Comman Law

For a community or society to work, it needs to have a level of structure that applies to everyone and is understood by everyone.

Laws create that structure and regulate the way in which people, organisations and governments behave.

A law is a rule that comes from a legitimate authority and applies to everyone. Laws are created to make sure that everyone understands what is expected of them as a member of society (their obligations) and what they can expect of others, including government (their rights).

Why do we have laws?

We have laws so that society can work effectively, to make sure that people or organisations are not able to use power, money or strength to take advantage of others or to make things better for themselves. We have laws to make sure that everyone understands their rights and obligations, and the rights and obligations of others.

What is a 'legal system'?

All countries have a legal system of some sort. The ‘legal system’ is a broad term that describes the laws we have, the process for making those laws, and the processes for making sure the laws are followed. Our legal system reflects how we, as Australians, behave and how we as a country expect people, organisations and governments to behave towards each other.

Where does the Australian legal system come from?

The Australian legal system developed from the legal system of Britain, which was brought to Australia as part of the process of Britain setting up a colony in Australia, beginning in the 1770s. Between 1855 and 1890 the British Parliament granted a limited right to set up a local system of government to each of the British colonies within Australia, usually referred to as granting ‘responsible government’. As each of the colonies was granted this right it was able to develop its own laws and legal systems to deal with its particular situation. So, the law and legal system in each of the colonies began to develop separately.

During the late 19th century, there was a move towards creating a central government for the whole of the country. Representatives of the six colonies (New South Wales, Queensland, South Australia, Tasmania, Victoria and Western Australia) met at a series of conventions held in the 1890s, to work on the wording of a constitution. A referendum was held in each colony to approve the draft constitution. The Australian Constitution was passed as an Act of the British Parliament, and took effect on 1 January 1901. The creation of the Australian Constitution in 1901 was the beginning of an independent Australian legal system that forms part of the system of government of Australia.

The Commonwealth of Australia was formed by the federation of the independent colonies (which then became states). This is why we refer to the establishment of the Commonwealth as ‘federation’ and our system of government in Australia as a ‘federal’ system. Under a federal system of government, power is divided between the federal government and the component state/territory governments.

The way in which the power is divided is set out in the Commonwealth of Australia Constitution Act 1900 (UK) (the Constitution). Section 51 of the Constitution lists what powers the federal government

will have. State and territory governments have power over anything else within their borders, that is, anything that isn't mentioned in section 51.[1]The Constitution is structured this way because the states came together to create the Commonwealth and they agreed amongst themselves what powers the Commonwealth they were creating could exercise and which powers they would keep.

Some of those areas contained in section 51 are: defence;

- external affairs;
- interstate and international trade;
- marriage and divorce;
- taxation;
- corporations;
- immigration; and
- bankruptcy.

This means that since Federation, all Australians have been subject to the laws of two legal systems: federal laws, and the laws of the state or territory in which they live.

HOT TIP –WHAT IS A CONSTITUTION?

A constitution is a set of rules that sets out how an organisation or country is to be run (governed), how the organisation or country decides who will have power, how that power can be exercised. The constitution of a country sets up the system of government for that country. The full title of Australia's Constitution is the Commonwealth of Australia Constitution Act 1900.

How laws are made

In the Australian legal system the main ways that laws are made are by:

- parliaments passing Acts known as 'statute law';
- the executive developing 'delegated legislation', which is, regulations, rules, ordinances etc, under the authority of parliament and statute law; and
- courts interpreting the law, and deciding cases on the basis of how similar cases have been decided in the past and applying those decisions to the circumstances of the case they are currently deciding, known as 'common law'.

Who is in the australian legal system?

We are all involved in the Australian legal system because it regulates what we may and may not do as members of the Australian community and because we elect those who make the laws:

- Commonwealth government – laws are passed by the Commonwealth Parliament, elected by all Australian citizens who are enrolled to vote.
- State/territory government – laws are passed by the state or territory parliament, elected by those Australian citizens who live in that state or territory who are enrolled to vote.
- Local government – local government by-laws are passed by the local councillors elected by people who live or own businesses within the local government area.

