Final Task Draft: LLM Version

Contents

[Summary 2](#_Toc139025698)

[Assessment Template 3](#_Toc139025699)

[Assessment Template: [example included] 9](#_Toc139025700)

# Summary

You will be required to identify and apply key ethical, legal and technical issues relating to a real-life data science problem, conflict or dilemma (case study). Normally each student will focus on a different case study than what was covered in the presentation. In this version of the task, you will write in dialogue with a large language model (LLM).

Each student is expected to consider (a) what ethical, legal and technical solutions could be implemented to ameliorate/stop a problem and (b) reflect on the importance of ethics, law and technical perspectives, in light of what they have learned about the case study/real life problem and their learning on the course.

The analysis should be comprised of a brief introduction, the main discussion, and a conclusion. The focus of the analysis should be on demonstrating an ability to identify, describe relevant issues and apply course learnings.

Word Count: 3000 words, including LLM’s material

**The written assessment should be divided into:**

1. Outline of a real-life data science problem. This should be a topic on which there is genuine and reasonable disagreement on what the right thing to do is. It may share some similarities with your presentation topic, but do not use the same case study(ies). Explain the case study and the problem, what your analysis aims to do, and the central legal, ethical and technical question/s. Indicate one central area of disagreement on which you wish to focus. (500w)

2. Ask a LLM like ChatGPT to write a 500 word defence of some stance on this focus topic. As your task will be to critique the LLM’s response, you might want to choose a stance on the topic which you disagree with. (Note that you may need to try a few times to get an appropriate response from the LLM - you are not required to use the first thing that it spits out.) (500w)

3. The first critique: discuss the plausibility of the LLM’s response. This could take the form of fact-checking it, critiquing it with reference to some of our ethical models, identifying legal problems with the LLM’s suggestions, checking the mathematics and technical feasibility, and/or checking in general whether the response is logical and sensible. (700w)

4. Second LLM response: Challenge the LLM to respond to your critique in 500 words. Remember that we need a discussion of relevant ethical, legal, and technical aspects, and their application to the problem. Do not focus on just one area at the expense of another area (i.e. primarily focusing on ethics and not law; or only focussing on one issue). Ethics, law and technical aspects should feature relatively equally. So, this could be a good point at which to introduce aspects of the problem which you have not yet discussed. (500w)

5. The second critique: discuss the plausibility of the LLM’s response. Again, this could take many different forms, but ensure that at some point in the task you have addressed ethical, legal, and technical. (700w)

6. Finally, provide a conclusion asserting what your paper aimed to do, what the key issues you identified were, and what you have concluded from your analysis. New information should not be included in the conclusion.

# Assessment Template

1. Outline of a real-life data science problem. (500w)

|  |
| --- |
|  |

2. LLM stance. (500w)

Enter the enquiry that you posed to the LLM here:

|  |
| --- |
|  |

Enter the LLM’s response here:

|  |
| --- |
|  |

Source:

|  |
| --- |
|  |

3. The first critique. (700w)

|  |
| --- |
|  |

4. Second LLM response. (500w)

Enter the enquiry that you posed to the LLM here:

|  |
| --- |
|  |

Enter the LLM’s response here:

|  |
| --- |
|  |

Source:

|  |
| --- |
|  |

5. Second critique. (700w)

|  |
| --- |
|  |

6. Conclusion.

|  |
| --- |
|  |

7. Bibliography.

|  |
| --- |
|  |

# Assessment Template: [example included]

1. Outline of a real-life data science problem. This should be a topic on which there is genuine and reasonable disagreement on what the right thing to do is. It may share some similarities with your presentation topic, but do not use the same case study(ies). Explain the case study and the problem, what your analysis aims to do, and the central legal, ethical and technical question/s. Indicate one central area of disagreement on which you wish to focus. (500w)

|  |
| --- |
| I am looking at the Australian Government’s MyGov Health Service privacy protections, and arguing that they are adequate and that the service is effective.  [explain this…] |

