Privacy law notes:

Week 1

Where did privacy law come from?

- Early cases, beginning in 1300's – see slides (in UK, Sweden, France – most around the 1700's)
- 'The Right to Privacy' (1890) Harvard law Review 193
    - Expand breach of confidence? Thinks privacy should be its own tort
- Development of the tort of secrecy – Richard Posner

General concepts of privacy

- Intimacy
- Right to be left alone
- Limited access to the self
- Secrecy
- Control over personal information
- Personhood

International Covenant on Civil and Political Rights has privacy provisions

In Australia:

- No constitutional right
- No tort of invasion of privacy
- Privacy Act (Cth)

US has much more in the way of privacy law – govt is highly regulated by not much related to business. UK is very limited – but has breach of confidence and regulated business.

Week 2

US Constitution

- Aus constitution was based on this partially (also based on Westminster system)
- US const has a bill of rights which are the first 10 amendments
    - Aus dropped this out
- US has a variety of amendments in addition to the bill of rights
- 14th amendment is important (no slavery) + other reconstruction amendment
    - Procedural due process (to follow fair procedures before depriving someone of life, liberty or property)
    - Substantive due process (prohibits states from infringing on fundamental liberty interests, protects individuals from the majority – unless legitimate state interest through narrow law)
    - Lochner v New York: limited time for working in a bakery rule was ruled in violation with 14th amendment as fundamental freedom to contract.
    - West Coast Hotel Co v Parrish: overruled Lochner. Minimum wage legislation was valid even though that may have been against 14th amendment. Unfair bargaining positions.
    - This amendment is about the liberty of individuals and not the liberty of businesses

- Private sector
    - Exemption: Small business exemption, journalists, political parties
- Australian link (S5B)
    - Factors? Carries on business
        - Conducting some form of commercial enterprise to make a profit
    - APP guidelines
        - Do they have a physical office?
        - Are people undertaking business on behalf of the organisation are in Australia? Employees in Australia?
        - Whether agent is carrying on business in Australia?
        - Australian website?
        - Is Australia a country on a drop-down menu?
        - Purchase orders in Australia?
        - Is individual physically present in Australia?
            - Ashley Madison case – based in Canada but 500k Australian users → meant they were carrying on business in Australia. Marketing conducted in Australia. Targeted Australian consumers. Advertised in Australia. Had Australian user pages.
    - Is Facebook carrying in business in Australia?
        - Officially no (from KWM perspective). When you have an account, you are contracting with US Facebook. When getting ads, you are contracting with Facebook Ireland. Facebook Australia is just a 'PR company' → not running your profile or selling ads.
        - But, recognises Australian mobile number, FB has Australian trademarks, generates revenue from Aus advertisers, personnel visit Australia, Aus businesses provide services to Australia.
- Does this Act apply to individuals?
    - Individual could be a sole trader making over $3m and be regulated.
    - Reason: we can do things that breach the APPs, but this is attributed to your employer.
- Records
    - Act covers personal information held in a record –
    - S 6(1) gives broad definition of a document an electronic or other device
    - Macquarie University v FM
        - Doctoral student – Macquarie terminated him and he went to UNSW.
        - Phone conversation involved. Person from Macquarie told UNSW person about incidents that happened.
        - Information held in the minds of employees was not personal information held in a record by Macquarie.
    - UQ is established by a Qld State Act of Parliament so Privacy Act 1988 (Cth) does not apply to state entities. Relevant state privacy law will apply. Unsure why the Macquarie case came under the Cth Act.
- Complaints process:
    - 1. S 36 – complain to organisation/agency
    - 2. Complain to privacy commissioner
        - S 38 – representative complaints
        - S 40(2) – own motions investigations

- Minimum access requirements – taking three days to give record was not unreasonable (LP and the Westin Sydney)

APP 13 – Correction:

- Reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, is accurate, up to date, complete, relevant and not misleading
- Must notify third parties if data has been corrected unless impractical or unlawful.
- Refusal to correct must be given with notice and reasons.
- Reasonable period to correct
- G v Australia

Week 7:

Security & Privacy Litigations

APP 11 - Security

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Not an absolute obligation.

APP 11 - Security

Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified.

APP 11 – Core components

Six key security considerations

Misuse – used for a purpose not permitted by the Privacy Act
Interference – hacking attack that leads to unavailability (ransomware) or modification
Loss – physical or virtual
Unauthorised Access – accessed by someone (internal or external) without permission
Unauthorised Modification – altered without permission
Unauthorised Disclosure – accessible or visible to others or releases from control

OAIC Guide to Information Security

Reasonable steps to secure personal information will depend on certain contextual circumstances.

Nature of the entity holding the personal information
Amount and sensitivity of personal information held
Adverse consequences to the individuals concerned if the personal information is not secured
Practicality of implementing information security, including time and cost
Privacy invasiveness of the security measure

Sensitivity

The Office of the Australian Information Commissioner (***OAIC***) has said that entities should treat this 30-day period as the maximum time limit, particularly given that the risk of serious harm to individuals tends to increase with time. However, the OAIC also recognises that it will not always be possible to complete an assessment of a suspected data breach within 30 days, for example, if systems or records were lost during the intrusion and significant recovery effort is required.

