A New Decade of Data Privacy

Eli Fisher, Senior Associate at Baker McKenzie, discusses the main developments in data privacy law in the 2010s and comments on what lies ahead in the 2020s.

Introduction

Data privacy sits today atop the regulatory agenda of many countries around the world. But it wasn't always this way. In fact, it is hard to think of an area of law that has leapt so decisively as did privacy law from peripheral to central in the concerns of regulators, businesses and individuals in the previous decade.

It's an interesting exercise to break things up by decades, as Sam Seaborn once did when advising on the nomination of a Supreme Court justice at the turn of the millennium:

> *It's not just about abortion, it's about the next 20 years. In the '20s and '30s it was the role of government. '50s and '60s it was civil rights. The next two decades are going to be privacy. I'm talking about the Internet. I'm talking about cell phones. I'm talking about health records and who's gay and who's not. And moreover, in a country born on the will to be free, what could be more fundamental than this?*

Two decades ago, in the year 2000, the Office of the Privacy Commissioner was established, and the *Privacy Amendment (Private Sector) Act 2000* extended coverage of the Privacy Act to some private sector organisations and introduced 10 National Privacy Principles. (I know. It doesn't have the same soaring Sorkinesque cadence as the way Sam put it.)

A decade later, the ALRC's *For Your Information* report was continuing to shape privacy policy, as it had been since August 2008 when it was first released to the public. That report with its 295 recommendations set in motion the reforms to the law that we have today.

APPs

In 2012, Attorney-General Nicola Roxon circulated the explanatory memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), which would explain the greatest changes to Australian privacy law to date. In response to the ALRC's report, the Bill would eventually amend the Privacy Act to create the APPs, a single set of privacy principles applying to both federal government agencies and private sector entities. The APPs replaced the federal public sector's IPPs and the private sector's NPPs that had previously governed the handling of personal information. The Bill also introduced more comprehensive credit reporting with improved privacy protections, introduced new provisions on privacy codes and clarified the functions and powers of the Privacy Commissioner.

These amendments took effect on 12 March 2014. Some of the most noteworthy changes were the introductions of APP 1 and APP 5, which forced APP entities to be more transparent about their handling of personal information, through privacy policies and collection notices. We were also introduced to the requirement under APP 2 to permit pseudonymity and anonymity where practicable. APP 7 enhanced the requirements for informed user consent in relation to direct marketing. And APP 8 proposed to hold the APP entity that transfers personal information overseas accountable for the conduct of the overseas recipient. The Privacy Commissioner was buttressed by new powers, including the ability to obtain enforceable undertakings, to seek civil penalty orders and to obtain injunctive relief.

These reforms were game-changing. But they left certain issues unresolved. When is information about a person as opposed to a device or a network? Is a voluntary data breach notification scheme sufficient? Do the penalties and enforcement powers of the Privacy Commissioner give privacy law enough teeth to warrant serious corporate attention? Can privacy really be protected by territorial laws, or is it necessary to take an international or extraterritorial approach to regulating data processing? Can consent really be the silver bullet for data handling in this day and age? Do individuals need the ability to protect their privacy directly, or can reliance be placed on a Data Protection Agency, such as the Privacy Commissioner? These questions would continue to arise throughout the decade.

Grubb

In 2013, still under the previous NPP framework, Ben Grubb a Fairfax tech journalist made a request for the metadata that Telstra, his mobile phone provider, held about him. This was back in the day when the Government was working on the introduction of the mandatory data retention laws requiring telcos to retain metadata on their customers for two years. Grubb was curious as to what metadata was being collected. Telstra provided some information, but refused to provide its mobile network data, which included metadata such as IP addresses and, most crucially, geolocation data.

Grubb responded by lodging a complaint with the Privacy Commissioner. Telstra maintained that the geolocation data it had for Grubb - the longitude and latitude of mobile phone towers connected to the phone at any point in time - were not personal information about a customer. Telstra's argument was that the data were

about the device, not about Grubb. The Privacy Commissioner found against Telstra in May 2015 on the basis that Telstra could cross-match different datasets allowing Grubb to be linked back to the geolocation data of his phone.

Telstra appealed the Privacy Commissioner's decision to the AAT, and was successful. Basically the arguments here dealt with whether the information Grubb was seeking, and Telstra was withholding, was 'personal information' as defined by the Privacy Act. The definition of personal information (which has since changed) relevantly referred to information about an individual whose identity is apparent, or can reasonably be ascertained from the information. The parties had argued about whether Grubb's identity could reasonably be ascertained from the network data, which depended on the cross-matching efforts Telstra would need to go to, to ascertain Grubb's identity. The AAT held that the network data that Grubb was seeking was not information about Grubb, but information about the service Telstra was providing to Mr Grubb.

