

Ethics Report

31272 | Project Management and the Professional

Student Name: Om Shah

Student ID: 24831101

Tutor Name: Amaan Ansari

Tutorial Number: 10

Due Date: 24 September 2025

Contents

1. Executive Summary	3
2. Introduction	4
3. Scope	4
3.1 Problem Statement	4
3.2 SMART Scope Statement	5
4. Ethical Considerations	6
4.1 Data Collection and Retention	6
4.2 Location Tracking and Guest Consent	7
4.3 Child Safety and Background Checks	8
5. Evaluation via Professional Codes of Ethics	10
5.1. ACS Code of Ethics.....	10
5.2. PMI / IEEE.....	11
5.3. Comparative Analysis	12
6. Recommendations	13
7. Conclusion	14
8. References.....	15
9. Appendix.....	15

1. Executive Summary

This report reviews the ethical challenges involved in creating the Guest Hospitality System (GHS) for the Tourism Resorts Group (TRG). The GHS will combine bookings, payments, childcare services, and an optional RFID tracking feature. While these tools are designed to make resorts more convenient and enjoyable, they also raise serious issues around privacy, safety, and professional responsibility.

Three main concerns are identified. The first is data collection and retention. Collecting more information than necessary, or keeping it longer than required, makes breaches far more damaging. The Australian National University (ANU) breach showed how years of stored data made the effects of one attack much worse, highlighting the need for data minimisation and timely deletion.

The second concern is RFID tracking. While this feature could help families locate each other, location data is highly sensitive and can be misused if leaked. The Tea app breach in 2025 exposed user verification images and location information, which were later used to build public maps and even turned into an online ranking game. This example shows how quickly leaked data can be exploited and why RFID systems must be optional, secure, and supported by strict consent and deletion practices.

The third concern is childcare and staff vetting. Children are a vulnerable group and require stronger protection. Queensland's Blue Card scheme enforces clearance checks, yet a 2025 ABC case showed how failures in the process allowed an unsuitable childcare worker to remain in the role. TRG must ensure that only qualified and cleared staff work with children or access their records.

These issues are evaluated against professional codes of ethics from the Australian Computer Society (ACS), the Project Management Institute (PMI), and the Institute of Electrical and

Electronics Engineers (IEEE). The report concludes with recommendations to limit data collection, ensure consent for RFID tracking, and enforce strict staff vetting in childcare services.

2. Introduction

The Tourism Resorts Group (TRG) is developing a Guest Hospitality System (GHS) that will combine bookings, payments, childcare services, and an optional RFID tracking feature. The system is intended to make resort operations more efficient and improve guest experiences, but it also raises important concerns about privacy, safety, and responsibility.

The GHS will collect and store sensitive information such as payment details, travel plans, and children's enrolments. This data must be managed with care. If these risks are not addressed, the consequences could include privacy breaches, misuse of information, or harm to children. They could also damage the trust that families place in TRG.

This report examines three main ethical issues: data handling, location tracking, and childcare. It then evaluates these issues against professional codes of ethics to provide guidance for TRG and PMP.

3. Scope

3.1 Problem Statement

The Guest Hospitality System (GHS) will process sensitive personal information, including names, payment details, itineraries, and childcare enrolments. While

designed to improve guest experiences and streamline resort operations, it raises ethical risks if TRG collects too much data, retains it for longer than necessary, or fails to properly protect it, the result could be privacy breaches, misuse of information, or harm to vulnerable groups such as children.

3.2 SMART Scope Statement

This report looks at three main ethical issues: data collection and retention, RFID-based location tracking, and childcare staffing. The analysis is organised using the SMART framework.

S	Focused only on these three issues.
M	Evaluated against the Australian Privacy Principles and three professional codes of ethics.
A	Based on real-world cases, regulations, and professional standards.
R	Aligned with TRG's goal of building a secure, family-friendly system.
T	Applied to the planned rollout of the GHS on 3 May 2027.

By setting the scope this way, the report stays focused on the most pressing ethical challenges while ensuring recommendations are practical and grounded in professional standards.

4. Ethical Considerations

4.1 Data Collection and Retention

The GHS will handle sensitive personal information across multiple functions, collecting information such as name, contact details, itineraries, payment information, and children’s enrolments in day care as mentioned in the project charter. The wide range of information GHS will need to compile due to both functional and regulatory compliance reasons means PMP needs to ensure that the data is handled both ethically and with care. Things like collecting only the data necessary, or retaining it only as long as is required reduces the scope of risk and this form of intrinsic data minimisation contains the damage caused by any leaks and reduces the possibility of profiling, misuse, or third-party use without the client’s consent. Both ethical practice principles and Australian law dictate how important it is for us as PMP to make sure that we use data minimisation in our system.

