DATA301
Assignment 1
Izzy Southon, 300597453

Ethics, Sovereignty, Privacy, Security and Confidentiality

Q1. (10 Marks)

a. Briefly describe the data collection and its purpose. Include a list of the key items collected.

This type of data collection involves gathering loan-level data (LLD) as part of the Reserve Bank of New Zealand's (RBNZ) data and information strategy. The RBNZ's current collection of data involves collecting a high-level aggregated financial report that includes lending data from banks. The purpose of collecting LLD is to create a way to anonymously collect very detailed data on individual loans. Broadly speaking, this will improve the RBNZ's data-driven decision making and analytical capabilities, which will assist them make policy decisions, take action as necessary and identify risks. LLD is gathered by banks to manage, authorise, and issue each individual loan. The key items collected are customer information, loan dates, and loan information (Reserve Bank of New Zealand, 2024).

b. Explain which items will not be collected and explain why.

Items such as names or account numbers will not be collected as these types of data can directly identify individuals, breaching the anonymity of the data. This is done because the RBNZ understands that LLD belongs to the individual clients and entities. Additionally, anonymity is crucial for ethical data collection and use because this data is sensitive. It is important to hold and manage personal data in accordance with the Privacy Act 2020. The risks associated with a security data breach are minimised when data is anonymised. Additionally, types of data that can directly identify individuals are not necessary to make valuable insights using LLD.

c. Identify any privacy, security or confidentiality risks associated with making this collection available.

<u>Privacy risks</u>

- Who gets access to the LLD, and can people be identified before being sent to the RBNZ? The RBNZ ensures that they have communicated with their stakeholders that data given to them will be anonymised before giving them access.

- There is a risk of re-identification, where although data such as names and account numbers are not collected, there is a risk that people may be re-identified through a combination of variables within the data, such as loan amounts, dates, or locations.
- Sensitive financial information could be exposed if a data breach were to occur, given that the LLD to be transferred from stakeholders to RBNZ.
- The potential misuse of the LLD could arise if used in ways it was not originally intended for. This could lead to privacy concerns in regard to principle 10 in the Privacy Act 2020.

Security risks

- There is a risk that unauthorized individuals or groups manage to get access to the LLD, which could lead to potential misuse of data or data breaches.
- Cyber criminals may be able to get their hands on the data for their own financial gain, causing a potential risk to peoples identities, potentially leading to identity theft, data theft, and many other risks.
- People with access to the data may intentionally or unintentionally misuse the data, potentially causing an insider threat.

Confidentiality risks

a. The publication of findings could accidentally identify individuals, breaching the anonymity of the data.
b. Data released may be able to re-identify individuals through aggregation with other datasets or with the high volume of variables.

Q2. (8 Marks)

a. What is ransomware?

Ransomware is a type of malware (malicious software) that permanently denies the user access until the demanded payment is made to avoid harm or to undo what they've done. It

is essentially malicious software that can do harmful things to your computer and personal information, and then demands a ransom to undo harm (Kaspersky, 2019).

b. Which dimension of the CIA classification of cyber security best describes ransomware? Briefly justify your answer.

The dimension of the CIA classification of cyber security that best describes ransomware is availability. Ransomware makes data unavailable to the user until a ransom is paid, thus meaning that information is not readily available for the authorised user. Ransomware therefore directly disrupts the ability to use information in a timely and reliable manner, which is the core concern of the availability dimension.

c. Find out what happened in the Colonial Pipeline attack in the US in 2021. Give the key dates, who the attackers were, what they did, what effects it had, and how the attack ended.

