RESPONSIBLE DATA SCIENCE

PRIVACY AND CYBERSECURITY LAW

HAMISH MACDONALD (H.MACDONALD1@UQ.EDU.AU)

WELCOME

- Week 6: Introduction to legal issues in data science
- Week 7: Intellectual property and contract law
- Week 8: Privacy and cybersecurity law
  - The concept of privacy
  - Emergence of privacy laws
  - Australian Privacy Principles
  - Data Availability and Transparency Bill
  - Cybersecurity Law
  - Cybercrime
  - Security of Critical Infrastructure

WELCOME

- Readings posted on Blackboard. Main and additional (optional) readings
- Quiz (10%) on 19/09/2021 at 2pm, covering lecture content
- Closes on 21/09/2021 at 2pm
- Tutorials this week will include mock quiz
- Group presentation: due 22 October (can submit early)
  - Make sure you contact your group! Let Andrew know if you are having issues

ESSAY

- Q&A and information session on at 11am Brisbane time (1 hour before lecture) next week on Zoom
- Due 29 October

RECAP - CONTRACTS

- Contracts are formed through an offer and an acceptance of that offer
- Advertisements and similar kinds of displays are not contractual offers
- Contracts must have certainty, consideration, intention to create legal relations, capacity, and comply with all formalities
- If the contract is breached, the injured party will be entitled to damages, and may have the option to terminate the contract if the breach is severe enough
- Vitiating factors (misrepresentation, duress, undue influence, unconscionable dealing, ect) can allow the other party to rescind the contract

RECAP – INTELLECTUAL PROPERTY LAW

- Creates property rights over intangible classes of things
- Patents cover inventions which are new, useful, patentable, and have an inventive step (meaning the invention was non-obvious to somebody in that field)
  - Abstract ideas, discoveries, and equations cannot be patented
  - Software is an ambiguous area (as are data based inventions like gene patents). May be patentable if it produces an artificial state of affairs, particularly if the computer is essential
- Copyright automatically protects creative works which are recorded, original, and are a protectable type of subject matter (dramatic, musical, artistic or literary)
  - Literary works include computer code, so all software is covered by copyright
  - Copyright only protects the specific expression of a work, not the underlying ideas

