


CP5806: WEEK 6 COLLABORATIVE TUTORIAL SESSION

Presented by Sisi

WEEK 6 TO-DO LIST

.....

- Go through week 6 subject materials and discussion topics
- Submit Assessment 3 (due **week 7 Wednesday 19 August, 11:59pm AEST**)



AUGUST							
	M	T	W	T	F	S	S
wk 4						1	2
wk 5	3	4	5	6	7	8	9
wk 6	10	11	12	13	14	15	16
wk 7	17	18	19	20	21	22	23
O Week	24	25	26	27	28	29	30
wk 1	31						

WEEK 6 LEARNING OUTCOMES

- List a set of hurdles that hinders data sharing
- List opportunities to make more productive use of datasets
- Benefit from the use of data
- Estimate the value of data
- Define personal information
- Apply Australian privacy principles from collection to access and correction
- List the main legislation and policy frameworks governing data availability and use in Australia
- Classify public sector data from private sector data
- List reasons why data matters
- List the economic properties of data
- Differentiate stakeholders in data management and access.

TOPICS FOR WEEK 6

- Topic 1: The data landscape in Australia
- Topic 2: Australia's legislative and policy frameworks
- Topic 3: Opportunities enabled by data
- Topic 4: What holds us back?

ASSIGNMENT 3: ETHICS OR PRIVACY REPORT

➤ Specifications

- Weight: 35%
- Due: **week 7 Wednesday 19/08, 11:59pm AEST**
- Be around **1500 words**, excluding references references (word counts 10% below or above the required word limit will be penalised by 10% deduction of the marks available. The word count **must be accurately stated at the end of the written piece**. Every printed element between spaces is to be counted **including quotations and in-text references** (but not including reference list or appendices)
- Be **less than 10 A4 pages** and in **12pt Arial font**

ASSIGNMENT 3: ETHICS OR PRIVACY REPORT

➤ Overview

- Investigate and research a case study in the area of **ethics scandals** and **privacy disputes** for one of three different party relationships
 - ❖ One organisation and another organisation (e.g. Samsung against Apple)
 - ❖ An organisation and its employees (e.g. Telstra against its employees)
 - ❖ An organisation and its consumers/users (e.g. Facebook against its users).
- To investigate and research a case study in the area of ethics scandals or privacy disputes involving the **Asia-Pacific component** for one of the three different party relationships, e.g., any involved party is located in the Asia-Pacific region or a case takes place in the Asia-Pacific region etc.
- References can be used across all sections.

SECTION 1: DESCRIPTION OF YOUR CASE STUDY (10%)

.....

- Write your description using the **5W1H** (who, what, when, where, why and how) approach
- Use around **5-20 references** (including websites, blogs, articles etc.) to research and to describe your case study
- Clearly state what is the privacy or ethical problem
- Clearly state who are the parties involved – who caused the problem and who is affected
- Include relevant details about the problem, including the impact, seriousness and so on.
- This section could be around 2-3 A4 pages, around 600 words, excluding references.

SECTION 2: JUSTIFICATIONS SUPPORTING THE PARTY CAUSING THE PROBLEM (7.5%)

- Use around **5-20** references, (including websites, blogs, articles etc.) to research support for the party causing the problem
- List **4-6 reasons** and justifications that back-up or support the party causing the problem (countermeasures, remedies, precautions)
- Use in-text citations and a reference list to indicate the sources
- This section could be around **1-2 pages, around 300 words**, excluding references.

SECTION 3: JUSTIFICATIONS SUPPORTING THE AFFECTED PARTY OR PARTIES (7.5%)

- Use around **5-20** references, (including websites, blogs, articles etc.) to research support for the party causing the problem
- List **4-6 reasons** and justifications that back-up or support the affected party or parties by the problem (as well as anti-justifications against the party causing the problem)
- Use in-text citations and a reference list to indicate the sources
- This section could be around **1-2 pages, around 300 words**, excluding references.

SECTION 4: WHOSE SIDE ARE YOU ON AND WHAT WOULD YOU DO? (10%)

- Reflect on the reasons and justifications others have given that support each party
- Use around **5-20** references (including websites, blogs, articles etc.) to justify your stand
- Use in-text citations and a reference list to indicate the sources
- This section could be around **1-2 pages, around 300 words**, excluding references.

SAMPLE CASE

- Case: **Red Cross Blood Service** admits to personal **data breach** affecting half a million donors. The personal data of 550,000 **blood donors** that includes information about "at-risk sexual behaviour" has been leaked from the Red Cross Blood Service in what has been described as Australia's largest security breach
- The party causing the problem: **Red Cross Blood Service**
- The affected party or parties: **Blood donors**
- “due to human error” the unsecured data had been posted on a website by a contractor who maintains and develops the Red Cross website.

