance of a bundle of broad-ranging policies when signing up to an account, which is what the CNIL found Google had in place at the time, will not be a reliable foundation for effective specific consent under the GDPR.

The €50 million fine that the CNIL handed down to Google was at the time the largest and most significant penalty issued under the GDPR (albeit that it may appear less significant when compared to Google's annual revenue!). While Google argued that the fine was disproportionate and that it should first have received a formal notice that would have enabled it to correct any potential compliance failures, the CNIL disagreed. In particular, the CNIL was influenced by the fact that the processing activities concerned a large number of data subjects and went to key requirements of the GDPR relating to transparency and the basis for processing personal data. Google has announced that it will appeal the CNIL's decision and the fine to the French Supreme Administrative Court, and it will be interesting to see whether or not the CNIL's approach will be affirmed through this process.

ICO v British Airways and Marriott International

Not wanting to be left behind, the ICO in the UK soon caught up with its French counterpart by announcing its intention to issue two massive fines on consecutive days in July 2019.

First up, on 8 July 2019, the ICO announced that it intends to fine British Airways (**BA**) £183.39 million for various breaches of the GDPR. The proposed fine relates to an incident that occurred in 2018 which saw customers booking flights via the BA website or mobile app diverted to a fraudulent third-party website where sensitive personal details (including usernames, passwords and credit-card details) were siphoned off by fraudsters. Approximately 500,000 customers were affected. Following an extensive investigation, the ICO found that the personal information had been compromised by BA's "poor security arrangements". The ICO has now invited BA to make representations as to the proposed findings and the intended fine. If the ICO proceeds with the fine, it will be by some margin the largest fine ever issued by the ICO, coming in at 1.5% of BA's total revenue for the year (though this is still significantly less than the maximum penalty of 4%).

The very next day, on 9 July 2019, the ICO issued a statement outlining its intention to fine Marriott International (**Marriott**) £99.20 million for an incident that resulted in the exposure of

personal data contained in approximately 339 million guest records. The exposure is believed to have stemmed from a vulnerability introduced in the systems used by the Starwood hotels group, which was acquired by Marriott in 2016. These issues were not discovered until 2018. The ICO's investigation concluded that Marriott had "failed to undertake sufficient due diligence" when acquiring Starwood and that it should have done more to secure its systems. Like BA, Marriott now has the opportunity to respond to the findings and proposed sanction before the ICO finalises its decision.

Each of these cases is significant not only for the size of the proposed fines but also for the circumstances from which they arose. We expect that there will many companies that are less than confident that their information security arrangements are adequate to defeat all would-be hackers, or that their corporate due diligence processes are always exacting and thorough. The fines proposed in these two instances highlight the urgent need for all companies that deal with consumer data to lift their game in these areas or else risk exposure to very significant financial penalties.

Future regulatory actions

One of the key players in the early days of enforcing the GDPR has been Max Schrems, the high profile privacy advocate and founder of noyb. Well-known as a serial litigant with some big wins under his belt, Mr Schrems is involved in a number of ongoing privacy-related actions, with regular updates on these being posted on noyb's website. Perhaps of greatest potential significance is his action in the European Court of Justice (**ECJ**) concerning the validity of the standard contractual clauses and the Privacy Shield scheme that together currently provide a framework for exchanges of personal data between the EU and the US. Essentially Mr Schrems argues that the protection from US government surveillance offered to EU data subjects is inadequate. His case was heard by the ECJ in July 2019, with a decision expected by the end of the year.

The ECJ's response to Mr Schrem's claims, may have wide ranging implications for entities that do business across the Atlantic Ocean and could cause significant disruption to the international flow of consumer data. However, the ECJ action is not Mr Schrems' only focus. As noted above, he is a founder of noyb, which as well as being one of the initial instigators of the complaint about Google to the CNIL has also made similar complaints in relation to the consent and data handling practices of a wide range of leading technology companies and services, including Apple Music, Amazon Prime, Netflix, YouTube, Soundcloud, Spotify, DAZN and Filmmit. Mr Schrems' dogged approach seems set to provide a stern test for new privacy laws, and compliance strategies, for some time to come.

The Assistance and Access Act? It's just one of the laws of Australia

On 6 December 2018, the final day of Parliament for the year, and in the midst of political manoeuvring and substantial industry criticism, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**Assistance and Access Act**) was passed by both Houses of Australian Parliament. It came into effect a few days later on 9 December 2018.