The Privacy Commissioner appealed the AAT's decision to the Full Court and lost (as, incidentally did everyone who wanted clarity on these important questions). The Full Court could only answer questions of law, and did not accept the Privacy Commissioner's interpretation of the definition of 'personal information'. But it did not determine whether the information in question was 'about' Grubb, or whether Grubb's identity could reasonably be ascertained from the metadata. And thus, the most authoritative review of the centrepiece of privacy law - 'personal information' - ended with no great clarity. The Privacy Commissioner released a public statement welcoming the decision as it provides important guidance as to what is 'personal information': "In particular, the Court has confirmed that assessing what is 'personal information' requires an 'evaluative conclusion, depending on the facts of any individual case' and that 'even if a single piece of information is not 'about the individual' it may be about the individual when combined with other information'."

GDPR

The General Data Protection Regulation (**GDPR**) came into force on 25 May 2018 in all member states of the European Union, and brought along a new regime of data protection laws - and large penalties - that replaced all existing privacy law in the European Union. It was approved and adopted on 14 April 2016 by the European Parliament, giving businesses over two years to prepare for significant changes.

The GDPR is an ambitious regime which aims to harmonise data protection laws across the EU, while enhancing the protections afforded to the privacy of people in the EU. The regime was described as the most important change in data privacy regulation in 20 years.

Much can and should be said about this significant development, including in relation to the mandatory data breaches scheme, the lawful bases for processing under Article 6, which require any processing of personal information to be justified by one of the listed lawful bases and expressly so, and the individual rights which captured much of the media attention surrounding the GDPR. The GDPR provided to individuals the right to be informed about the personal data an organisation holds about them; to access the personal data; to rectify the data; to have the data erased (otherwise known as the right to be forgotten); to restrict processing of personal data; to data portability; to object to the processing of personal data; and rights in respect of protection from automated decision making, including profiling.

The GDPR also changed the privacy game by providing for penalties that are starkly unfamiliar to Australian privacy practitioners. Under the GDPR, there are increased administrative fines for non-compliance: serious contraventions can result in penalties of up to €20 million or 4% of annual worldwide turnover (whichever is higher), and less serious contraventions can result in penalties of up to €10 million or 2% of annual worldwide turnover (whichever is higher). Penalties under the GDPR are in sharp contrast to those available under the Privacy Act, which (at least currently) gives the Privacy Commissioner enforcement powers including maximum civil penalties of up to $2.1 million. Ordinarily, privacy complaints in Australia are resolved with limited financial cost to the infringer, by way of penalty or compensation.

But perhaps the most interesting aspect of the GDPR both generally and for practitioners here in Australia is its purported extraterritorial reach. An Australian business needs to comply with the GDPR if it: (a) has an establishment in the EU; or (b) targets people in the EU, either in relation to the offer of goods or services to them or in relation to monitoring their behaviour. Thus, it is necessary for businesses in Australia to apply not just the standards of the Australian privacy law to their data processing, but also in certain circumstances the stricter foreign standards of the EU.

As with the former Data Protection Directive, the GDPR imposes restrictions on the transfer of personal data overseas. The approach is more permissive in respect of transfers to countries that have achieved an 'adequacy decision' from the European Commission. Australia is not on the EU's white list, unlike New Zealand, Canada, Israel, Argentina and Japan among others, which means that Australia's participation in the European market is hindered by its privacy laws. In other words, there may be pressure to reform

Australian privacy law in order to achieve an 'adequacy decision' from the European Commission and more freely participate in the European market.

The ACCC raised this as an issue in its Digital Platforms Inquiry, discussed below, as a potential benefit of enhancing privacy protection in Australia. Australia's privacy law framework was last considered for these purposes in 2001, and there were eight principal areas of concern, including the exemption of most small businesses and employee data from the scope of the Privacy Act.

Mandatory Data Breaches Notification (MDBN) Scheme

In February 2018, roughly thirty years after the Privacy Act's commencement, it became mandatory for APP entities to notify the Privacy Commissioner and affected individuals of certain types of data breaches. Prior to this, the notification of a data breach was voluntary and rarely used.

This requirement came into effect a few months prior to the GDPR coming into effect, but well after it had been adopted in April 2016. The Australian scheme was modelled heavily on the European one, although there are some differences.

In Australia, APP entities must give notice of eligible data breaches. Eligible data breaches take place where: (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by any entity; and (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates. The APP entity must give notification if it has reasonable grounds to believe that an eligible data breach has happened, or it is directed to do so by the Privacy Commissioner. If unsure about whether what has happened is an eligible data breach, but there are reasonable grounds to suspect that it may have been an eligible data breach, the APP entity must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that an eligible data breach has taken place.

