Table of Contents

Week 1 – Introduction

Introduction

When did privacy emerge?

- The concept of privacy is relatively recent, emerged during the 19th century and generally developed in parallel with (or in response to) technological advancement. Cameras, newspapers, early computers…
- Early formulations of privacy were around the value of 'private life' and the 'general right of the individual to be let alone'.
- Warren and Brandeis article:
    - Concerned newspaper coverage of well-known people.
    - Discussed *Prince Albert v Strange* (High Court of Chancery, 1849)
    - Formally recognised a right to privacy based on a "right to be let alone".
- But privacy not recognised by High Court: *Victoria Park Racing & Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479*:
    - 'However desirable some limitation upon invasions of privacy might be, no authority was cited which shows that any general right of privacy exists' *[Latham CJ, 496]*.

Privacy = "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" *(Alan Westin Privacy and Freedom 1967, 7)*.
This is basically a right to control self-disclosure.

- Theorists have focused on privacy as an essential component of democracy, of individuals' ability to develop social relationships, engage in intimacy, operate in a democracy, exercise self-determination over personal information and/or sustain a 'personal space'.
- *Daniel Solove*: taxonomy of privacy, no overarching clear definition, problem with this approach is that it doesn't let us add new categories of privacies or to even understand what is worth protecting about privacy. This theory is now no longer relevant.
- *Richards (see reading)*: 'Privacy is the degree to which human information is neither known nor used.'

Key Issues:

- Is privacy about control of information? Westin would say yes, others disagree.
- Is it about secrecy, such that once the information is public it no longer needs protection? Richards would say no.
- Can the boundaries of privacy be easily described? Most academics would say no, and the *Solove taxonomy approach is fading*.

- Is privacy a personal thing, or is it central to civic life and social freedom? The more authoritarian a government is the less it respects privacy.
- What is the relationship between privacy and technology? It seems that privacy concerns are generally closely tied to technological developments.

The "Privacy Is Dead" Myth

- A widespread public narrative claims that privacy no longer exists due to pervasive data collection by governments, corporations, schools, advertisers, and private individuals.
- Statements like "you have zero privacy, get over it" and "privacy is no longer a social norm" reflect a fatalistic belief that the loss of privacy is inevitable.
- Richards argues this myth benefits those who profit from surveillance—tech companies and governments—and disempowers the public.

Privacy Is Not Dead – It Is Contested

- Although our information flows widely, most information still exists in intermediate states between "totally private" and "completely public".
- We still maintain basic privacy practices: locking doors, keeping secrets, choosing who to share confidential information with.
- The real issue isn't disappearance of privacy but the struggle for control over human information.

Privacy as Social Power

- Information = power in a digital society.
- Privacy debates are fundamentally about who controls information flows, who benefits from them, and how this redistributes power across society.
- Companies framing data as "the new oil" reinforce the idea that data extraction is inevitable and socially necessary—but this framing hides the need for regulatory controls analogous to pollution laws, safety standards, and climate protections.

Instrumental Values of Privacy (Richards)

Richards claims privacy is not an end in itself, but an instrumental value that protects human flourishing. It supports three essential social functions:

(a) Identity Formation

- Privacy gives individuals the space to develop political, personal, and social identities without surveillance pressure.
- Identity "play" and exploration—sometimes contradictory—is a normal part of humanity, not deception.
- Surveillance can distort or inhibit personal development.

(b) Democratic Freedom

- Privacy prevents excessive state surveillance that undermines political liberty, democratic processes, and separation of powers.

- Bulk surveillance can actually make societies less safe by diverting resources and creating risks of political manipulation (e.g., blackmailing officials, election interference).

(c) Consumer & Worker Protection

- In an information economy, privacy rules determine whether individuals can resist:
    - data-driven persuasion
    - discriminatory profiling
    - manipulative advertising
    - intrusive employer monitoring
- Without privacy, individuals cannot make autonomous or rational choices.
- Privacy rules also create trust in relationships with digital intermediaries (Google, social platforms, ISPs).

What does privacy cover?

Solove: Privacy = 'concept in disarray', focused on taxonomy instead.

Are concepts of privacy universal, or culturally dependent?

- USA: freedom from government, autonomy and liberty
- EU: about human rights, primarily rights to respect and dignity in community
- Australia: somewhere in between?
- Japan (see Youtube): protective of personal privacy
- Overall, some core elements are universal, but details are culturally dependent.

- What is the overlap with confidentiality? Does privacy still apply to information which has been shared?
    - Simply disclosing personal information does not reduce its protection going forward.

Personal information = broadly defined as information that can be used to identify a person.

Bodily privacy = you have rights over your body, this includes freedom from unwanted touching and what apply to deepfakes, including parts in person's body.