As memorably put by former Prime Minister Malcolm Turnbull in relation to the initial plans for the law: "The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia." Now the Assistance and Access Act is part of that select club, it remains to be seen exactly what impact it will have. As already mentioned, the Act has from its initial inception been highly controversial, and the controversy has not subsided over the time that it has been in force. While the impact of the Act can be hard to assess as an outsider, due to the strict secrecy provisions that largely prevent public discussion of any specific actions taken under the Act, it is currently under review by the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) with a report scheduled to be issued by April 2020.

What does the Assistance and Access Act do?

Also known colloquially as the "Encryption Act", the Assistance and Access Act is intended to improve the ability of law enforcement and national security agencies to address the potential for the use of encrypted messaging services to frustrate their work in investigating serious crimes, terrorist activities and other national security threats.

The Act is not a standalone piece of legislation, but rather inserts new powers and provisions into a number of other pieces of legislation. Some of the key changes implemented by the Act include:

- the ability for law enforcement and security organisations to request or require designated communications services providers to provide certain types of assistance, either by issuing voluntary "Technical Assistance Requests" or mandatory "Technical Assistance Notices" or "Technical Capability Notices". The scope of entities that may be treated as designated communications services providers is very broad. As well as traditional telecommunications carriers, it may cover entities that manufacture or supply network equipment or end user handsets, entities that provide electronic services (which the Explanatory Memorandum indicates may be so broad as to cover "websites" and "messaging applications"), and entities that provide services or software for use in connection with a carriage service or electronic service. Effectively, this means that the whole communications supply chain, including "over the top" online operators may be caught. The assistance that may be requested or required of these entities under the Act is also similarly broad, and may amongst other things include removing electronic protections, providing technical information, installing software nominated by an agency and notifying agencies of technological developments;
- the introduction of covert warrants under the *Surveillance Devices Act 2004* (Cth), which allow relevant agencies to search electronic devices and access content on those devices while concealing their actions. This can, for example, include removing a computer or other device from the owner's premises and then returning it after adding, deleting, copying or altering data stored on it without notifying the device owner; and
- the extension of warrants issued under the *Crimes Act 1914* (Cth) for the purpose of collecting information from electronic devices remotely and to permit access to "account-based data" such as data associated with an email or social media account.

You can read more about the Assistance and Access Act at our previous alerts on this topic.

Why is the Assistance and Access Act so controversial?

There are a host of reasons why the Assistance and Access Act has proved to be so controversial. In the words of the PJCIS, the Act "has attracted significant domestic and international interest" on the basis that it "introduced significant new powers on technical matters that have global implications". Certainly much of the public commentary from industry in the lead up to its passage was very negative, particularly with reference to its impact on user privacy, with newspaper editorials comparing the new measures to government technology interventions in Russia and China and sections of the technology sector labelling it an "appalling piece of legislation".

Amongst the many concerns that have been expressed are: the relative lack of judicial oversight over the new powers established under the Act and the sweeping nature of these new powers. Many in the communications industry have voiced concerns that in exercising these powers government may have an adverse impact on the performance and security of the underlying communications services concerned, which may reverberate across the globe given the interconnected nature of global communications networks. Chief amongst these concerns is that the powers under the Act could be used to establish a "backdoor" into encrypted communications services, which may compromise the overall security of those services to the detriment of all users. Amendments were introduced to the Act in an attempt to allay these concerns – including by specifying that a communications provider may not be obliged to build in a systemic weakness or systemic vulnerability that will render existing methods of authentication or encryption ineffective or be prevented from taking steps to rectify such a systemic weakness or vulnerability – but nevertheless the concerns persist.

A number of submissions to the ongoing PJCIS review of the Assistance and Access

Act continue to be critical of the legislation. Notably, a submission by the Law Council of Australia raises concerns about potential inconsistencies with overseas laws, including the CLOUD Act in the US. In particular, the Law Council argues that the US may not enter into an executive agreement with Australia under the CLOUD Act (in order to facilitate law enforcement access to information across borders) unless the US Attorney General determines that the domestic law of Australia "affords robust substantive and procedural protections for privacy and liberties in light of the data collection and activities of the foreign government that will be subject to the agreement". The Law Council is of the view that the lack of judicial oversight under the Assistance and Access Act, along with other factors, means that the US Attorney General could not make such a determination.