On May 7, 2021, an American pipeline system that transports gasoline, jet fuel, and diesel fuel from Texas to the East Coast encountered a ransomware attack (Wood, 2023). This Colonial Pipeline attack resulted in the shutdown of its computerized operations such as systems for billing and accounting, affecting consumers of fuel and airlines along the East Coast (Kerner, 2022). On May 10 it was confirmed by the FBI that a hacker group known as the Darkside were responsible for the Colonial Pipeline attack (FBI, 2021; Wood, 2023). On May 6, within two hours the attackers stole 100 gigabytes of data and locked computers, requesting a ransom (NCYTE CENTER, 2021). The following day they implemented ransomware that impacted the Colonial Pipeline IT network, essentially infecting it (Kerner, 2022). This cyberattack utilised ransomware that compromised important Colonial Pipeline systems, and payment was requested to recover the data and information (Metabase Q Team, 2022). On the same day, the Pipeline was taken offline to mitigate risks associated with the ransomware. Furthermore, a ransom of 75 bitcoin ($4.4 million) was paid to the attackers from the Colonial Pipeline (Kerner, 2022; NCYTE CENTER, 2021). Joe Biden declared an emergency declaration on May 9 in attempt to mitigate the impact of the shutdown on fuel supply. Pipeline operations began to resume on May 12 (Kerner, 2022). The effects that this had were that the Colonial Pipelines operations were shut down for approximately five days. This caused shortages of gasoline, jet

fuel, and diesel fuel. Consumers of gasoline and fuel became fearful, and the panic-buying of these began (Wood, 2023). Additionally, average fuel prices increased in affected areas to the highest it had been in 6 years (Wikipedia, 2024). The attackers just wanted money, therefore once the ransom was paid by the Colonial Pipeline, the attack ended as the decryption key was obtained (Wood, 2023).

Q3. (9 Marks)

a. Briefly explain the purpose of the Act, and who it applies to.

The EU artificial intelligence (AI) Act is designed to regulate AI by organising its applications into three risk levels: unacceptable risk, high risk, and applications left unregulated. The Act aims to ensure that AI systems are used safely and ethically, banning those that pose risks that are unacceptable. AI can have positive and negative effects of people's lives; thus, the Act could become the global standard. The Act applies to anyone that uses AI systems within the EU and those outside of the EU if their AI systems impact people in the EU.

b. Briefly describe the likely impact of the Act to AI practices in New Zealand. Include comments about the dimension of Māori Data Sovereignty.

The Act is likely to set a global standard for AI practices. The EU is in the vanguard for law that are no longer subject to dispute. Some parts of the GDPR (established in 2018) have equivalents in the NZ Privacy Act 2020 (Privacy Commissioner, 2024). For example, the NZ Privacy Act 2020 states in their information privacy principles that personal information collected by an agency is collected for a lawful purpose, and that the collection of that information is necessary for the purpose (Ministry of Justice, 2020). Similarly, the GDPR states in article 5 that personal information should be collected for a specific purpose, and be processed lawfully, transparently, and fairly (General Data Protection Regulation, 2018). This reflects how NZ has adopted legislation from the EU, and therefore, it is likely that NZ will align their AI practices with EU regulations and ethical principles to facilitate international trade with the EU. To maintain access to European markets, NZ is likely to adopt standards of the Act, potentially leading to safer AI systems within NZ. It is critical to consider how AI practices may impact Māori because we need to be aware of Māori data sovereignty. Māori data

sovereignty advocates for Māori to have the right to govern the collection, ownership, and use of their data (Lilley et al., 2024). If principles from the EU Act or the Act was implemented in NZ, Māori would still not be in control of their data collection and usage. This is because Māori would be following regulations that are not their own, and still not have governance of Māori data.

c. What ethical principles of Data Science have meant that social scoring has been listed as Unacceptable in the Act? (In your answer include a brief definition of social scoring.)

Social scoring is when individuals or groups are classified or evaluated based on how they behave socially or their personal traits, resulting in the unfavourable or detrimental treatment of those people (EU Artificial Intelligence Act, 2024). Social scoring systems require vast amounts of personal data, posing significant risks to privacy. This is because it involves monitoring and evaluating behaviours and personalities. The ethical principle of privacy means that people should have the right to control their personal information, and social scoring would be violating this right through the unwarranted surveillance of people. This leads into the principle of consent, as social scoring involves collecting personal data about individuals without them necessarily knowing, violating another ethical principle. Social scoring systems have the ability to amplify existing biases in society, leading to the unfair treatment of people, contradicting the ethical principle of fairness and being unbiased. Fairness and unbiased in data science is when decisions made by analysing data should not result in the unfair treatment of people or discriminatory practices. Additionally, it can be difficult for people to understand how their scores are calculated and used by social scoring systems due to the common lack of transparency of the system.

d. Which article of the Act explicitly prohibits social scoring? Include the reference to the section, and the full text of the relevant clauses in the Act.