Spatial privacy = concerned with your location and whether you can be tracked. Surveillance would violate this, including if someone were to place a tracker on your car or in your bag, or track your phone signal without your consent.

Communication or privacy = who are you talking to and what are you saying? This would be engaged by phone tapping or other surveillance of your communications.

Proprietary privacy = this relates to information you own, such as trade secrets or confidential information.

Privacy as "Rules for Human Information"

- Privacy is not simply secrecy, nor individual control; it is best understood as rules that govern detection, collection, use, storage, and sharing of human information.
- Information can remain "private" even after disclosure, depending on the rules and obligations applied to the recipient (e.g., confidentiality, privacy policies).

- Privacy rules determine how data is allowed to shape or influence our lives.

Privacy as a Foundation of Trust

- Many modern relationships depend on sensitive information flows: intimate partners, doctors, and digital service providers.
- Trust cannot exist without meaningful privacy rules.
- A functioning digital society requires privacy protections that maintain trust in intermediaries.

Privacy in international treaties

- The first inclusion of privacy in international law was in the *1948 Universal Declaration of Human Rights ('UNDR'), article 12*: - not legally binding, it is a declaration

"No-one shall be subject to arbitrary interference with his privacy, family, home or correspondence… Everyone has the right to the protection of the law against such interference…."

- In *1966, the International Covenant on Civil and Political Rights* was developed as a treaty based on the UNDR, Australia ratified it. Article 17 included same wording as article 12 UNDR. -> this is a binding treaty. From 1980 Article 17 required Australian government to offer a legal protection for privacy.

- This set the scene for Australian privacy legislation, which we will discuss next week.

Privacy at common law

- While privacy is recognised as a human right under legislation, it is not clearly or uniformly recognised by Australian courts as a common law right.

- *Victoria Park Racing & Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479*: A neighbour built a high platform on his property overlooking a Sydney racecourse, facilitating live radio broadcasts from the platform. Racecourse argued this caused them economic harm.

- Argument unsuccessful. High Court held that looking over a fence and describing it was not a nuisance or an infringement of property rights and did not recognise a general right to privacy.

- *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199*: Possum processing facility in Tasmania, animal rights activists secretly trespassed and filmed activities inside the facility and supplied it to the ABC for broadcast. Lenah sought an injunction to stop publication.

- *Lenah* cont'd: HCA held that **corporations do not have a right to privacy**. The Court did not recognise a new tort of privacy (considering this the "wrong vehicle" given the plaintiff was a corporation) but **left the door open** for Australian courts to develop such a tort in the future.

- Callinan J: 'time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country' [335].

Further development at State level:

- *Grosse v Purvis [2003] QDC 151*: heard by the District Court of Queensland (concerned stalking by an ex-partner). Senior Judge Skoien held that a tort of invasion of privacy does exist in Australia – awarded $178K.
- *Jane Doe v Australian Broadcasting Corporation [2007] VCC 281*: ABC negligently disclosed victim of rape. Criminal case, then civil case. County Court: plaintiff succeeded, the ABC had invaded the plaintiff's privacy by unjustifiably publishing personal information that the plaintiff had a reasonable expectation would remain clearly private-- "actionable wrong which gives rise to a right to recover damages according to the ordinary principles governing damages in tort" [157].

Week 2 – Data Protection

Privacy vs Data protection

- Data protection has some overlap with privacy but really focuses on the need to process personal data and protections from any resulting harms.
- Data protection has a multi-decade history in Europe where it is an established field of law and policy but is less central to Australian legal practice.
- Data protection theories arose from significant developments in the field of personal information processing, which triggered fears not adequately addressed by other laws.
- Some countries' data protection emerged from legal foundations distinct from privacy, such as information self-determination (Germany), protection of liberty (France), and fair information practices (the United States).
- Data protection law is also concerned with elements of data quality— such as the integrity and availability of data — which are not privacy issues.

Transparency vs Opacity

- *De Hert & Gutwirth*: compare 'transparent', procedural role of data protection with more 'opaque' protection offered by privacy laws (secrecy [provisions, provisions on surveillance).
  - Transparent protection = data can be used but must be used appropriately
  - Opaque protection = data cannot be used at all
- *De Hert & Gutwirth*: consider that the purpose of data protection laws is ***not to prohibit but to allow access***, with commensurate protection. Personal information can be legitimately processed and shared provided that certain requirements and protections are applied.
- *Bygrave*: 'data privacy legislation tends to operate with largely procedural rules that avoid fundamentally challenging the bulk of established patterns of information use. In the language of road signs, it usually posts the warning "Proceed with Care!"; it rarely orders "Stop!"'. *Lee A Bygrave, Data Privacy Law: An International Perspective (Oxford University Press, 2014) 122.*
- Data protection is most often a creature of statute or negotiated frameworks such as the 1980 *OECD Guidelines*, which we will discuss next.