Ongoing international debates

The extent and use of law enforcement investigatory powers continues to be an issue of hot public debate in Australia, with particular controversy over the extent to which law enforcement agencies have been exercising their powers to investigate journalists in a way that could threaten the freedom of the press. The PJCIS is conducting a separate review on these issues, with a report on that review due in October 2019. In the meantime, meetings from the intelligence agencies from the "Five Eyes" nations – the UK, the US, Australia, Canada and New Zealand – have reportedly sparked calls for agencies to be allowed special access to encrypted messaging applications. The fierceness of these ongoing debates clearly demonstrates that in a democratic society, striking the right balance between respecting individual privacy and empowering law enforcement and national security agencies to effectively deal with the threat of sophisticated criminal and terrorist activity is a constant challenge. We expect this debate to continue attracting attention in Australia, as the PJCIS hands down its further findings on the Assistance and Access Act and other related matters over the coming year.

Mandatory data breach reporting turns one

The mandatory data breach notification regime introduced in Australia in February 2018 has now been in effect for 18 months. To mark the first year of its operation, the Information Commissioner released a special report with some interesting statistics and observations about the cause and effect of data breach issues in Australia. According to this report, during the regime's first year:

- **There were 964 reported breaches (up 712% from the last year of the voluntary reporting regime).**

  This is obviously a very significant increase! What hasn't increased though are the resources available to the Information Commissioner to deal with all of these breach notices. At Senate estimates in 2018, the Commissioner indicated that she had only 5 people working part time on overseeing the mandatory data breach reporting regime. There have been consistent calls for the Commissioner to be provided with more funding in order to add the resources required to cover the full (and ever-expanding!) scope of her role.

- **60% of the reported breaches were due to malicious or criminal attacks (compared with 35% due to human error, and 5% due to system faults).**

  This particular statistic suggests that we shouldn't be too quick to blame technology for data security issues. In fact, humans – whether through malicious intent or by accident – are the true weak link in the data security chain.

- **The vast majority of cyber incident data breaches were the result of compromised access credentials – 153 of these involved credentials compromised through a phishing attack, 39 involved credentials compromised through a brute-force attack, and 112 involved credentials compromised by an unknown method.**

  This is an interesting statistic as it again highlights the key role that human fallibility – in this case, the likelihood of human recipients being duped by a phishing email – plays in many data breaches. It provides a useful lesson that any effective data security regime must pay attention to human security issues as technical issues.

- **83% of breaches affected fewer than 1,000 people.**

  While the larger breaches tend to hog the media headlines, most reportable breaches actually affect a relatively modest number of people. In fact, there were 232 reported breaches that affected no more than one individual. This illustrates the dangers of measuring the significance of a breach incident solely by reference to the number of people involved – any proper assessment must consider the relative impact on the security of those affected as well as the raw numbers.

Another interesting take-out from the report is this passage from the introduction written by the Commissioner:

> *We also encourage entities to move beyond compliance to effectively support consumers. While the law obliges entities regulated under the Privacy Act to provide transparent and useful information to consumers, it is those entities who focus on the consumer and navigate beyond compliance to support affected individuals to take steps to minimise or prevent harm in a meaningful way who will differentiate themselves and maintain trust over time.*

This provides a useful insight into the regulator's mindset and approach to dealing with data breach incidents. The purpose of the mandatory notification regime is not simply to punish those who do not comply, but rather it is to protect consumers and defend against potential harm that may flow from a data breach. Even with increased resources, it is unlikely that the Commissioner will ever have the capacity to actively investigate every reported breach. The Commissioner's words suggest that entities who experience a breach but go beyond what is strictly required by the law in order to look after the interests of those affected – in other words, who comply with the spirit and not simply the letter of the law – may find that they are less likely to suffer the scrutiny of the regulator as a result.