EXAMPLE

- Stand: the affected party
- Develop problem statement (**state fact** and **be specific**):
 - Data breach mainly caused by lack of supervision and inspection of third-party contractor;
 - Organisation does not treat privacy issue seriously (risk assessments and precautions)
- Identify alternatives: **propose possible solutions**
 - National laws and regulations
 - Organisational policies and standards
 - Structured system to mitigate security risks
- Choose alternatives: select **one or two solutions** that are possible to be implemented **within certain scope**
- Implement decision: briefly explain the implementation process
 - Why are we doing this?
 - What is wrong with the current way we doing?
 - What are the benefits of the new way for you?
- Evaluate results: **expected outcomes** or explain how to **measure the results**

LIST OF CASES

- Telstra privacy breach
- 7-Eleven labor scandal
- National Australia Bank (NAB) foreign exchange scandal
- Australia real estate network First National data leak
- Western Australia P&N Bank data breach
- Melbourne TAFE data breach
- Commonwealth Bank privacy breach
- Westpac consumer protection provisions breach

TOPIC 1: THE DATA LANDSCAPE IN AUSTRALIA

- Categories of data used in the report
 - Hierarchies of data
 - ❖ *Data* refers to representations of facts that are stored or transmitted as qualified or quantified symbols.
 - ❖ A *dataset* is a collection of related data points or records with a common context (such as the collation of credit card records across a bank's customer base) that can be manipulated as a unit.
 - ❖ *Information* is the meaning resulting from the interpretation of facts conveyed through data (and other sources).
 - ❖ *Knowledge* is information and experience that has been internalised or assimilated through learning (OECD 2015b).
 - Sectoral groupings of data
 - ❖ *Public sector data* is defined in this Report to be data held by government agencies — at all levels of government — and other entities that are publicly funded.
 - ❖ *Private sector data* is defined in this Report as data held by businesses and not-for-profit organisations (but not necessarily collected by them).
 - Identifiability and sensitivity of data

TOPIC 1: THE DATA LANDSCAPE IN AUSTRALIA(CONS)

- The growth in the volume and variety of data
 - **Three** emerging sources
 - ❖ social media posts, video and audio files, and emails
 - ❖ mobile devices, such as mobile phones and fitness trackers
 - ❖ physical objects (apart from computers, mobile phones or tablets) embedded with sensors
 - Data collected as:
 - ❖ *volunteered data* — when an individual actively and deliberately shares data about themselves, such as by creating a social network profile or entering credit card information for online purchases (OECD 2015a)
 - ❖ *observed data* — when an individual's action or activity is recorded.
 - ❖ *inferred data* — from the analysis (including linking) of data about an individual.

TOPIC 1: THE DATA LANDSCAPE IN AUSTRALIA(CONS)

.....

- Data — a range of potential stakeholders
 - **data collector** — a party that instigates or conducts data collection, such as a business or government agency
 - **data subject** — the party that is the subject of data, such as an individual
 - **data user** — a party that uses data that they have collected themselves or attained from other parties
 - **data compiler** — a party that compiles existing data from different sources, adding value by tailoring it for specific markets or their own use (such as data brokers or data aggregators)
 - **data funder** — a party that commissions the creation of data
 - **data transformer** — a party that transforms data with the intent of adding value, such as by de-identifying personal data
 - **data custodian** — a party that stores data; normally responsible for maintaining its security and deciding which other parties may access the data. The data custodian may very well be the data collector or data user, but may equally be a separate party entirely.
 - **data purchaser** — a party that buys data; this party may also be the ultimate data consumer.

TOPIC 2: AUSTRALIA'S LEGISLATIVE AND POLICY FRAMEWORKS

.....

➤ Definitions of personal information

- **Commonwealth** — 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.
- **New South Wales** — Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It does not include information about a person who has been dead for more than 30 years.
- **Victoria** — Information or an opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained.
- **Queensland** — Information or an opinion, 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.
- **South Australia** — Information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
- **Western Australia** — Information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion; or who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.
- **Tasmania** — Any information or an opinion in recorded format about an individual whose identity is apparent or reasonably ascertainable from the information or opinion and who is alive or has not been dead for more than 25 years.
- **Northern Territory** — Government information that discloses a person's identity or from which a person's identity is reasonably ascertainable. Personal information ceases to be covered five years after an individual's death.
- **Australian Capital Territory** — Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, whether the information or opinion is recorded in a material form or not.

