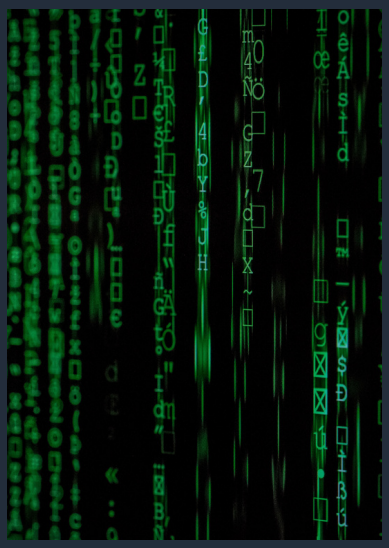
Flinders University

Jeff Bleich Centre for the US Alliance in Digital Technology, Security & Governance



The Obligation to Protect

Australian law and the requirements to protect information

Joel Lisk
Research Associate (Space & Regulation)
Jeff Bleich Centre

JBC POLICY PERSPECTIVES #2

Data breaches are becoming increasingly frequent and can involve the information of millions of Australians. Does Australian law say enough about how information should be protected?

Data breaches have been increasing in frequency in recent years and Australians have not been immune. The last 12 months have seen massive data breaches involving Australian companies entrusted with personal information on hundreds of thousands to millions of individuals. Recent data breaches have brought the issue of data protection into common conversation. Medibank Private, a large private health insurer, suffered a breach in 2022 that has involved an estimated 9.7 million current and former customers. Optus was victim of an attack that compromised the personal information on 9.4 million individuals (including drivers licences and passports). Latitude Financial announced that it had been the victim of a cyber attach in March 2023 that compromised the personal information of 14 million customers and saw the release of identity documents dating back to 2005. In April 2023, hackers targeted a different type of entity, stealing 2.6TB of data – including personal information and sensitive client documents – from large law firm, HWL Ebsworth.

These recent and large-scale data breaches are not isolated. The Australian Cyber Security Centre reported that it received 76,000 cybercrime notifications in the 2021-2022 Financial Year. These statistics, along with the recent large scale data breaches, has led to serious questions being asked about the measures that businesses employ to protect the personal information they collect, hold and process, but what does the law say? And should it say more?

Privacy Law

There is no broad, economy wide requirement on businesses to protect the personal information they hold. Saying this, there are some requirements in the *Privacy Act*. The *Privacy Act*, originally introduced in 1988 and amended over time, sets out the legal obligations of a range of entities – primarily businesses in Australia – with respect to personal information. It is important to recognise, personal information is not any and all information related to an individual, it is information about an identified or reasonably

identifiable individual. This means that there are substantial volumes of data that are not directly regulated or are subject to narrower regulation (like the protection of information in the My Health Records system).

The Privacy Act requires that businesses take reasonable steps in the circumstances to prevent personal information from being misused, interfered with, lost or from being the subject of unauthorised access, modification or disclosure. This obligation applies to personal information irrespective of its form – so both digital and hard copy information must be protected.

So, how should information be protected?

While the Privacy Act's requirement to protect personal information is important, it is far from specific and this intentional. The vague paraphrasing allows those that hold personal information to decide the measures they deem to be reasonable in their circumstances. This means that a small family retail business that only sells from their physical shop front can employ different data protection mechanisms to that of their bank with millions of customers. In practice, the regulator, the Office of the Australian Information Commissioner, recommends that businesses consider the nature of information they hold and implement appropriate organisational, technical and physical measures. Again, this is not overly specific, but does suggest that businesses should create a culture that protects personal information, use technology to protect personal information and physically secure personal information when necessary.

Is vague enough?

Understandably, in the context of the recent large scale data breaches, the Privacy Act has been subject to a degree of scrutiny with the prevailing question being – is the law doing enough?

Internationally, data protection is an important issue. Some would know that the European Union's General Data Protection Regulation is renowned for containing strong protections for individuals. Recent laws in other countries including New Zealand, the United Kingdom and several US States have also started to put greater emphasis on protecting the individual.

At the time of writing, the Privacy Act is under review and the generality of the information protection requirements has been recognised. This has included the suggestion that the text of the law make specific reference to technical and organisational measures and that retaining a non-specific law protects the flexibility of the law. At the same time, there have been calls for the law to also include a set of 'baseline' outcomes, much like the European Union's approach that lists out 'appropriate' measures that can be used. The risk with this approach is that once 'minimum' measures are specified, they might become the only measures a business employs to protect personal information.

Relevant to the discussion on whether Australia's law currently does enough is the broader landscape. As noted earlier, the

Privacy Act is not the only instrument that regulates consumer information in Australia. In 2019, the Australian Government introduced a regime known broadly as the 'Consumer Data Right'. The purpose of this regime was to increase data portability and ensure individuals had greater access to the personal information that exists about them. The Consumer Data Right is far from ubiquitous though and only applies to the banking and energy sectors at the time of writing. The framework for the Consumer Data Right is dense and prescriptive. While there is a vague top level obligation to protect information falling within the four corners of the Consumer Data Right regime, the statutory rules that govern the operation of the scheme are far more prescriptive. These rules include obligations around the design and implementation of governance frameworks for Consumer Data Right information, minimum information security control standards (which includes requirements to use multi-factor authentication, encryption and system vulnerability management, amongst other things). The specificity of this regime when it comes to protection obligations is extremely far from the general obligation contained within the *Privacy Act*. In many respects, this reflects the specific and sensitive nature of the information falling within the Consumer Data Right regime, but does suggest that the Australian Government is willing and capable of imposing stricter standards on the holders of personal information in the right circumstances.

Whatever the ultimate decision of the best approach is, any change in obligation will impact millions of Australians in an increasingly precarious technological landscape where information is valuable.

Further Reading

For further analysis of Australia data protection laws, please see the forthcoming article Data Security in Australia: The Obligation to Protect, which will appear in the October issue of the Australian Law Journal.

Australian Cyber Security Centre, Annual Cyber Threat Report: July 2023 to June 2022, Australian Signals Directorate (4 November 2022) https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

Attorney-General's Department, Privacy Act Review: Report 2022, Australian Government (16 February 2023) https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

Joel Lisk is a Research Associate with the Jeff Bleich Centre.

His research focuses on the ways that nations approach the regulation of technology, with a focus on digital technology and outer space. Joel writes on topics in areas such as space regulation, competition and consumer protection law and data protection.

LEARN MORE ABOUT THE JBC

July 2023

Flinders University

Jeff Bleich Centre

for the US Alliance
in Digital Technology,
Security & Governance

Partner with us
Collaborating with the JBC will maximise the opportunities of emerging technologies to laws, policy, governance and political behaviours. Our independence, which we continuously endeavour to protect, amplifies the advantages for our partners.

Contact us
Flinders.edu.au/jeff-bleich-centre