There are, however, some people and organisations that are at the heart of the legal system:

- the federal, state and territory parliaments;
- courts and tribunals;
- government departments;
- government ministers;
- police; and
- lawyers.

Each has a slightly separate role to play in the legal system and these are described further on in this Hot Topics.

HOT TIP – THE 'RULE OF LAW'

Australia's system of government is based on the rule of law. This means that everyone has to obey the law; that no-one, no matter how important or powerful, is above the law. This means that the law applies not only to citizens but also to organisations and to people in government including the Prime Minister, the heads of government departments, and members of the armed forces. So, the same law that makes it a criminal offence to steal someone's property applies to everyone. Another aspect of the rule of law is that no-one is allowed to exercise powers except those powers given to them by law.

1. There are some situations where state and territory governments agree to give specific powers back to the Commonwealth, such as the referral of certain powers by Queensland, New South Wales, Victoria and South Australia to the Commonwealth to enable the passing of the Water Amendment Act 2008, which amended the Water Act 2007, creating a single body responsible for overseeing water resource planning in the Murray-Darling Basin.

Overview of Privacy Law in Australia

The handling of personal information in Australia is governed by legislation at both a federal and state/territory level.

At a federal level, the Privacy Act 1988 (Cth) (Privacy Act) governs the way in which business entities and federal government agencies must handle personal information, largely through the 13 Australian Privacy Principles (APPs) set out within the Privacy Act.

'Personal information' is defined by the Privacy Act as:

information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

State and territory government agencies must comply with the relevant state or territory based privacy legislation.

Entities handling personal information in Australia must also be aware of their obligations under:

- health records legislation (in Victoria, New South Wales and the Australian Capital Territory) (further explained in section 12 below)

- state and federal surveillance legislation (further explained in section 13 below), which governs the way in which individuals can and cannot be monitored through video surveillance, geographical tracking, data/computer surveillance and/or listening devices (including, in some jurisdictions, within the workplace) and

- federal legislation that governs email marketing and telemarketing, such as the Spam Act 2003 (Cth) and Do Not Call Register Act 2006 (Cth).

Who must comply with the Privacy Act?

The Privacy Act imposes obligations on 'APP entities'.

An APP entity is, generally speaking:

- an agency (which largely refers to a federal government entity and/or office holder) or

- an organisation (which includes an individual, body corporate, partnership, unincorporated association, or trust).

An APP entity does not include:

- a 'small business operator' (subject to the exceptions below), which is an operator of a business with an annual turnover of less than $3 million

- a registered political party or

- a state or territory authority.

However, a small business operator will be deemed to be an APP entity, and therefore required to comply with the Privacy Act if they:

- operate another business with a turnover of $3 million or more

- provide a health service or otherwise hold health information (other than in an employee record)

- disclose, or collect, personal information about another individual for a benefit, service or advantage

- are a contracted service provider for a Commonwealth contract or

- are a credit reporting body.

Obligations under the Privacy Act

The key features of the Privacy Act include:

- the 13 APPs which are the principles that govern the way in which personal information is to be collected, used, disclosed and stored. We have included a summary of the APPs in section 4 below. The full text of the APPs can be viewed on the Australian Information Commisioner's website.

- the credit reporting provisions of the Privacy Act (further explained in section 10 below), which govern the way in which credit-related personal information is to be collected, used, disclosed and stored. These provisions will be particularly relevant to entities that are credit providers (or agents of credit providers), credit reporting bodies, or that otherwise handle or deal in credit-related personal information and

- the obligation to comply with an 'APP code', which is a written code of practice usually specific to a particular entity or industry. In particular, there is a Credit Reporting Code (CR Code) which imposes on entities handing credit information additional obligations to those set out in the credit reporting provisions of the Privacy Act.