TOPIC 2: AUSTRALIA'S LEGISLATIVE AND POLICY FRAMEWORKS

.....

➤ Australian Privacy Principles

- **Collection** — Personal information should be collected fairly and lawfully (APP 3, APP 4).
- **Notification** — An entity should take reasonable steps to notify an individual, or to otherwise ensure that the individual is aware of certain matters when personal information is collected about them (APP 5).
- **Disclosure** — Personal information cannot be used or disclosed for a purpose other than that for which it was collected, unless an exception applies, such as where the secondary purpose is related to the primary purpose, and the individual would reasonably expect that disclosure (APP 6). (For sensitive information, the secondary purpose must be directly related to the primary purpose).
- **Direct marketing** — Personal information may not be used for direct marketing unless the individual has consented, or it is impractical to obtain their consent (for personal information that is not sensitive). The Spam Act 2003 (Cth) and the Do Not Call Register Act 2006 (Cth) also regulate certain direct marketing communications — these are administered by the Australian Communications and Media Authority.
- **Disclosure of personal information overseas** — APP entities within Australia must take reasonable steps to protect personal information before it is disclosed overseas, except where the entity reasonably believes the overseas country has similar laws about privacy protection and enforcement/compliance.
- **Data quality and security** — an entity must take reasonable steps to ensure the personal information it holds is accurate, complete and up to date. It must also take reasonable steps to protect the information from misuse, interference, loss, unauthorised access, modification, or disclosure (APP 10).
- **Access and correction** — an entity must, on request by an individual, give access to information or correct it if inaccurate, out-of-date, incomplete, irrelevant or misleading.

TOPIC 2: AUSTRALIA'S LEGISLATIVE AND POLICY FRAMEWORKS

Table D.1 Comparing privacy principles across Australian jurisdictions

	<i>Cth</i>	<i>NSW</i>	<i>Vic</i>	<i>Qld</i>	<i>SA^a</i>	<i>WAb</i>	<i>NT</i>	<i>Tas</i>	<i>ACT</i>
Open and transparent management of personal information	✓	✓	✓	✓	✗	✗	✓	✓	✓
Sensitive information	✓	✓	✓	✓	✓	✗	✓	✓	✓
Right to anonymity/pseudonymity	✓	✗	✓	✓	✓	✗	✓	✓	✓
Notification of collection	✓	✓	✓	✓	✓	✗	✓	✓	✓
Purpose test for use / disclosure	✓	✓	✓	✓	✓	✗	✓	✓	✓
Direct marketing restrictions	✓	✗	✗	✗	✗	✗	✗	✗	✓
Cross border disclosure	✓	✗	✓	✗	✗	✗	✓	✓	✓
Government-related or unique identifiers	✓	✗	✓	✗	✗	✗	✓	✓	✓
Data quality	✓	✓	✓	✓	✓	✗	✓	✓	✓
Data security	✓	✓	✓	✓	✓	✗	✓	✓	✓
Access and correction	✓	✓	✓	✓	✓	✓	✓	✓	✓

^a Circular only — not legislative. ^b WA does not have privacy legislation.

TOPIC 3: OPPORTUNITIES ENABLED BY DATA

- Opportunities for individuals
 - Finding the right product, getting a better deal
 - Improved service delivery for individuals
- Opportunities for business
 - Improve the efficiency of processes and products
 - A basis for product innovation
- Benefits for society
 - Better monitoring and use of resources
 - Risk management
 - Improved governance structures
 - Improved government service delivery
 - Better government decision making
 - Expose government waste or corruption
 - Better research can improve social outcomes

TOPIC 4: WHAT HOLDS US BACK

- A key to achieving the many potential benefits of data use will be **building and retaining community trust** in how data is managed and used and building a shared understanding of the benefits that flow from better data access and use, including by consumers themselves.
- Community surveys indicate some concerns about the **privacy and security of personal information**.
- Legislation restricting access to data was formulated up to a century ago, and much is no longer fit for purpose.
- **A culture of risk aversion** among public servants has led to overly cautious interpretation of relevant legislation, lack of willingness to make it known that some data exists.
- **A lack of national leadership** has contributed to piecemeal bureaucratic processes for data sharing and release.
- The extent of productive linking and integrating of datasets varies substantially across jurisdictions, but is generally inadequate when viewed against the potential opportunities or practices in some other countries.
- Technical challenges are used to justify risk averse practices:
 - the risk of data breaches and re-identification of de-identified personal data;
 - fragmented data collection and release;
 - lack of common standards;
 - a shortage of skills and dedicated resources.