RECAP – OPEN SOURCE

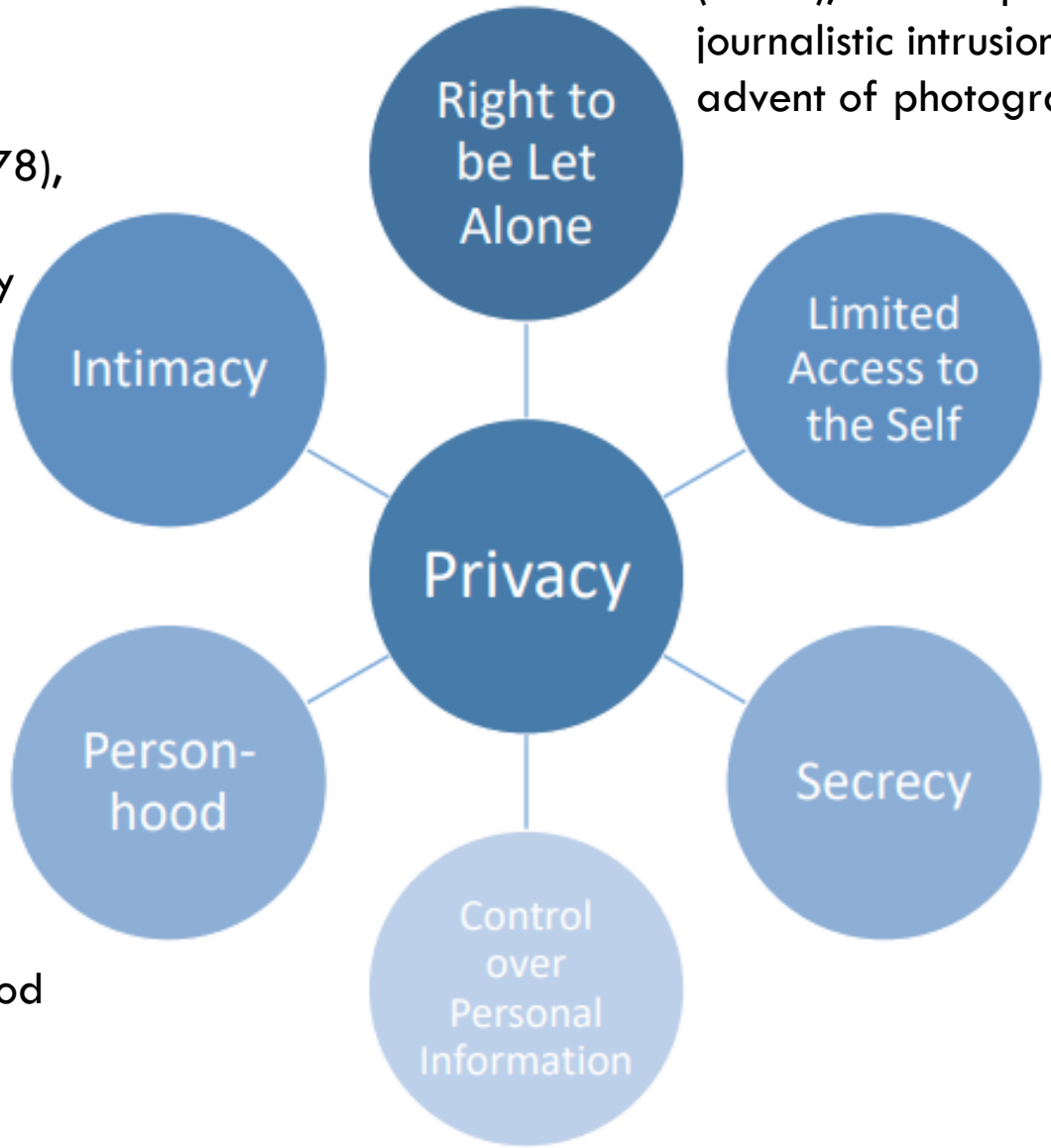
- Uses licences (contracts for use) to ensure that copyrighted material is freely available
- Similar concepts have been applied for software, science, and data
- Copyleft is a variant which requires all subsequent users to also attach the same contract

THE CONCEPT OF PRIVACY

- What is privacy?
- Why is it important (or not)?
- https://padletuq.padlet.org/hamishmacdonald/tirxc7stm4jrm40f

‘The Right to Privacy’ (1890), as a response to journalistic intrusions and the advent of photograph

‘Intimacy and Privacy’ (1978), suggesting that intimacy cannot exist without privacy



‘Privacy and the Limits of Law’ (1980), linking privacy to information, attention, and physical access

‘Privacy as an aspect of human dignity’ (1964), arguing that privacy is an important part of our individuality and personhood

‘The Right of Privacy’ (1966), economic analysis which treats privacy as secret information, and argues people should generally not have a right to conceal information about themselves

GDPR framework, intellectual property

THE EMERGENCE OF AUSTRALIAN PRIVACY LAWS

- United States Privacy Act of 1974 – covers data held by the government
- European Union Data Protection Directive (1995) – covered all data processed in the EU. Replaced by the GDPR
- These laws influenced the Australian Privacy Act 1988 (Cth) – covers data held by government agencies, and some specified businesses


Minimality
Purpose specification
Information quality
Participation and control
Disclosure limitation
Information security
Sensitivity
Fair and lawful processing

Minimality
Purpose specification
Information quality
Individual participation
Consent
Sensitivity

Information security

Disclosure limitation
Sensitivity

AUSTRALIAN PRIVACY LAW

- *Privacy Act 1988* (Cth) borrows heavily from US and EU privacy approaches
- Regulates the handling of personal information by 'APP entities', including:
  - Commonwealth agencies
  - Organisations with a turnover greater than $3 million/year
  - Private health services
  - Businesses which sell or purchase information
  - Government contractors
  - Credit reporting bodies
  - Some other small businesses

AUSTRALIAN PRIVACY LAW

- Sets out 13 Australian Privacy Principles (APPs) which APP entities must comply with
- These relate to “personal data” and “sensitive data”