Accordingly, APP entities must be aware of the full scope of the obligations imposed upon them according to the nature of their business activities.

The Australian Privacy Principles

APP 1: Open and transparent management of personal information

APP 1 requires an APP entity to implement privacy practices, procedures and systems:

- to ensure compliance with the remaining APPs and

- that enable them to deal with inquiries and complaints.

It also requires them to develop and make readily available a policy about its management of personal information.

APP 2: Anonymity and pseudonymity

APP 2 entitles individuals to the option of anonymity or using a pseudonym, when dealing with an APP entity, except where impracticable or another prescribed exception applies.

APP 3: Collection of solicited personal information

APP 3, in summary:

- permits an APP entity to collect personal information only where reasonably necessary for one or more of its legitimate functions or activities

- requires personal information to be collected directly from the individual to whom it relates, unless impracticable or another prescribed exception applies and

- requires the consent from an individual in order to collect that individual's sensitive information, or another prescribed exception applies.

APP 4: Dealing with unsolicited personal information

APP 4 requires an APP entity that receives unsolicited personal information to determine whether it would otherwise have had grounds on which to collect it (i.e. under APP 3) and:

- where it does have such grounds, to ensure compliance with the remaining APPs or

- where it does not have such grounds, to destroy or de-identify the personal information (provided it is lawful and reasonable to do so).

APP 5: Notification of the collection of personal information

APP 5 requires an APP entity to notify an individual (or ensure they are aware), at or before the time of collection, of prescribed matters. Such matters include but are not limited to whether the individual's personal information is collected from any third parties, the purpose (s) of collection, to whom personal information is disclosed and the processes through which an individual can seek access and/or correction to their personal information, or otherwise complain about the way in which it is handled.

Compliance with APP 5 usually requires 'collection statements' to be included on or with forms, or other materials, through which personal information is collected. Such statements should refer and include a link to the APP entity's privacy policy.

APP 6: Use or disclosure of personal information

APP 6 prohibits an APP entity from using or disclosing personal information for a purpose other than the purpose for which it was collected, unless the individual consents, the individual would reasonably expect their personal information to be used for the secondary purpose, or another prescribed exception applies.

Such prescribed exceptions generally arise where the disclosure is necessary to protect someone's health or safety or is otherwise in the public interest.

APP 7: Direct marketing

APP 7 generally prohibits personal information to be used for direct marketing purposes unless the individual reasonably expects it, or consents to it, and prescribed 'opt out' processes are in place through which the individual can elect not to receive direct marketing communications (and the individual has not elected as such).

APP 8: Cross-border disclosure of personal information

If an APP entity is to disclose personal information to an overseas recipient, APP 8 requires it to take reasonable steps to ensure the recipient does not breach the APPs. This usually requires the APP entity to impose contractual obligations on the recipient.

Relevantly, if the overseas recipient does breach the APPs, the Privacy Act imposes liability on the APP entity that made the overseas disclosure.

There are exceptions to this obligation, including but not limited to where:

- the APP entity reasonably believes the overseas recipient is bound by a law or scheme that protects personal information in a substantially similar way to that of the APPs or

- the individual consents to the disclosure in the knowledge that such consent will negate the APP entity's obligation to ensure the overseas recipient does not breach the APPs.

APP 9: Adoption, use or disclosure of government related identifiers

APP 9 prohibits an APP entity from adopting, using or disclosing a government-related identifier unless:

- required or authorised by law

- necessary to verify an individual's identity and/or
- another prescribed exception applies.

Government-related identifiers are identifiers that have been assigned by a government agency including an individual's licence number, Medicare number, passport number and tax file number.

APP 10: Quality of personal information

APP 10 requires an APP entity to take reasonable steps to ensure personal information it collects, uses, discloses and holds is accurate, up-to-date and complete. Additionally, personal information can only be used or disclosed to the extent to which it is relevant to the purpose of the use or disclosure.