At the Privacy Commissioner's encouragement, APP entities around Australia prepared for the MDBN scheme by developing data breach response plans tailored for their organisation. According to the OAIC, in the first year of the MDBN scheme, 964 data breaches were notified, being a 712% increase on the previous twelve months under the voluntary scheme. 60% of the data breaches were malicious or criminal attacks, and 153 of the notifications were attributed to phishing. 28% of the breaches were cyber incidents where credentials were obtained by unknown means, and the vast majority of data breaches - 83% - affected fewer than 1,000 people. 35% of the notified data breaches involved human error such as unintended disclosures of personal information or the loss of a data storage device. 55% of the data breaches that occurred within the health sector, and 41% of the data breaches that occurred within the finance sector were attributed to human error (compared with 35% for all sectors). 86% of the notified breaches involved the disclosure of contact information.

Following the introduction of the Australian scheme was the implementation of the GDPR scheme in May 2018, as well as a Canadian mandatory data breach notification scheme in November 2018, and a proposal for a mandatory data breach notification scheme in New Zealand.

OAIC

The Office of the Australian Information Commission, which houses the Privacy Commissioner, was overhauled in 2010, at the same time as the FOI system which the OAIC also administers was being revamped. Three roles were introduced at the head of the OAIC: the Information Commissioner, the Privacy Commissioner and the FOI Commissioner. In 2014, the Coalition government tried to abolish the office altogether, and almost succeeded. Its attempts were knocked back in the Senate. The OAIC's funding was so heavily cut, though, that the office in Canberra was closed and the former Commissioner was working from home.

Even with funding partly restored in 2016, the OAIC was still, according to many commentators, under-resourced. Transparency International Australia has said that the under-resourcing of the OAIC has left it on 'life support'. In March 2019, the Government announced a $25.1 million increase to the OAIC's funding over three years, which according to the current Information and Privacy Commissioner, Angelene Falk, enabled the OAIC to hire 31 more staff, boosting its head count to 124.

Stronger privacy protection

On 24 March 2019, tougher penalties and other measures to protect Australians' privacy were announced. Once implemented, serious or repeated privacy breaches may attract increased penalties of whichever is the greater of: (a) $10 million; (b) three times the value of any benefit obtained through the misuse of the information; or (c) 10% of a company's annual domestic turnover. These penalties are still well short of those enacted by the GDPR, but bring contraventions of the privacy law in line with those of the Australian Consumer Law.

Further, the OAIC will have new infringement notice powers and other expanded options available to address breaches. Rather than having to approach the Federal Court to seek a pecuniary penalty, the OAIC would once implemented be able to use this relatively straightforward administrative remedy, in a manner similar to the ACCC and the ACMA.

Additionally, social media and online platforms will be required to stop

using or disclosing an individual's personal information on request. This would be a powerful new individual right, albeit somewhat less powerful than the right to erasure.

Moreover, there will be enhanced protection for vulnerable groups, in particular children. Lastly, the OAIC will receive significant additional funding, which did not happen when the MDBN scheme was implemented - despite the considerable additional pressure that administering the MDBN scheme would have placed on the OAIC's resources.

Digital Platforms Inquiry

In December 2017, the ACCC began its inquiry into digital platforms - that is, search engines, social media providers and digital content aggregators - on competition in the media and advertising services markets. The inquiry was a wide-ranging exploration of the market power of digital platforms and their role in Australian society, which surveyed competition and consumer law, M&A, copyright and media regulation and the viability of journalism and the importance of media literacy in the community. But with various high-profile privacy breaches unfolding during the course of the inquiry, the focus firmly shifted to privacy regulation in Australia. One of the most noteworthy aspects of the ACCC's final report is the relatively new role for the competition and consumer regulator to play (alongside the OAIC) in protecting privacy.

The ACCC made a raft of recommendations designed to strengthen privacy protections in Australia. First, perhaps harking back to the Grubb case, the ACCC recommended that the definition of 'personal information' be amended so that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual. The ACCC wants the requirements around notification and consent to be strengthened. Drawing inspiration from the European Union, the ACCC wants to see an erasure right, direct rights of action for individuals and higher penalties for breach. In addition to these changes, the Australian law should remove the exemptions for small businesses, employers and political parties. This would bring Australian law more in line with the European Union. There's yet another recommendation for a statutory tort of privacy. And the ACCC also recommends that the law require that all uses and disclosures of personal information be "fair".

That last point is an interesting one, because it makes really clear the intersection between privacy law and consumer law reflecting the author of the report.