2. Ask a large language model (LLM) like ChatGPT to write a 500 word defence of some stance on this focus topic. As your task will be to critique the LLM’s response, you might to choose a stance on the topic which you disagree with. (500w)

Enter the enquiry that you posed to the LLM here:

|  |
| --- |
| Please write a 500 word critique of the Australian government’s privacy measures concerning MyGov Health Service. |

Enter the LLM’s response here:

|  |
| --- |
| Title: A Critical Analysis of the Australian Government's Privacy Measures for MyGov Health Service  Introduction: The Australian government's MyGov Health Service has been touted as an innovative platform that aims to provide citizens with seamless access to their healthcare information. While the concept of a centralized digital platform for health services is commendable, it is crucial to examine the government's privacy measures to ensure the protection of sensitive personal data. This critique explores the Australian government's approach to privacy within the MyGov Health Service and highlights potential concerns and areas of improvement.  Insufficient Transparency: One major issue with the government's privacy measures is the lack of transparency surrounding data collection, usage, and storage practices. Users of the MyGov Health Service are not provided with clear and concise information regarding how their personal information is being handled. A comprehensive and easily accessible privacy policy is necessary to foster trust and allow users to make informed decisions about their data sharing.  Data Security and Breach Risk: The security of personal health information is of paramount importance, particularly considering the sensitive nature of the data involved. The government needs to ensure that robust security protocols are in place to safeguard against potential breaches and unauthorized access. Unfortunately, there have been instances in the past where government systems, such as the My Health Record, have experienced data breaches, raising concerns about the overall security posture of the MyGov Health Service.  Scope of Data Collection: Another concerning aspect is the extent of data collection within the MyGov Health Service. While it is understandable that certain information is required to provide adequate healthcare services, there is a need for clear delineation of the types of data being collected. The government must ensure that only relevant and necessary information is being accessed and stored, minimizing the risk of potential misuse or unauthorized access.  Third-Party Data Sharing: The Australian government should address concerns regarding the sharing of personal health data with third parties. Users need to be informed about any instances where their data might be shared with external entities and the purposes for which it will be used. Without explicit consent and appropriate safeguards in place, the government risks compromising the privacy and trust of its citizens.  User Control and Consent: Ensuring that individuals have control over their personal health information and granting them the ability to provide informed consent is crucial. The MyGov Health Service should implement robust mechanisms for users to manage their data, including options for opting out of data sharing or providing selective access permissions. Empowering individuals with control over their data will promote trust and mitigate privacy concerns.  Stronger Legal Framework: To enhance the privacy measures surrounding the MyGov Health Service, it is essential for the Australian government to establish a stronger legal framework. Legislation should clearly outline the rights and responsibilities of both the government and users concerning data privacy. It should address key aspects such as data retention periods, breach notification requirements, and penalties for non-compliance. A well-defined legal framework will provide a solid foundation for privacy protection and accountability.  Independent Auditing and Oversight: To instill confidence in the privacy measures of the MyGov Health Service, independent auditing and oversight mechanisms should be implemented. Regular audits by reputable third-party organizations can evaluate the effectiveness of privacy controls, identify vulnerabilities, and ensure compliance with established guidelines. Such oversight would enhance transparency and serve as a crucial check on the government's handling of personal health data.  Conclusion: While the MyGov Health Service has the potential to revolutionize healthcare access, the Australian government's privacy measures require significant improvements. Transparency, data security, scope of data collection, third-party data sharing, user control and consent, a stronger legal framework, and independent auditing are crucial areas that need attention. By addressing these concerns and implementing appropriate safeguards, the government can foster trust, protect individual privacy, and ensure the success of the MyGov Health Service in the long run. |