Landmark White – a case study

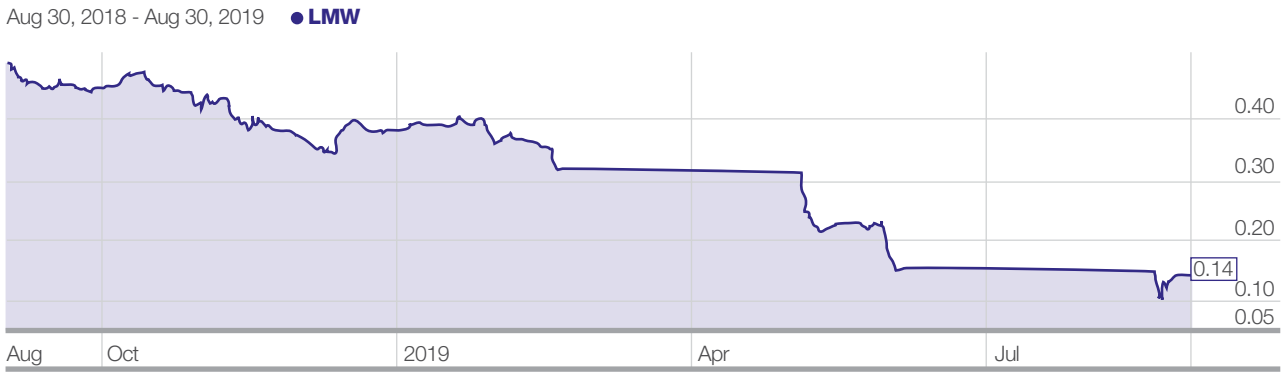
ASX-listed Landmark White experienced one of the higher profile data security breaches in 2019. The property valuation company announced to the market on 5 February 2019 that it had become aware of a data security incident involving the disclosure of a dataset containing property valuation and personal information relating to approximately 137,500 unique valuation records. The company's largest customers, the Australian banks, suspended business with the company pending the outcome of forensic investigations, and trading in the company's securities was voluntarily suspended until the financial impact of the incident could be determined.

The CEO and two non-executive directors resigned. It took approximately 6 weeks for the first of the large banks to be satisfied that their customers' data was no longer at risk and to re-instate the company to their panel of property valuers. Others followed in subsequent weeks. The company stated that the conclusion of their forensic investigation was that, except for 25 individuals, the incident presented a very low risk of harm to individuals. Despite this, the company estimated that the financial impact of being excluded from bank valuation panels resulted in a loss of revenue of between $6-7 million. Trading in the company's securities was reinstated on 7 May 2019, slightly more than 3 months after the initial announcement of the data security incident.

When trading recommenced, the share price was down by over one third of its value at the time of the initial announcement of the incident. The company then announced on 30 May 2019 a second data security incident, which they considered did not constitute a notifiable data breach for the purposes of the Privacy Act. This caused the banks to suspend instructions to the company for a second time in a short period, and a second lengthy period of suspension of trading in securities on the ASX. By the time trading in the company's securities was reinstated on 19 July 2019, the company needed to raise capital to continue operations. The share price fell again – see figure 1 for a chart of Landmark White's share price.

The case of Landmark White illustrates the potential for data security incidents to have financial consequences far beyond the direct liability to affected individuals.

Figure 1 – Share price of Landmark White



Source: Google Finance 2019

Information security for prudentially regulated financial institutions

On 1 July 2019 a prudential standard on information security took effect. Amongst other things, the standard requires regulated financial institutions to notify the Australian Prudential Regulation Authority (APRA) of certain information security incidents, including any incidents that have been notified to other regulators anywhere in the world. This means that all banks, insurers, and regulated superannuation funds will need to notify APRA as well as the Office of the Australian Information Commissioner if they are required by the Privacy Act to notify the Information Commissioner of an eligible data breach. For further information about this prudential standard, please see our alert from late 2018.

As clear as mud

There is a relative lack of case law interpreting the Australian Privacy Act. This can on occasion contribute to uncertainty as to how to comply with the Act in practice. As such, any further guidance that the Courts may provide is always welcome. This year, there were a few cases that provide an insight into some difficult interpretive challenges that apply in this area of law, though on some aspects they may perhaps only serve to add to the confusion.

Shahin Enterprises Pty Ltd v BP Australia Pty Ltd [2019] *SASC 12*

This case in the Supreme Court of South Australia primarily concerned an alleged breach of contract. However, because of the particular facts of the breach it also involved a detailed analysis of the lawfulness under the Privacy Act of providing personal information to another entity for the purposes of direct marketing. While not an easy read, given the relative scarcity of case law in this area, the judgement provides very interesting and significant (if not straight-forward) insight into how the Act may be applied in practice. Please bear with us as we step through the details for the privacy geeks out there.

Context:

The issue arose in this case after BP Australia Pty Ltd (**BP**) refused to provide Shahin Enterprises Pty Ltd (**Shahin**), one of BP's franchisees of 25 service stations in South Australia, with customer purchase information and contact details collected via a BP promotional loyalty card.

The contract between BP and Shahin provided that:

> ***Subject to relevant privacy legislation***, *BP will regularly provide to the Dealer information reasonably requested about BP card customers who visit the Dealer sites so that the Dealer may market goods and services to these customers.* [emphasis added]

Shahin requested that BP provide the name, contact details, purchase volume, and non-fuel purchase information of BP cardholders who had made a purchase at one of Shahin's service stations in the prior 24 months. BP refused, on the basis that it would breach the Privacy Act.