APP 11: Security of personal information

APP 11 requires an APP entity to take reasonable steps to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure.

An APP entity must also destroy or de-identify personal information it no longer requires (unless otherwise required to retain it by law).

APP 12: Access to personal information

APP 12 requires an APP entity to provide an individual, upon request, with access to their personal information unless a prescribed exception applies.

APP 13: Correction of personal information

APP 13 requires an APP entity to take reasonable steps to correct personal information it holds upon request from an individual for correction or where it is otherwise satisfied, having regard to the purpose for which it holds the personal information, that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If an APP entity refuses a request for correction, it needs to provide the individual with the reasons for the refusal and may be required to associate with the personal information a statement evidencing the individual's view that the information is incorrect.

Where correction does occur, the APP entity may need to notify third parties to which the personal information, in its incorrect form, was disclosed.

Sensitive information

The Privacy Act generally affords a higher level of protection to 'sensitive information' given the mishandling of it can generally have a more detrimental impact on the relevant individual.

'Sensitive information' is defined under the Privacy Act and includes information about an individual's racial or ethnic origin, political opinions, professional or political or religious affiliations or memberships, sexual orientation or practices, criminal record, health, genetics and/or biometrics.

As an example, APP 3, which deals with the collection of solicited personal information, prohibits (with some exceptions) the collection of sensitive information unless the individual to whom it relates consents to the collection and the information is reasonably necessary for the collecting entity's functions or activities.

The collection of non-sensitive information is otherwise generally permitted where it is reasonably necessary for the collecting entity's legitimate functions or activities.

Extra-territorial application of the Privacy Act

An entity operating outside Australia will still have obligations under the Privacy Act if the entity has 'an Australian link'. An entity will have an Australian link for the purposes of the Privacy Act if, generally speaking, the entity was formed in Australia, has its central management and control in Australia, or is otherwise carrying on a business and collects or holds personal information in Australia.

This expands the reach of the Privacy Act to overseas entities, or Australian subsidiaries of overseas entities, who are engaging in business-related acts within Australia, even if the business is otherwise predominantly conducted outside of Australia.

The Australian Information Commissioner has also pointed to specific indicators that an entity is carrying on a business within Australia, including where an entity has an agent or agents within Australia, websites offering goods or services to Australia, purchase orders being actioned within Australia, or personal information being collected from a person who is physically in Australia.

Penalties for breaching the Privacy Act

If an APP entity is found to have engaged in a serious, or repeated, interference with an individual's privacy, the APP entity may face penalties of up to:

- $1.8 million for corporate bodies and/or
- $360,000 for non-corporate bodies (including government departments/agencies, sole-traders, partnerships, trusts, unincorporated associations).

An APP entity will interfere with an individual's privacy if (among other things) it:

- breaches an APP
- breaches an APP code that is binding on the relevant entity (noting that the Australian Information Commission may impose an APP code on a particular organisation or industry)
- breaches the credit reporting provisions of the Privacy Act
- breaches the CR Code
- breaches a provision of a Commonwealth contract for which it is to provide services and/or
- handles a tax file number contrary to the Tax File Rule (which has been issued by the Australian Information Commissioner pursuant to the Privacy Act).

Implications for related bodies corporate

Generally, related bodies corporate can share personal information, provided they comply with the APPs and any applicable APP code. Where personal information is disclosed from one related body corporate to another, the Privacy Act requires the personal information to be handled (by the related body corporate to which it is disclosed) in accordance with the purpose for which it was initially collected (by the related body corporate from which it is disclosed).

Exempt acts: the employee records exemptions

Employee information is, generally speaking, excluded from the ambit of the Privacy Act.

Specifically, where an employer engages in an act or a practice that is directly related to:

- a current or former employment relationship between the employer and an individual and
- an 'employee record' held by the employer relating to the individual
- the act or practice will not be covered by, and therefore need not comply with, the Privacy Act.