Source (Note: as this is not your own work, it is very important that you properly acknowledge whose work it is!):

|  |
| --- |
| This was written by OpenAI’s ChatGPT3 |

3. The first critique: discuss the plausibility of the LLM’s response. This could take the form of fact-checking it, critiquing it with reference to some of our ethical models, identifying legal problems with the LLM’s suggestions, checking the mathematics and technical feasibility, and/or checking in general whether the response is logical and sensible. (700w)

|  |
| --- |
| [Note that Chat was asked for a critique and has responded with something a bit more like a list of suggestions! We will have to think carefully about how to use this. If I am seeking to defend the MyGov system, that will mean finding the most difficult tasks here and demonstrating that they can be done. Or, denying that they need to be done! I could also have tried a different prompt to get a better response from the LLM]  I am going to look specifically at the expectation of explicit consent and the plausibility of a clear legal framework regarding privacy.  [why these? I have to narrow the scope somehow, and this choice allows discussion of ethics, law, and technical matters.]  I will talk about the difficulty of a system like that suggested functioning while requiring explicit and ongoing consent. I will draw analogies to other sorts of digital tools here, such as social media, which also requires a critical mass of users and their data. The purpose is to argue that explicit consent is too much to ask, with a view to demonstrating that the service is also too important to constrain with an unfeasible explicit consent requirement.  As for a legal framework regarding privacy, it is not immediately clear how we can clearly delineate relevant and irrelevant data here, given that our ‘health’ relates to so many other aspects of our lives. I set myself the task here of defending roughly the existing legal system.  [- I will have to explain both of these points, with reference to professional sources of course  - then I will have to argue for the current system, presumably also with reference to professional sources!] |

4. Second LLM response: Challenge the LLM to respond to your critique in 500 words. Remember that we need a discussion of relevant ethical, legal, and technical aspects, and their application to the problem. Do not focus on just one area at the expense of another area (i.e. primarily focusing on ethics and not law; or only focussing on one issue). Ethics, law and technical aspects should feature relatively equally. So, this could be a good point at which to introduce aspects of the problem which you have not yet discussed. (500w)

Enter the enquiry that you posed to the LLM here:

|  |
| --- |
| Could you write a further 500 words explaining the view of someone who thinks the following:  I don’t think that a system like MyGov Health Service can function while requiring explicit and ongoing consent. Much like social media, it requires a critical mass of users and their data, which would be compromised if it kept asking for consent.  As for a legal framework regarding privacy, I do not see how we can clearly delineate relevant and irrelevant data here, given that our ‘health’ relates to so many other aspects of our lives. |

Enter the LLM’s response here:

|  |
| --- |
| In response to the view that a system like the MyGov Health Service cannot function with explicit and ongoing consent requirements and the challenge of delineating relevant and irrelevant data within the context of health, this further response aims to provide an alternate perspective. While there are valid concerns regarding consent and defining relevant data, it is crucial to explore potential solutions that balance the needs of the system with privacy protection and user trust.  Functionality and Critical Mass: One argument against requiring explicit and ongoing consent in the MyGov Health Service is that it could hinder its functionality and compromise the critical mass of users and data necessary for its success. Similar to social media platforms, maintaining user engagement and data flow is vital to harness the full potential of such services.  However, it is important to note that consent mechanisms do not have to be intrusive or disruptive to the user experience. The implementation of well-designed consent processes that are clear, concise, and integrated into the user interface can mitigate these concerns. By obtaining broad initial consent and offering users the ability to manage their data sharing preferences through granular controls, the system can strike a balance between data accessibility and user privacy.  Furthermore, the critical mass argument assumes that individuals would not be willing to participate in a health service that respects their privacy rights. However, surveys and studies have shown that individuals value privacy and are more likely to engage with platforms that offer robust privacy protections. By prioritizing user privacy and ensuring transparent communication about data handling practices, the MyGov Health Service can build trust and encourage participation without compromising consent requirements.  Defining Relevant Data within Health: The complexity of delineating relevant and irrelevant data within the context of health is indeed a challenge, as health is a multidimensional concept intertwined with various aspects of our lives. It is not limited to medical records but encompasses factors such as genetics, lifestyle choices, environmental influences, and social determinants of health.  While it may be challenging to clearly delineate all aspects of relevant data, a legal framework can provide overarching principles and guidelines. Rather than trying to define specific data points as relevant or irrelevant, the focus should be on establishing clear principles that govern the collection, use, and protection of personal health information. These principles should encompass data minimization, purpose limitation, data anonymization or de-identification, and secure storage practices.  To address the multifaceted nature of health-related data, a flexible legal framework can adopt risk-based approaches. This involves evaluating the sensitivity of different data elements and tailoring privacy protections accordingly. It acknowledges that certain types of data may require stricter safeguards due to their potential impact on individuals' privacy and well-being.  Moreover, stakeholder engagement and collaboration are crucial in defining the scope of relevant data. Consulting healthcare professionals, privacy advocates, legal experts, and individuals directly affected by the MyGov Health Service can ensure a comprehensive understanding of the intricacies involved. This collaborative approach allows for diverse perspectives and ensures that the legal framework considers the evolving needs and expectations of individuals.  Conclusion: While concerns about consent and defining relevant data in the MyGov Health Service are valid, there are ways to address these challenges without compromising functionality or privacy protection. By implementing well-designed consent mechanisms that integrate seamlessly into the user experience and offering granular controls, the system can strike a balance between user convenience and privacy rights. Additionally, a flexible legal framework based on overarching privacy principles and stakeholder collaboration can guide the collection, use, and protection of personal health information.  It is important to recognize that privacy and functionality are not mutually exclusive. By prioritizing user trust, transparency, and ongoing engagement with stakeholders, the MyGov Health Service can successfully navigate the complexities of consent and relevant data. Ultimately, the goal should be to build a system that respects individuals' privacy while leveraging data for [ChatGPT cuts off here inexplicably, perhaps because of its assigned word count] |