The use and collection of data by BP in relation to BP card customers was governed by the terms and conditions for the card program (**T&Cs**). On application for a card, BP card customers agreed to the T&Cs, which included purported consent for a range of uses and disclosures of the card information, including for direct marketing activities.

However, despite this, Blue J held that BP was not obliged to provide the requested information to Shahin as to do so would result in a breach of the Privacy Act. The process by which Blue J reached this conclusion was somewhat convoluted, but we will do our best to lay it out simply below.

Relevant provisions of the Privacy Act:

To help explain this case, and its broader significance, it is useful to provide a brief recap as to how the Privacy Act regulates direct marketing activities. The Australian Privacy Principles (**APPs**) made under the Act deal with direct marketing as follows:

- **APP6** sets out general rules that apply to use and disclosure of personal information but provides expressly that it does not apply to use and disclosure for the purpose of direct marketing.
- **APP7** deals with use and disclosure for the purpose of direct marketing. The basic proposition under APP7.1 is that an organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies. APP7.2 and APP7.3 then create two different exceptions depending on the circumstances in which the information was collected.
- **APP7.2** establishes an exception that covers circumstances where the organisation in question collected the relevant information directly from the individual concerned (rather than from a third party) **and** the individual would reasonably expect them to use or disclose the information for direct marketing.
- **APP7.3** establishes an exception that covers circumstances where the organisation in question collected the relevant information from a third party (rather than directly from the individual concerned) or collected the relevant information directly from the individual concerned but the individual would not reasonably expect them to use or disclose the information for direct marketing. In other words, APP7.3 deals with all situations not covered by APP7.2.

The drafting of APP7, in particular as to the interaction between APP7.2 and APP7.3, is complex and challenging to interpret. This fact is well illustrated by the judgement in this case, as we will shortly see.

The Court's decision:

Justice Blue made several important determinations about the effect of APP6 and APP7 which are not necessarily obvious or well appreciated.

Firstly, Blue J found that use and disclosure of personal information by an organisation for direct marketing is exclusively regulated by APP7, irrespective of whether the direct marketing in question is by the organisation itself or by a third party. In other words, the disclosure of information by BP to Shahin for the purposes of direct marketing by Shahin would be regulated by APP7, not by APP6. In reaching this conclusion, Blue J was heavily influenced by the fact that the latter parts of APP7 contain rules for how individuals may ask that organisations cease using their information for the purpose of **facilitating** direct marketing by another organisation, which led Blue J to the conclusion that the whole of APP7 must apply to that type of conduct, even though it is evidently poorly adapted for that purpose.

Secondly, Blue J found that APP7.2, which deals with information that an organisation collected directly from an individual themselves, only authorises an organisation to disclose such information for the purpose of direct marketing by that organisation itself. In this regard, Blue J was influenced by the fact there is a condition in APP7.2 that requires the organisation in question to provide a means by which an individual may request not to receive further direct marketing from that organisation. According to Blue J,

this only makes sense when there is a direct relationship between the individual and the organisation, so that APP7.2 cannot have been intended to apply to the disclosure of information for marketing activities to be carried on by a different organisation.

Thirdly, based on a somewhat technical construction, Blue J found that where an organisation has obtained personal information directly from the individual concerned then the exception under APP7.3 can only apply if the individual has consented to the use or disclosure of that information for direct marketing **but** would not reasonably expect the organisation to use or disclose their information for that purpose. In other words, Blue J reached the surprising conclusion that consent and reasonable expectation are "mutually exclusive" for the purposes of APP7.3. With respect to the Judge, this does not appear to necessarily follow from the drafting of APP7.3. An alternative, and perhaps more pragmatic, reading of APP7.3 is that it may apply where an organisation collects information from an individual in circumstances that mean, at the time of collection, that the individual would not reasonably expect the organisation to use their information for direct marketing but the individual then subsequently consents to the organisation using the information for that purpose. In other words, it may apply where a later consent overrides the original expectations of the individual about the use of their information.

