HERBERT SMITH FREEHILLS

DOING BUSINESS IN AUSTRALIA

PRIVACY

HERBERT SMITH FREEHILLS

Chapter 22

Privacy

In Australia, privacy legislation impacts how organisations handle personal information, conduct surveillance and engage in direct marketing. National privacy laws and state-based health privacy laws govern the collection, use, disclosure and transfer of personal and health information.

Most state and territory public sector agencies are regulated by state-based privacy laws, and these sometimes extend to private sector organisations engaged by those public sector agencies.

There are also a range of specific laws and codes regulating information, industries and activities including surveillance, telecommunications, direct marketing, websites, criminal records, financial services, government registers, cybercrime, identity theft, market and social research and company registers.

This chapter is designed to provide an introduction to some of the key regimes.

Privacy Act 1988 (Cth) (Privacy Act)

The Australian Privacy Principles

The Australian Privacy Principles (**APPs**) apply to private sector organisations with an annual turnover of more than A$3 million and their related companies, as well as some others including health service providers and organisations that trade in personal information. The APPs also apply to Federal government agencies.

The Act extends to the activities of foreign companies in Australia, and to the activities of foreign companies outside Australia, where those companies carry on business in Australia, and collect or hold personal information in Australia. The Office of the Australian Information Commissioner (**OAIC**) considers the collection of personal information from an individual located in Australia to be a collection ‘in Australia’, even if the company collecting the information is outside Australia at the time.

It is important to note that the approach of the Privacy Act differs from the European model in that the Privacy Act does not contemplate the roles of, and distinctions between, 'data controllers' and 'data processors'.

The 13 APPs regulate the manner in which any regulated organisation can collect, store, use and disclose personal information. Special provision is made with respect to health and other sensitive information, which includes personal information about racial or ethnic origin, religious beliefs or affiliations, political or philosophical beliefs, membership of a political, professional or trade union or association, sexual preferences or practices, genetic and biometric information and criminal record.

Some exemptions apply, including for employee records, media and political parties.

Data breach notification

Entities regulated by the APPs are also subject to the 'notifiable data breaches' scheme. Entities must promptly notify the OAIC and affected individuals where there is loss of or unauthorised access to or disclosure of personal information, and the incident is likely to result in serious harm.

Credit reporting

Part IIIA of the Privacy Act and the *Privacy (Credit Reporting) Code* apply to Australia's consumer credit reporting system, under which credit providers contribute to and access the consumer credit histories of individuals held by credit reporting bodies such as Equifax, Illion (formerly Dun & Bradstreet) and Experian. The requirements primarily relate to consumer credit information, but this is sometimes used in connection with commercial credit arrangements, e.g. where sole traders or guarantors are involved.

Tax file numbers

The Privacy Act also deals with the protection of tax file numbers, primarily through the binding Privacy (Tax File Number) Rule issued by the Privacy Commissioner. This Rule also complements some related provisions in tax legislation.

Spam

The *Spam Act 2003* (Cth) (**Spam Act**) regulates the sending of 'commercial electronic messages' by anyone (including individuals) in, into or from Australia. In most cases, commercial electronic messages must not be sent without consent, and must include valid contact information and an unsubscribe facility. The collection and use of some automatically

harvested lists of email addresses is also banned.

Telemarketing and the Do Not Call Register

The Do Not Call Register was established in 2006. The types of numbers which may be included on the Register include home phone, personal mobile and fax numbers. Businesses must 'wash' their marketing lists against the Register to avoid calling or faxing those numbers.

An associated mandatory industry standard regulates telemarketing and market research calls generally, including prohibited calling times, information to be provided during calls, call-termination requirements and the use of calling line identification.

Health records

Notwithstanding the fact that the Privacy Act regulates the manner in which all personal information (including health information) is handled, there are additional health records laws in three state/territory jurisdictions: New South Wales, Victoria, and the Australian Capital Territory.

These health privacy regimes have many similarities to the APPs, but go further in some areas including deceased individuals, information access procedures, retention periods and additional requirements for health service providers.

Australia's e-health records system also includes specific privacy requirements.

A number of health-related privacy guidelines have also been published by regulators, including in relation to medical research and genetic information.

Surveillance

Surveillance devices laws

All states and territories have some form of surveillance devices legislation. These laws generally prohibit certain uses of surveillance devices and information obtained using surveillance devices, with some exceptions for law enforcement. Depending on the jurisdiction, these laws may regulate optical surveillance devices (e.g. cameras), listening devices (e.g. microphones), location-tracking devices (e.g. GPS) and data surveillance devices.

The Australian Law Reform Commission has recommended the introduction of national surveillance devices laws to replace the existing state and territory laws, including in relation to

workplace surveillance.

Workplace surveillance

Specific workplace privacy legislation exists in New South Wales and the Australian Capital Territory. Those laws regulate overt and covert camera, computer and tracking surveillance, including:

- requirements to provide employees with 14 days' notice (unless otherwise agreed) of an intention to commence surveillance;
- provision for covert surveillance by order of a Magistrate where unlawful employee conduct is reasonably suspected; and
- prohibition of surveillance in change rooms, bathrooms and toilets (Victoria also has similar requirements to this).

Telecommunications interception and listening devices

With respect to telephone communications, the federal *Telecommunications (Interception and Access) Act 1979* (Cth) prohibits listening to or recording communications passing over a telecommunications system without the consent or knowledge of the parties to the communication.

Listening and surveillance devices legislation in each state generally prohibits the use of a listening device to listen to or record private conversations to which the user is not a party without the consent of all parties.

Spent convictions

All Australian jurisdictions except Victoria have 'spent convictions' laws which limit the use and disclosure of information about old minor criminal convictions.

Tort of privacy

Consistent with a general trend in common law countries, including the UK and New Zealand, there appears to be some movement in Australian courts towards recognising new rights to recover damages to for invasions of privacy generally, separate from statutory remedies for

inappropriate dealing with personal information.

The federal government is considering legislating in this area, having released a law reform report in 2014 proposing either a new right to sue for serious invasions of privacy, or a new tort of harassment coupled with an extension of breach of confidence to cover emotional distress. A NSW law reform report in 2016 has also recommended introducing a right to sue for serious invasions of privacy.

Consumer protection

The Australian Consumer Law prohibits certain misrepresentations and misleading and deceptive conduct in trade or commerce in Australia. This can be relevant to the content of privacy policies and statements, which sometimes over-commit companies by promising to meet privacy standards which exceed legal requirements and are difficult to maintain.

Enforcement

The OAIC investigates complaints from individuals about interferences with privacy that are contrary to the Privacy Act. The OAIC also has the power to initiate own motion investigations about potential breaches of privacy that do not relate to a particular complainant.

Following its investigation, the OAIC has the power to make a determination ordering compensation and reparatory action, among other things, which is enforceable in the Federal Court or Federal Magistrates Court.

Certain breaches of the Privacy Act, Spam Act or *Do Not Call Register Act 2006* (Cth) can result in fines of up to AU$2.1 million. Regulators can also agree enforceable undertakings with entities that breach these Acts.

In some jurisdictions, contravening privacy legislation can result in the imposition of fines or imprisonment. For example, a breach of the *Surveillance Devices Act 1999* (Vic) can result in imprisonment of up to two years or the imposition of substantial fines..

Last updated: 01/03/2019

Key contacts

Kaman Tsoi
Special Counsel
+61 3 9288 1336
Melbourne
kaman.tsoi@hsf.com