Top tip: Where an entity cannot reasonably conduct a data breach assessment within 30 days, the OAIC recommends that an entity prepare and retain documentation that will allow it to demonstrate:

that all reasonable steps were taken to complete the assessment within 30 days;
the reasons for the delay; and
that the assessment was reasonable and expeditious.

Employee Records

Businesses will **not** be required to notify the OAIC or individuals about data breaches relating to employee records – that is, personal information of an employee relating to their employment.

The employee records exemption provided for in the *Privacy Act 1988* (Cth) applies to the Notifiable Data Breaches Scheme. See *Data breach preparation and response* guide.

Even where the employee records exemption applies, the OAIC recommends notifying individuals affected by a breach of employee records if it is likely to result in serious harm.

Think carefully about whether the information involved in a data breach is *truly* covered by the exemption.

For example, employees often use their work email accounts to receive personal emails, such as communications from their bank, which would not be covered by the exemption. In practice, it may be difficult to distinguish between what data does and does not fall within the exemption.

The employee records exemption will not extend to a data breach involving tax file numbers.

The employee records exemption only applies to an employee record held by the employer. If the organisation stores its employee records with a third party, the exemption will not extend to a data breach involving those records and the service provider will need to notify the OAIC of the breach.

Why do we have a NDB scheme?

Direct marketing (APP 7) & Spam

APP 7 – Direct marketing

APP 7.1 – May not use personal information for direct marketing.

APP 7.2 to 7.5 – Exceptions to APP 7.1.

APP 7.6 – Must allow recipients to opt out of direct marketing.

GDPR applicable to Australian businesses?
Examples: Australian businesses that may be covered by the GRPR include:
an Australian business with an office in the EU
an Australian business whose website targets EU customers for example by enabling them to order goods or services in a European language (other than English) or enabling payment in euros
an Australian business whose website mentions customers or users in the EU
an Australian business that tracks individuals in the EU on the internet and uses data processing techniques to profile individuals to analyse and predict personal preferences, behaviours and attitudes

What activities are caught by the GDPR?
Additional obligations for Australian organisations
Right to restrict and object to processing
Consent
Right to be forgotten (or right to erasure)
Data breach notification
Appointment of a Data Protection Officer (DPO)
Data portability
Additional obligations for Australian organisations
Appointment of a representative in the EU
Compulsory Data Protection Impact Assessment
Data transfer restrictions
Automated Processing
Privacy by Design
Records of Processing Activities
What are the consequences of breaching the GDPR?
For a serious breach of the GDPR, the maximum fine is up to 4% of the global annual turnover of the company or €20 million, whichever is greater.
Other contraventions may be subject to the greater of up to €10 million, or 2% of the global annual turnover, whichever is greater.
These levels of fines are substantially more than those that may be imposed under the AU Privacy Act.
Comparison
Privacy Act – civil penalty of up to $2.1 million for serious or repeated breaches and/or compensation determined by the OAIC in response to a complaint and enforced by a Court (no direct right of action for damages, though still open question about potential availability of a claim in tort for serious invasions of privacy)
ACCC (Digital Platforms Inquiry, Preliminary Recommendations) – increase civil penalties to the greater of $10 million **or** 3 x the value of any benefit obtained through the misuse of information or 10% of a company's annual domestic turnover (in line with ACL remedies) plus introduce a direct right of action for individuals plus introduce a separate statutory cause of action for serious invasions of privacy

tracking all copies of an item and of information derived from it
determining a person's right to request removal of data
effecting the removal of all exact or derived copies of the item, once authorised

Set your Google data to self-destruct
Should Australia have a "right to be forgotten"?
Privacy in the US

US attitudes towards privacy
Federal and State laws
No single federal data privacy law
Industry laws at federal and state level requiring data privacy protection
Federal examples
    Federal Trade Commission Rules
        Facebook investigation and fine
    COPPA: Children's Online Privacy Protection Act
    HIPPA: Health Insurance Portability and Accountability Act
States: no other state follows the Californian example

California Consumer Privacy Act
Commenced on 1 January 2020
Enforcement begin July 2020
Provides Californian residents with the right to:
    Know what personal data is being collected about them
    Know whether their personal data is sold or disclosed and to whom
    Say no to the sale of personal data
    Access their personal data
    Request a business delete any personal information about a consumer collected from that consumer
    Not be discriminated against for exercising their privacy rights
California Consumer Privacy Act
Will apply to any entity, which does business in California, and satisfies at least one of the following:
    annual gross revenues in excess of $25 million
    possesses personal information of 50,000+ consumers, households, or devices
    earns more than half of its annual revenue from selling consumers' personal information
GDPR and CCPA compared
California Privacy Rights Act 2020 (CPRA)
Modified and expands CCPA
CPRA creates new and expanded rights for California residents
New compliance obligations for businesses.
Creates a new agency, the California Privacy Protection Agency, that is tasked with implementing regulations and conducting investigations and enforcement actions.

Politics
Tech companies are lobbying for the implementation of a federal bill