Fourthly, Blue J held that while APP7.3, like APP7.2, is not well adapted for dealing with the disclosure of information by one organisation to another organisation for the purposes of direct marketing by the other organisation it nonetheless does apply to such disclosures. APP7.3 contains the same condition as APP7.2 that requires an organisation to provide a means by which an individual may request not to receive further direct marketing from that organisation. As Blue J observed in the context of APP7.2, this condition only makes sense in the context of direct marketing by the organisation itself. However, in the context of APP7.3, Blue J decided that the condition (along with other aspects of APP7.3) should simply be ignored when seeking to apply APP7.3 to a disclosure for the purposes of direct marketing by another organisation. It seems that Blue J was intent on finding a way for APP7.3 to apply to disclosures for direct marketing by a third party, even though APP7.2 could not apply to that activity. With respect, this approach does not seem well supported by the drafting of the provisions in question. While the drafting is certainly hard to tie down, it seems equally open if not preferable to conclude that either:

- APP7.3 does not apply to disclosures for direct marketing by a third party organisation for the same reasons as APP7.2 and, for that reason, it would be better for such disclosure to be regulated under APP6. This reading could be supported by drawing a distinction, as some parts of APP7 do, between a disclosure "for the purpose of direct marketing" and a disclosure "for the purpose of **facilitating** direct marketing" [emphasis added] with the former regulated exclusively under APP7 but the latter regulated by a combination of APP6 and APP7; or
- both APP7.2 and APP7.3 do apply to disclosures for direct marketing by a third party organisation, but that the conditions they impose as to how the direct marketing may be carried out should only apply to the organisation actually responsible for the direct marketing activity.

Finally, having reached the conclusions above, in order to resolve the contractual dispute Blue J had to determine whether relevant BP cardholders had in fact consented to BP disclosing their information to Shahin for the purpose of direct marketing by Shahin. Based on the wording used in the T&Cs and associated privacy policy, Blue J found that they had not – they only contemplated use for marketing by BP, not by a third party. Accordingly, BP was not obliged to share any cardholder information with Shahin, as to do so would result in a breach of law under the APPs.

One final important practice point worth noting is that Blue J also rejected the proposition that APP6 only contemplates and permits a single primary use of information collected by an organisation. However, Blue J did say that "nevertheless the purposes for which information was collected will necessarily be finite, will typically be a single purpose and will usually be of very limited number if more than one." In other words, according to Blue J, the primary purpose for which information is collected should be construed narrowly and usually, even if not always, limited to a single purpose. This runs counter to concerns raised by the ACCC in the Digital Platforms Inquiry about the potential for organisations to define primary purposes of collection very broadly and thereby to subvert the rest of the regime established under the APPs. If that conclusion does not match with the actual interpretation of APP6 by the Courts, then it raises questions as to the foundation for some of the more wide-ranging recommendations for law reform in this area made by the ACCC.

Key takeaways:

- The state of the law on use and disclosure of information for the purposes of direct marketing by a third party is less than clear. It would benefit from either a redrafting of the current APPs, or else from further judicial consideration to shed more light on this area.
- Clear wording is required in end user T&Cs to provide a basis to argue that consumers have consented to the disclosure of their information to a third party for the purposes of direct marketing by that third party.
- If two APP entities wish to enter into a data sharing arrangement for marketing purposes, it would be wise to include a contractual obligation to obtain appropriate consents and give relevant notices to individual customers to facilitate that objective.
- In the view of Blue J, the primary purpose for which an organisation collects information should be narrowly construed. Organisations do not have licence to define their own broad primary purposes. This may raise some queries about the basis for some recommendations made by the ACCC in the Digital Platforms Inquiry.

Jeremy Lee v Superior Wood Pty Ltd [2019] FWCFB 2946 (1 May 2019)

This decision of the Fair Work Commission Full Bench (**FWCFB**) concerned an unfair dismissal claim where an employee had refused to use biometric fingerprint scanning at his workplace.

The plaintiff, Mr Lee, was dismissed by his employer, Superior Wood, for failing to comply with a new site attendance policy that required employees to use fingerprint scanners to sign on and off at work. Mr Lee argued that the biometric data contained in his fingerprint was sensitive information under the Privacy Act and that Superior Wood was not entitled to require such information from him. On that basis, Mr Lee claimed that his failure to comply with the new site attendance policy was not a valid reason for his dismissal.