Source (Note: as this is not your own work, it is very important that you properly acknowledge whose work it is!):

|  |
| --- |
| This was written by OpenAI’s ChatGPT3 |

5. The second critique: discuss the plausibility of the LLM’s response. Again, this could take many different forms, but ensure that at some point in the task you have addressed ethical, legal, and technical. (700w)

|  |
| --- |
| [the discussion is now getting to a more sophisticated phase, and ChatGPT is struggling to keep up. this could be a good place to start pointing out straight-up inconsistencies and fallacies in the responses. ChatGPT also seems very keen to defend the MyGov system – maybe it needs to be told more sternly that this is not its job in the dialogue!]  The first thing to point out is that the claim that “it is crucial to explore potential solutions that balance the needs of the system with privacy protection and user trust” is ‘begging the question’ [i.e. - to believe this, the MyGov opponents have to assume that they were wrong from the start! But we don’t want to assume that, we want to see an argument that they were wrong]. So, I reject the claim that a middle ground needs to be found, unless more of an argument can be given that these services are indeed essential.  The discussion of consent takes us into a discussion of choice and the difference between opting in and opting out…. I do think, and will argue, that if we follow ChatGPT’s suggestion here, either users will be overwhelmed with choice, or insufficient users will consent for the service to be worth maintaining… [Cite the literature on online consent and/or behavioural economics here] So the existing system is the best we can hope for.  ChatGPT is correct to suggest that critics may overemphasise the importance of delineating what exactly is health data and what is not. There are other distinctions which may be important, and techniques for managing extremely extensive datasets such as would be generated on a broad understanding of ‘health’…  Nevertheless, we have some problems here…. For example, much of the data need to be de-anonymizable if they are to all be used for their intended purpose of personal healthcare…  I propose this solution…. [citing the relevant literature.] |

6. Finally, provide a conclusion asserting what your paper aimed to do, what the key issues you identified were, and what you have concluded from your analysis. New information should not be included in the conclusion.

|  |
| --- |
| In conclusion, MyGov Health Service privacy protections are adequate and the service is effective.  (repeat key concerns, and key responses to these)  [It may be that ChatGPT needed more substantive input that I gave it here, but I do not feel that the sceptic’s view has been given a full hearing here...] |

7. Bibliography.

|  |
| --- |
| [Insert bibliographical list here]  [given the formatting of the document, in-text referencing will probably be more appropriate than footnotes] |