AUSTRALIAN PRIVACY LAW – PERSONAL INFORMATION

- Information can be specified as personal or sensitive by other legislation
- There is not an exhaustive list of personal information
- Includes:
  - Credit information
  - Health information
  - Employee records
  - Tax file number information
  - “Sensitive information”

AUSTRALIAN PRIVACY LAW – SENSITIVE INFORMATION

- Includes information about:
  - Racial or ethnic origin
  - Political opinions, and membership of political associations
  - Religious beliefs
  - Philosophical beliefs
  - Sexual preferences and practices
  - Criminal records
  - Health records
  - Membership of trade associations or trade unions

AUSTRALIAN PRIVACY LAW – PRIVACY PRINCIPLES

- Principles based law – gives regulators and APP entities some flexibility (at the cost of certainty)
- Breach can lead to penalties, usually fines

APP 1: OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

- APP entities must take reasonable steps to implement practices, procedures and systems to ensure that it complies with the APPs, and can deal with inquiries and complaints
- APP entities must have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information

APP 2: ANONYMITY AND PSEUDONYMITY

- Individuals must have the option of dealing anonymously with the APP entity
- Anonymity means the individual cannot be identified
- This APP does not apply when it would be impractical for APP entities to deal with non-identified individuals

APP 3: COLLECTION OF SOLICITED PERSONAL INFORMATION

- Deals with the intentional collection of data
- For personal information, APP entities can only collect information that is reasonably necessary for the organisation's function or activities
- For sensitive information, the above applies and also the individual must explicitly consent to the collection
- Information must be collected from the individual concerned (and not from somebody else providing information about that individual), unless an exception applies

APP 4: DEALING WITH UNSOLICITED PERSONAL INFORMATION

- Deals with situations where personal information is received without being requested
- This information must be destroyed or de-identified if it could not have been collected under APP 3, unless it is part of a Commonwealth record

APP 5: NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

- APP entities must notify the individual of certain things, including:
  - The organisation's identity and contact details
  - The purpose, circumstances, and legality of the collection
  - The organisation's Privacy Policy
  - Whether the organisation is likely to disclose personal information overseas, and where

APP 6: USE OR DISCLOSURE OF PERSONAL INFORMATION

- APP entities must only use or disclose information for a purpose for which it was collected
- Some exceptions, including:
  - Consent
  - Disclosure authorised by another law
  - Law enforcement
  - Permitted health situations
  - Where an individual would reasonably expect the information to be used or disclosed in this secondary way, and that secondary way is related to the primary purpose (or “directly related”, if it is sensitive information)

APP 7: DIRECT MARKETING

- APP entities must not use personal information for direct marketing, unless the individual would reasonably expect to receive direct marketing (for example, consent)
- Direct marketing must include a way to opt out

APP 8: CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

- Before disclosing personal information overseas, APP entities must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information
- APP entities are accountable for privacy breaches that occur by overseas recipients

APP 9: ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

- Relates to letters, numbers, or symbols used to identify individuals
- APP entities must not use or disclose a government related identifier of an individual, unless an exception applies

APP 10: QUALITY OF PERSONAL INFORMATION

- APP entities must take reasonable steps to ensure that any personal information it collects, uses, and discloses is:
  - Accurate
  - Up-to-date
  - Complete

APP 11: SECURITY OF PERSONAL INFORMATION

- APP entities must take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access
- Information must be destroyed or de-identified once it is no longer needed

APP 12: ACCESS TO PERSONAL INFORMATION

- APP entities must give individuals access to their personal information on request

APP 13: CORRECTION OF PERSONAL INFORMATION

- APP entities must take reasonable steps to correct personal information to ensure that it is accurate, up-to-date, complete, relevant, and not misleading
- Applies if the organisation knows the data is incorrect, or if an individual requests correction

GENERAL DATA PROTECTION REGULATION (GDPR)

- Covers any company that stores or processes personal information about EU citizens
- Companies must provide a “reasonable” level of data protection for personal information – significant room for interpretation
- Emphasis on rights and control over data
  - Must be possible to withdraw consent at any time
  - Right to access data in a clear form
  - Right of erasure (replaced right to be forgotten)
  - Right to object to automated decisions