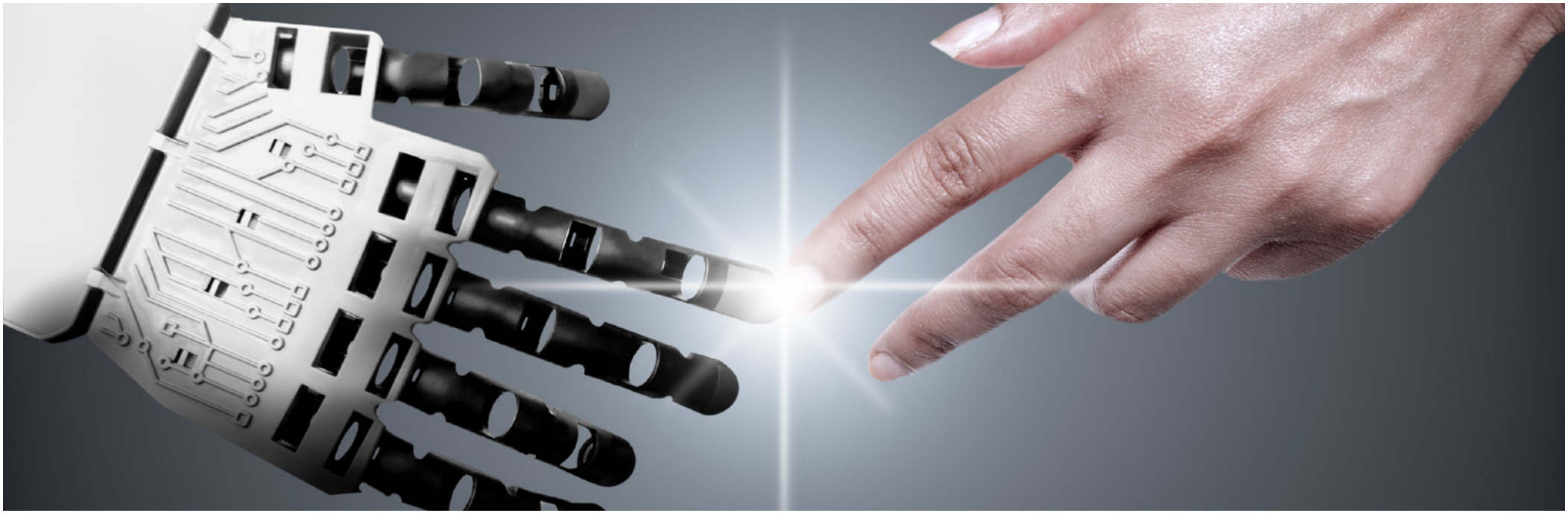
In response, Superior Wood argued that the biometric data collected through the fingerprint scanner formed part of an "employee record" and as such was covered by an exemption that applies under the Privacy Act for use of such records by an employer in relation to a current or former employee relationship. However, the FWCFB held that this exemption only applied to the use and disclosure of employee records already held by an employer, and not to the process of collecting those records in the first place. The reasoning to support this conclusion rested largely on the fact that the relevant exemption in the Privacy Act is drafted in the present tense – that is, it refers to an act or practice related to an employee record held by the relevant entity (where "hold" is defined to mean having possession or control over a record). This could, on it face, suggest that the exemption should only apply to existing records *held* by the employer, rather than future records that are yet to come into existence.

The FWCFB's approach may be considered a relatively novel construction that substantially narrows the effect of the exemption and does not fit neatly with the remainder of the Privacy Act. For example, if correct, the FWCFB's findings mean that an employer will need to comply with the requirement under APP5 to provide a collection notice to employees before collecting information required for an employee record, including by setting out in those notices information relating to APPs that may not in fact apply to any subsequent handling of the employee record (such as how to complain about a breach of the APPs, even though they may not apply to the employee record). This would seem an incongruous and redundant requirement.

Respectfully, the approach taken by the FWCFB does not appear to necessarily follow from the wording of the Privacy Act itself, and the FWCFB has perhaps over-emphasised a grammatical subtlety. In any event, it is clearly arguable that the act of an employer in collecting information required for the creation of an employee record should be taken to be an act or practice relating to the resultant record that is then held by the employer. Certainly such a reading would appear to more closely follow the intention of the then Attorney-General Daryl Williams QC when he said in the second reading speech introducing the relevant amendment to the Privacy Act that "It should be noted, however, that the exemption is limited to *collection*, use or disclosure of employee records where this directly relates to the employment relationship." Mr Williams may be surprised that the law he proposed did not in fact apply to the act of collection as he meant it to.

Key takeaways:

- The employee records exemption may be applied quite narrowly in practice. Adopting a cautious approach, employers may wish to assume that the exemption will not apply to the collection of new information from an employee. In this case, they should prepare suitable collection notices and otherwise follow standard collection procedures that comply with the APPs when dealing with employees as well as when dealing with other individuals.
- Further consideration of the Privacy Act by higher courts may help to provide greater certainty as to how the Act, including relevant exemptions and rules set out in the APPs, will be applied in practice.