The article of the Act that explicitly prohibits social scoring is chapter II, Art.5 (more specifically 1c) (EU Artificial Intelligence Act, 2024). Other prohibited AI systems are deploying subliminal, manipulative, or deceptive techniques, exploiting vulnerabilities, biometric categorisation systems, assessing the risk of an individual committing criminal offenses, compiling facial recognition databases, inferring emotions in workplaces or educational institutions, and 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement (EU Artificial Intelligence Act, 2024).

> (c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:
>
> > (i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;
> >
> > (ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity;

Figure 1: screenshot of the full text explaining the prohibition of social scoring in the Act (EU Artificial Intelligence Act, 2024)

Q4. (13 Marks)

a. In a few sentences give a definition of data governance, and explain what governance means in the context of indigenous and/or Māori data sovereignty. How is data governance distinct from data ownership and data management?

According to a variety of websites, data governance is the process of managing the availability, security, integrity, usability, and quality of an organisations data (IBM, 2023; Olavsrud, 2023; Stedman, 2022). It encompasses strategies, standards and policies that are designed and utilised to ensure that data are accurate and protected (Stedman, 2022).

In the context of Māori data sovereignty, governance pertains the right for Māori to collect, hold, manage, and use their data. It means that Māori should be able have access and control to data about them. Furthermore, Māori should be able to make decisions about their data

usage and collection in ways that align with their cultural values. Most data that comes from indigenous communities is managed by non-indigenous governments (Carroll et al., 2020). Therefore, data governance in relevance to indigenous data involves the processes and stewardship needed to have indigenous control in terms of collection, analysis, storage, and use over their data (Carroll et al., 2020).

Data governance differs from data ownership as it focusses on strategies to manage data through standards that ensure data quality, availability, integrity, and security, whereas data ownership refers to legal rights to data and who has the authority to make decisions about its usage. Data governance is distinct from data management as data management is the operational practices associated with handling data, such as its storage and processing.

b. Watch the video by Professor Tahu Kukutai (from the University of Waikato) regarding the question 'What is Māori Data Governance?'. Briefly summarise the definition she gives of Māori Data Governance, and the reasons that it is important.

Professor Tahu Kukutai defines Māori data governance as putting Māori data in Māori hands, where Māori are able to control and have authority over data that belongs to them in a way that is tika and safe. She describes that it provides a clear way for Māori to have control over data about them, that comes from them, that's about their environment, their relationships, culture, and identity. It means for data to be utilised in a way that enables Māori and their environment to flourish. This is important because an abundance of data has been collected about Māori, yet it has always been to serve someone else's agenda. Māori have not benefitted from a lot of data that has been collected about them, therefore it is important to reorientate that relationship so that Māori can be the decider of how their data is used and for what narratives.

c. When Te Hiku media decided not to share their data with an open source projects, what principles of indigenous data governance were they considering?

When Te Hiku media decided not to share their data with an open-source project, they were considering the indigenous data governance principle of kaitiakitanga (guardianship). They recognise that they do not own the data that has been collected, but they are guardians of it.

They proposed the kaitiakitanga license which allows Māori organisation to have access to speech recognition before anyone else, as it is the only way that Māori could have equal opportunities to compete against non-Māori if they also had access to speech recognition. They wanted to be guardians of their data so Māori could benefit from it and serve Māori before anybody else.

d. In a few sentences explain the tension between open data, where any user can access a data set, and curated data in which only trusted users who have the data guardians' permission may have access. Use an example (from any setting you choose) to clarify your explanation.