1980 OECD Guidelines

- First international instrument addressing data protection: non-binding 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data* ('OECD Guidelines').
- Australian Michael Kirby (Chairman of ALRC, later a High Court judge) led the drafting process.
- Guidelines prompted by fear of barriers, desire to preserve international commerce.

- Tensions: Europe conscious of WWII, Cold War, Holocaust. America interested in commerce, free speech. Difficult to reach agreement, hence the high-level nature of the Guidelines.
- Guidelines: 8 principles, technology neutral, flexible implementation.
- Remarkably, still very relevant to data protection law today.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or
b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Impact of OECD Guidelines

- The OECD Guidelines laid the foundation for data protection legislation in many countries.
- Their language and approach (including the use of principles) has stood the test of time.
- Greenleaf regards the OECD Guidelines principles as offering 'the best guide to the minimum requirements of a data privacy law'.
- In Australia, government agreed to adhere to the OECD Guidelines (1984).
- ALRC report on privacy (1983) recommended legislation for public sector including unforceable OECD-style principles → Privacy Bill 1986.
- Australia card furore → led to *Privacy Act 1988* (Cth) containing enforceable principles based on OECD principles and also implement art 17 of *ICCPR*. So, the Australia Card strengthened the nation's privacy framework but due to so much dissent from the public it was abolished and the TFN was instead established.

The Privacy Act 1988 (Cth)

- Stronger privacy legislation than originally proposed, OECD Guidelines.

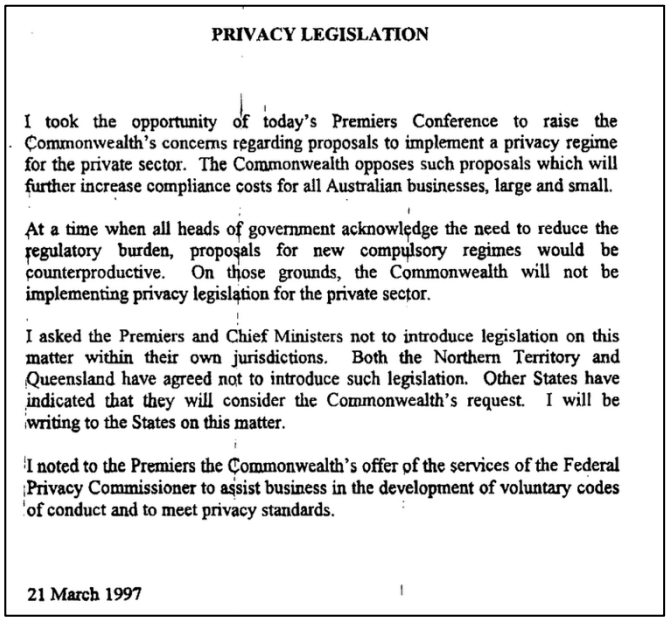
- A key term: 'personal information' (s 6): information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Definition was amended in 2014
- Legislative framework for information privacy at the federal level, covering the data activities of 'APP entities' — federal public sector agencies as well as organisations with annual turnover exceeding $3 million- *Margaret Allars, 'Automated Decision-Making and Review of Administrative Decisions' (2024) 58* Georgia Law Review *1145.*
-

Identifying what personal information means:

- It contributes to identifying an individual.
- "Identity is apparent"-- examples include name, address, phone number, photo, driver licence number, fingerprint. Clearly personal information.
- "Reasonably be ascertained" – trickier. Age? Date of birth? Gender? Nationality?

The Act contains 11 Information Privacy Principles modelled on the OECD Guidelines. Some key protections:

- Collection and purpose limitation: collection for appropriate purpose, collection notice
- Use and disclosure limitations: for primary purpose of collection, or in limited other cases (eg customer consent, law enforcement, emergency)
- Openness and transparency: open practices,
- Data quality and security: data to be kept up to date and secure (reasonable steps to ensure security).
- The original Privacy Act only applied to the public sector and so do all the State and Territory Acts. What about the private sector?



PRIVACY LEGISLATION

I took the opportunity of today's Premiers Conference to raise the Commonwealth's concerns regarding proposals to implement a privacy regime for the private sector. The Commonwealth opposes such proposals which will further increase compliance costs for all Australian businesses, large and small.

At a time when all heads of government acknowledge the need to reduce the regulatory burden, proposals for new compulsory regimes would be counterproductive. On those grounds, the Commonwealth will not be implementing privacy legislation for the private sector.

I asked the Premiers and Chief Ministers not to introduce legislation on this matter within their own jurisdictions. Both the Northern Territory and Queensland have agreed not to introduce such legislation. Other States have indicated that they will consider the Commonwealth's request. I will be writing to the States on this matter.