Australian government agencies – privacy governance code

All Australian government agencies have been required to comply with the Privacy (Australian Government Agencies – Governance) APP Code 2017 since 1 July 2018. A key feature of the Code is a requirement for agencies to have a privacy management plan and to designate Privacy Officers and a Privacy Champion as part of an agency's privacy management and governance framework. The Code also mandates the conduct of a privacy impact assessment for all "high risk privacy projects". A project will be a 'high privacy risk project' if an agency reasonably considers that the project involves new or changed ways of handling personal information – where that is likely to have a significant impact on the privacy of individuals. Agencies are required to maintain a register of the privacy impact assessments that have been conducted under the code and to publish a version of that register. Some agencies have been choosing to publish the privacy impact assessments they have conducted (notably the Australian Bureau of Statistics), whereas others have merely published a list and indicated that a copy may be sought under Freedom of Information law.

Will the United States get with the program on privacy?

In January 2019, Apple CEO Tim Cook published an article calling for "comprehensive federal privacy legislation" in the United States. It may come as a surprise for those used to doing business in a jurisdiction, such as Australia or any European country or any number of other countries around the world, that already has a cohesive national privacy law in place. However, the United States has long been a vexed jurisdiction on privacy matters, with a complex and patchy web of state-based laws.

Cook's call was for consumer controls – such as rights of notification of collection and rights of access to data – that will be recognisable to those familiar with Australian and European privacy regimes. However, he also proposed a national "data-broker clearinghouse" to be established by the Federal Trade Commission, which would register and track bundled data transactions and represents a far more novel concept. Details aside, the key theme of his article is that legal protections for privacy are important and demand a unified national approach.

These moves from industry are symptomatic of the growing importance of privacy and trust to companies wishing to protect and deepen their relationship with their customers. A consistent and comprehensive system of privacy laws is actually a very useful tool for building trust. It is also something that has been a topic of interest for politicians of all persuasions in the US. For more than a year now, the US Congress has hosted committee hearings to determine whether the legislative body should pass such a federal privacy law and, if so, what it should look like. Alongside these hearings, members of Congress have introduced a number of privacy bills (7 already in 2019, coming from both sides of the increasingly wide political aisle), with each setting out a different vision for what will be required of companies dealing in personal data. While none of the bills have been put to a vote, taken together they give a clear indication that there is broad political will on this issue.

The privacy regime most commonly considered to be a likely model for a federal US law is that of the State of California. First introduced in the California State legislature in 2018, the California Consumer Privacy Act (**CCPA**) was signed into law by Governor Jerry Brown in June 2018 and will become effective on 1 January 2020. Under the CCPA, Californian residents will be able to view the data that businesses have collected on them, request the deletion of their data, and opt-out of having their data sold to third parties. One of the main concerns raised in relation to the prospect of a new federal privacy law in the US is that it may pre-empt state initiatives like the CCPA and result in watered-down protections for consumers and their data. Of course, one of the main upsides would be a consistent and potentially more globally aligned set of domestic standards for the many multinational organisations that call the US home. Only the politics, comity and intellectual rigour of the current US Congress now stands in the way!

KING&WOOD MALLESONS
金杜律师事务所

The Power of Together

About King & Wood Mallesons

Recognised as one of the world's most innovative law firms, King & Wood Mallesons offers a different perspective to commercial thinking and the client experience. With access to a global platform, a team of over 2,000 lawyers in more than 27 locations around the world works with clients to help them understand local challenges, navigate through regional complexity, and find commercial solutions that deliver a competitive advantage for our clients.

As a leading international law firm headquartered in Asia, we help clients to open doors and unlock opportunities as they look to Asian markets to unleash their full potential. Combining an unrivalled depth of expertise and breadth of relationships in our core markets, we are connecting Asia to the world, and the world to Asia.

We take a partnership approach in working with clients, focusing not just what they want, but how they want it. Always pushing the boundaries of what can be achieved, we are reshaping the legal market and challenging our clients to think differently about what a law firm can be.

Media enquiries

Charlotte Geddes
Corporate Affairs Senior Manager
T +61 2 9296 3348
charlotte.geddes@au.kwm.com

Join the conversation on Facebook, Twitter, LinkedIn, and on our blogs China Law Insight and In Competition.

Asia Pacific | Europe | North America | Middle East

0690O - 08/18