There is tension between open data and curated data because open data prioritizes accessibility whereas curated data prioritizes security and privacy. There are benefits and risks to both open data and curated data, and it is important to navigate a balance. To clarify my explanation, consider a dataset containing medical data regarding a disease. With open data, benefits would include that more research would be conducted by a number of people. This could potentially lead to the development of new treatments or healthcare technologies, an improved understanding of the disease, or innovative strategies to manage the disease. However, there are privacy risks associated with medical data being open for anyone to view. Anonymised data can sometimes be re-identified which may expose sensitive information. This could lead to discrimination, the misuse of data, and a loss of trust in the healthcare system. In contrast, curated medical data would mean that only trusted researchers and professionals would have access to the data. This means that patient privacy is likely to be upheld and reduces the risk of data misuse. The risks associated with curated medical data is that restricted access may slow down the process of developing a treatment or cure for a disease because less researchers or scientists are working on it because they do not have access to relevant data.

References

Carroll, S., Garba, I., Figueroa-Rodriguez, O., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J., Anderson, J., & Hudson, M. (2020). The CARE Principles for Indigenous Data Governance. *Data Science Journal* , *19*, 1–12. https://doi.org/10.5334/dsj-2020-042

EU Artificial Intelligence Act. (2024, February 27). *High-level summary of the AI Act* . EU Artificial Intelligence Act. https://artificialintelligenceact.eu/high-level-summary/

FBI. (2021, May 10). *FBI Statement on Network Disruption at Colonial Pipeline*. News . https://www.fbi.gov/news/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline

General Data Protection Regulation. (2018). *Principles relating to processing of personal data* . Intersoft Consulting . https://gdpr-info.eu/art-5-gdpr/

IBM. (2023). *What is data governance?* IBM. https://www.ibm.com/topics/data-governance

Kaspersky. (2019). *What is Ransomware?* Kaspersky. https://www.kaspersky.com/resource-center/threats/ransomware

Kerner, S. (2022, April 26). *Colonial Pipeline Hack explained: Everything You Need to Know*. TechTarget. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Lilley, S., Oliver, G., Cranefield, J., & Lewellen, M. (2024). Māori data sovereignty: contributions to data cultures in the government sector in New Zealand. *Information, Communication & Society*, 1–16. https://doi.org/10.1080/1369118X.2024.2302987

Metabase Q Team. (2022, November 14). *Inside DarkSide, the ransomware that attacked Colonial Pipeline*. Metabase Q. https://www.metabaseq.com/inside-darkside-the-ransomware-that-attacked-colonial-pipeline/#:~:text=Colonial%20is%20the%20largest%20pipeline

Ministry of Justice. (2020). *Part 3 Information privacy principles and codes of practice*. New Zealand Legislation. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23342.html

NCYTE CENTER. (2021). *CYBERSECURITY AND SOCIETY*. https://maui.hawaii.edu/wp-content/uploads/2022/07/Scenario-Colonial-Pipeline-Ransomware-Attack.pdf

Olavsrud, T. (2023, March 24). *Data governance: A best practices framework for managing data assets*. CIO. https://www.cio.com/article/202183/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.html

Privacy Commissioner. (2024). *How do I comply with the GDPR?* Privacy.org.nz. https://privacy.org.nz/tools/knowledge-base/view/482#:~:text=Some%20parts%20of%20the%20GDPR

Reserve Bank of New Zealand. (2024, June 17). *Loan-level data collection*. Reserve Bank of New Zealand. https://www.rbnz.govt.nz/statistics/surveys/loan-level-data-collection#dataprivacy

Stedman, C. (2022, May). *What Is Data Governance and Why Does It Matter?* TechTarget. https://www.techtarget.com/searchdatamanagement/definition/data-governance

Wikipedia. (2024, June 7). *Colonial Pipeline ransomware attack*. Wikipedia. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack#:~:text=After%20the%20shutdown%2C%20the%20average

Wood, K. (2023, March 7). *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack*. Law Georgetown. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/#:~:text=The%20attack%20shut%20down%20Colonial