The ACCC is naturally occupied with administering competition and consumer law. Privacy law is usually the domain of the OAIC, and communications and media law are usually the domains of the ACMA. Although privacy was not initially within the remit of the Ministerial direction commissioning the inquiry, various international developments prompted the ACCC to focus on data privacy as well. This was an interesting development in the approach to regulating personal data, because it made clear that data protection is a consumer welfare issue too.

One recommendation in particular bears that out really clearly, being the one that recommends that the *Competition and Consumer Act* be amended so that unfair contract terms are prohibited (as opposed to merely voidable, as is the current position). This would mean that there would be penalties applying to the use of unfair contract terms in any standard form consumer or small business contract. This came up in the context of the digital platform inquiry because the ACCC is concerned, in particular, with the bargains being struck between consumers and digital platforms for the collection, use and disclosure of personal data. That is, instead of looking at privacy through privacy lens only (notice, consent, reasonable expectations and so forth), the ACCC is protecting privacy by focusing on consumer issues such as unfair terms in standard form contracts between parties with bargaining power imbalances. There's an important paradigm shift there.

What practical changes will follow from the report? The Government has committed immediately to establishing a special digital platform unit in the ACCC. The Government is also setting in motion a broad review of the privacy law, and it supports most of the ACCC's recommendations in respect of privacy law changes. The Government stated that it "will commence a review of the Privacy Act to ensure it empowers consumers, protects their data and best serves the Australian economy. A review will identify any areas where consumer privacy protection can be improved, how to ensure our privacy regime operates effectively for all elements of the community and allows for innovation and growth of the digital economy. The review will also allow for further consultation on the ACCC's reform proposals to enable consumers to request the erasure of their personal information."

What's next?

Sam Seaborn was right when he said in 1999 that the next two decades would be about privacy. And this sentiment was not at the time to be taken for granted. In the same year, Sun Microsystems CEO, Scott McNealy, famously told a group of reporters: "You have zero privacy anyway. Get over it." But with some certainty, we can say that privacy is going to continue sitting atop the regulatory agenda throughout the 20s. As Mark Zuckerberg said in 2019: "the future is private".

If the ALRC's report in 2008 set the tone for privacy reforms that came into effect in 2014, it may be fair to say that the ACCC's digital platforms

report and the inquiries that it will trigger will shape the next round of privacy reform well into the 2020s.

Putting on a pundit hat, here is some shamelessly unaccountable privacy speculation for the roaring 20s:

- With bipartisan support, the US will overcome the obstacles that had to date prevented the enactment of a comprehensive omnibus GDPR-like privacy law that applies federally and extraterritorially. Importantly, a clear, comprehensive statute will provide greater certainty to the tech companies that are subject to increasing regulatory scrutiny. Already in 2019, Mark Zuckerberg, Tim Cook and Sundar Pichai called for a comprehensive federal privacy legislation. Just as the GDPR went some way to becoming a default industry standard for data handling worldwide through its extraterritorial reach and sizeable market, the US law will drive the notion of a default industry standard even further. With GDPR-like restrictions on cross-border sharing to jurisdictions with inadequate privacy protection, other countries will look to enhance their data processing laws.
- Australia, in part motivated by a desire to trade more freely with Europe and the US, will enhance its privacy laws to bring them in line with what will increasingly become over the decade international standards. The small business and employee records exceptions will be the first to go.
- The ACCC, the eSafety Commissioner and the ACMA will join the Privacy Commissioner in the administration of data privacy in Australia. The Government's heightened appreciation for the value of data and the importance of data security will lead to stronger funding and a more holistic approach to privacy enforcement.
- With the increased application of privacy law across the Australian economy (with the removal of the small business exception), and with the increase in penalties and funding of enforcement, privacy law will become a critical compliance issue for businesses, similar to competition and consumer law.
- We will have at least four more commissioned recommendations for a privacy tort. But no tort.
- Lawmakers will struggle to find a way around the 'privacy paradox', whereby individuals purport to care about privacy but behave in ways that suggest otherwise. The well-intentioned attempts to require meaningful, informed, clear and unambiguous consent fail - because individuals don't have the capacity to grapple with each service provider's privacy policy. Instead of placing any reliance on an individual's 'consent', the Government will turn to a set of replaceable rules for data processing that effectively constitutes each entity's privacy policy. The replaceable rules become the default position, whereby entities can assume they have consent and data subjects understand the general rules of operating in the digital economy. Where a particular entity proposes to do something contrary to the replaceable rules, they are required to obtain the Privacy Commissioner's authorisation to implement such a practice and then each user's consent in relation to those items only.