PRIVACY LAW SUMMARY

- Privacy is a complex topic with many elements, but is broadly seen as important to protect
- Government agencies, large organisations, and certain smaller organisations (APP entities) must comply with the Australian Privacy Principles or face penalties
- Has been criticised for not extending to all organisations which handle personal information, and for not going far enough in protecting individuals' privacy

DATA AVAILABILITY AND TRANSPARENCY BILL 2020

- Aims to improve data availability, sharing, and use by government agencies and contractors
- Allows accredited organisations to request controlled access to government data for the purpose of:
  - Improving government service delivery
  - Informing government policy and programs
  - Research and development

CYBERSECURITY LAW

- Broad category covering a number of different types of laws relating to information systems
- Can be roughly grouped into two types of cybersecurity laws
- Criminal laws – create penalties for people who commit offences (*retributive justice*)
- Security regulations – create obligations for organisations to store data securely (*preventative justice*)

CYBERSECURITY LAW

- *Criminal Code Act 1995* (Cth) criminalises hacking, DDoS attacks, phishing, malware infection, ect
- *Privacy Act 1988* (Cth) requires reporting of data breaches and safe storage of data
- *Security of Critical Infrastructure Act 2018* (Cth) sets out extra security requirements for critical infrastructure
- *Corporations Act 2001* (Cth) puts obligations on company directors to run their company effectively

CYBERSECURITY LAW – CRIMINAL CODE

- Criminal law refers to law which can result in criminal sanctions (imprisonment)
- In Australia, criminal codes exist at the State and Commonwealth levels
- Hacking-type offences are usually charged under the Commonwealth Criminal Code

CYBERSECURITY LAW – UNAUTHORISED ACCESS OFFENCES

- Division 478 of the *Commonwealth Criminal Code* create criminal offences for accessing, modifying, or impairing restricted data without authorisation
  - Covers electronic theft, viruses, malware, hacking
- Also creates various offences for possessing or distributing tools for committing cybercrime
  - Covers data intended to be used to commit cybercrime

CYBERSECURITY LAW – UNAUTHORISED ACCESS OFFENCES

- Division 477 creates more serious computer offences, including intent to commit a serious offence, modification of data which impairs access, or impairing electronic communications
  - Covers DDoS attacks, viruses, cybercrime used to facilitate other crimes

CYBERSECURITY LAW – OTHER CRIMINAL OFFENCES

- Phishing, and other types of online deception, are criminalised through fraud offences at the Commonwealth and State levels
- Identity theft, including the supply of fake identity materials, is criminalised by Division 372 of the Code

CYBERSECURITY LAW – PRIVACY ACT

- APP 11 creates an obligation to store data securely
- Act also requires APP entities to notify the Office of the Australian Information Commissioner (OAIC), and affected individuals, whenever there is are reasonable grounds to believe that an "eligible data breach" has occurred
- Malware signatures, observable network vulnerabilities, and so on could be reasonable grounds

PRIVACY ACT - ELIGIBLE DATA BREACH

1. There is unauthorised access to or disclosure of personal information
2. This is likely to result in serious harm to one or more individuals
3. The APP entity has not been able prevent the risk of likely harm with remedial action

CYBERSECURITY LAW – JURISDICTION

- These criminal laws have *extended geographical jurisdiction*, and apply when:
  - The offence occurs wholly or partly inside Australia, or on an Australian airport or ship
  - The result of the offence occurs wholly or partly inside Australian, or on an Australian airport or ship
  - The perpetrator is an Australian citizen or company

CYBERSECURITY LAW – SECURITY OF CRITICAL INFRASTRUCTURE ACT

- Establishes a register of Critical Infrastructural Assets
- Creates information gathering powers for relevant government Minister
- The Minister can issue directions to mitigate national security risks

CYBERSECURITY LAW SUMMARY

- Cybersecurity laws create either criminal offences or security obligations for organisations
- Australian criminal laws have extended geographical jurisdiction, and don't only cover crimes within the country
- Special provisions exist for the security of critical infrastructure

THANK YOU!

- Quiz will cover lecture content
- Get in touch if you are unsure about something
- Enjoy the rest of the course!