I noted to the Premiers the Commonwealth's offer of the services of the Federal Privacy Commissioner to assist business in the development of voluntary codes of conduct and to meet privacy standards.

21 March 1997

Privacy Act and the private sector

- Privacy Act extended to the private sector in 2001 under the *Privacy Amendment (Private Sector) Act* 2000, which applied National Privacy Principles (NPPs) instead of IPPs.
- Exempt: small businesses and not-for-profit organizations with an annual turnover of $3 million or less.
- Major reform in 2014 unified the legislation, applying the Australian Privacy Principles (APPs) to public and private sector.
- That reform also updated the definition of 'personal information' and attempted to modernise the legislation in response to a 2008 ALRC report.
- We have also had a more recent review, the Privacy Act Review, which we will discuss next week. This led to 2024 amendment legislation, with potentially more to come.

Objects of Privacy Act

Objects were added in the 2014 amendments (s 2A).

2A Objects of this Act

The objects of this Act are:

(a) to promote the protection of the privacy of individuals; and

(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities; and

(c) to provide the basis for nationally consistent regulation of privacy and the handling of personal information; and

(d) to promote responsible and transparent handling of personal information by entities; and

(e) to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected; and

(f) to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected; and

(g) to provide a means for individuals to complain about an alleged interference with their privacy; and

(h) to implement Australia's international obligation in relation to privacy.

Australian Privacy Principles (APPs), summarised

APP	Focus	Key Compliance Obligations	Common Pitfalls
1	Open and transparent management	Maintain and publish a current privacy policy; integrate privacy into governance	Outdated policy; policy not accessible or overly complex
2	Anonymity & pseudonymity	Offer non-identifying options where lawful/practicable	Requiring ID unnecessarily
3	Collection of solicited info	Only collect what's necessary; collect by lawful/fair means; consent for sensitive info	Over-collection "just in case"
4	Unsolicited info	Assess if you could have lawfully collected it; destroy/de-identify if not needed	Storing irrelevant unsolicited resumes
5	Notification	Inform individuals at collection about purpose, disclosure, rights	Missing or hidden collection notices
6	*Use/disclosure*	*Use for primary purpose or with consent; exceptions for related purposes*	*Secondary use without consent*
7	Direct marketing	Use only with consent or clear opt-out; comply with Spam Act/Do Not Call Register	Failing to offer opt-out
8	Cross-border disclosure	Ensure overseas recipients handle info per APPs or equivalent law	Sending data offshore without safeguards
9	Gov. identifiers	Don't adopt government IDs as your own unless allowed	Using Medicare number as customer ID
10	Quality of info	Take steps to ensure accuracy, completeness, and relevance	Not verifying data before use
11	Security	Protect from misuse, loss, unauthorised access; destroy/de-identify when no longer needed	Storing unencrypted data indefinitely
12	Access	Provide access on request unless exception applies	Refusing without valid reason
13	Correction	Correct info to ensure accuracy and completeness	Ignoring correction requests

Privacy legislation at State level

- NSW public sector: *Privacy and Personal Information Protection Act 1998*
- Victorian public sector: *Information Privacy Act 2000* (now replaced: *Privacy & Data Protection Act 2014* (Vic))
- Qld: *Information Privacy Act 2009* (now replaced: *Information Privacy and Other Legislation Amendment Act 2023* (Qld))
- WA: *Privacy and Responsible Information Sharing Act 2024* – **new!** Covers data sharing also.
- *Information Act 2002* (NT); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2014* (ACT). (SA has a cabinet instruction but no legislation)
- All are based on OECD Guidelines; all State legislation applies only to public sectors.

Health records legislation

- Some states have data protection legislation focused on personal medical information. Eg *Health Records Act 2001* (Vic), *Health Records and Information Privacy Act 2002* (NSW), *Health Records (Privacy and Access) Act* 1997 (ACT).
- Protect 'health information', broadly (see s 3(1) Vic Act): …information or an opinion about the physical, mental or psychological health (at any time) of an individual; disability; expressed wishes about future provision of health services; a health service… that is personal information. Includes organ donor information and genetic information.
- Operates similarly to regular data protection legislation, but with this clear coverage of medical records.

Impact of OECD Guidelines on Australian Privacy Principles

OECD Guidelines Principle	Requirement	Cth APP	Vic IPP	ACT TPP	QPP
Collection Limitation	Applies limits to personal data collection, minimisation and lawful and fair collection; where appropriate with knowledge and consent.	3-4	1	3-4	3-4
Data Quality	Data is to be relevant, complete, accurate and up to date.	10	3, 6	10	10
Purpose Specification	Requires notification of purposes of collection at the time and subsequent use limited to those purposes or other compatible purposes specified on each occasion where the purpose changes.	5-6	1–2	5–6	5-6