An 'employee record' refers to a record of personal information relating to the employment of the employee. This includes, but is not limited to, health information about the employee and/or personal information about, discipline, resignation, termination, terms of employment, personal contact details, wages or salary, performance or conduct, periods of leave and/or memberships of professional bodies.

Accordingly, employers need not comply with the Privacy Act and the APPs to the extent they are dealing with an employee record in a manner that is directly related the employment relationship.

This does not mean, however, that employers can handle personal information about its employees with general disregard. Where the personal information does not fall within the employee records exemption (i.e. the personal information is not an employee record and the employer's act or practice is unrelated to the employment relationship), compliance with the Privacy Act will be required.

Specifically, compliance with the Privacy Act is required with respect to:

- personal information about prospective employees (unless and until they are employed by the employer)
- personal information about contractors, company officers, volunteers and/or work experience students and/or
- personal information contained in, and obtained from, personal emails or other IT/phone use, which does not directly relate to the employee's employment.

Additionally, employee information is likely to be subject to common law obligations of confidentiality and, in some states, health records legislation.

The employee records exemption has also been marked for possible repeal in the future, which would result in employers having to handle employee information in accordance with the Privacy Act.

Credit reporting provisions and the CR Code

The credit reporting provisions of the Privacy Act and the CR Code set out the ways in which entities are to handle credit-related personal information.

The credit reporting provisions of the Privacy Act are long and complex and impose obligations and prohibitions on credit reporting bodies and credit providers (and agents of credit providers).

An entity captured by the credit reporting provisions is required to take steps (often in addition to those set out in the APPs) to ensure compliance with the Privacy Act. Such obligations include, in some circumstances, acting with the express consent of the individual to whom the information relates. Additionally, specific obligations will depend on the type of information being handled. For example, a

credit provider can only access and use information about an individual's history of debt repayments if the credit provider is a 'licensee' under the National Consumer Credit Protection Act 2009 (Cth).

Mandatory breach notifications

On or before 22 February 2018, APP entities will also be required to notify the Australian Information Commissioner, and affected individuals, if the APP entity experiences a data breach that is likely to cause an individual serious harm. This obligation is designed to enable affected individuals to take steps to protect themselves.

Handling health information

The Privacy Act includes health information within its definition of 'sensitive information'. Health information is therefore afforded a higher standard of protection.

Additionally, both private and public sector entities need to be aware of obligations that may arise under state-based legislation, including:

- Health Records and Information Privacy Act 2002 (NSW)
- Health Records Act 2001 (Vic) and
- Health Records (Privacy and Access) Act 1997 (ACT).

These laws also impose obligations on employers in Victoria and the ACT when handling health information about their employees. While health records law in NSW contains an employee records exemption for private sector employers, such employers may nevertheless be bound by the NSW legislation if the health information is unrelated to their employment.

Health and other sensitive information will also be subject to common law principles of confidentiality.

Surveillance

The use of surveillance and/or listening devices is governed by both state/territory and federal legislation. Obligations in relation to surveillance will depend on the type of device (e.g. computer and/or video surveillance, geographical tracking and/or the use of listening devices), the nature and purpose of the surveillance, the specific activity being observed/recorded including whether it is occurring in the workplace or not and, in some cases, whether it occurs in the private or public sector.

While each jurisdiction differs, generally speaking, the use of surveillance and/or listening often requires consent and/or notification. However, exceptions may apply, including where the use of such a device is necessary to protect a party's lawful interests, for an enforcement-related purpose, and/or is in the public interest. Specific obligations may also be impacted by whether the person using the surveillance or listening device is a party to the activity/conversation and whether the activity/conversation is private or in a private space.

Hall & Wilcox is well placed to advise on privacy law compliance and any other issues arising from the handling of personal information.

Tags: app, Do Not Call Register Act, Health Records (Privacy and Access) Act, Health Records Act, Health Records and Information Privacy Act, National Consumer Credit Protection Act, privacy act, Spam Act, surveillance