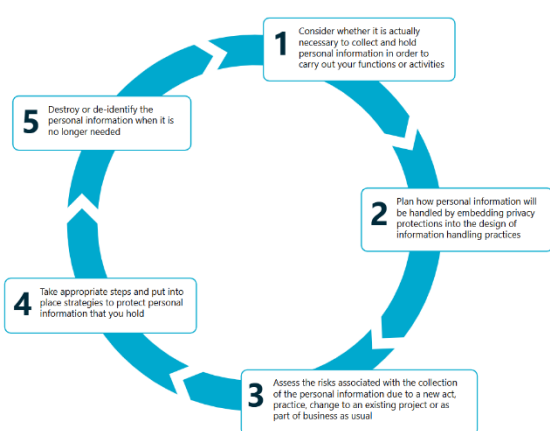


Figure 1 - Information Lifecycle (OAIC, 2023)

kept. The OAIC explains this responsibility as part of the information lifecycle, which begins with deciding if information really needs to be collected and ends with securely disposing of it when it is no longer required (**Figure 1; OAIC, 2023**).

The importance of these obligations can be seen in the Australian National University (ANU) breach, which was disclosed in June 2019. ANU confirmed that a “sophisticated operator” had gained unauthorised access to significant amounts of personal staff, student and visitor data

Under the Australian Privacy Principles, APP 3 requires organisations to only collect personal information that is genuinely necessary for their function. APP 11.2 goes further by requiring organisations to take reasonable steps to either destroy or de-identify that information once it is no longer needed unless the law requires it to be

extending back 19 years (*Palacios & Morales-Rocha, 2021, p. 10*). This incident demonstrates how retaining large volumes of historical data that are no longer required magnifies the scale of a breach and directly undermines the intent of APP 11.2, which requires organisations to destroy or de-identify personal information once it is no longer needed. Supporting research also shows that human factors are a major driver of risk.

4.2 Location Tracking and Guest Consent

The GHS will include an optional RFID-based feature that allows families to track the location of their group members, particularly children, within the resort. While this can be convenient and provide reassurance for parents, it raises significant ethical concerns around privacy, surveillance, and informed consent. RFID tracking may seem less intrusive than mobile GPS because it only logs presence at certain points, but in practice it is tied directly to named guest accounts, payments, and childcare enrolments. This linkage means that if compromised, the data is no longer anonymous and could be used to reconstruct detailed routines. In the case of children, that risk is especially serious.

The sensitivity of location data has been highlighted in real-world scenarios. During the COVID-19 pandemic, businesses were legally required to collect check-in data using QR codes. Under APP 3, only the minimum information reasonably necessary could be collected, and under APP 11.2, organisations were required to de-identify or destroy that data once restrictions were lifted because they no longer had a legitimate purpose to retain it. This example shows how important it is that location tracking remains purpose-limited, short-term, and backed by strong deletion practices.

A more recent illustration comes from the Tea app breach in 2025, which is now the subject of federal litigation in the United States. In *Reyes v. Tea Dating Advice, Inc. (N.D. Cal., filed July 28, 2025)*, plaintiffs alleged negligence and unfair business practices after unsecured Firebase storage exposed around 72,000 images, including 13,000 identity selfies, and over 1.1 million

private direct messages. A parallel case, *Karam v. Tea Dating Advice, Inc.* (*E.D. La., 2025*), raised similar claims of harm. Beyond the litigation, leaked image metadata was extracted and used to build public maps plotting the precise locations of women who had registered with the app (*Figure 2*). Worse still, the images were repurposed into a ranking game on the website TeaSpill, where users assigned scores to women based on appearance (*Figure 3*). Even with redaction, these examples demonstrate how leaked identity and location data can be weaponised for harassment, humiliation, and exploitation.

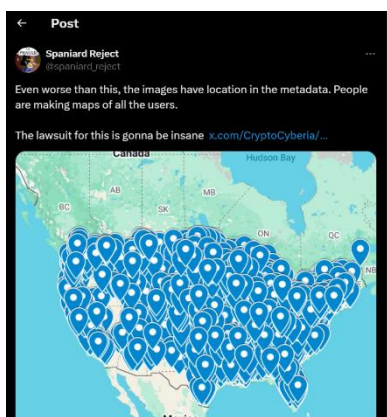


Figure 2 - Map tracking leak victims via metadata and driver's licenses (Spaniard Reject, 2025)



Figure 3 - Example of secondary exploitation of Tea app breach data (faces blurred and offensive language redacted by author) (Teaspill, 2025).

The key lesson for PMP is that even limited RFID tracking can become dangerous once tied to individuals. A breach could turn movement logs into maps of children or guest routines or see the data exploited in unexpected and harmful ways. The Tea app cases show that poor governance of identity and location data leads not only to financial liability but also to public shaming, stalking, and a loss of trust in the organisation responsible.

4.3 Child Safety and Background Checks

As GHS will also support childcare and supervised activities, as identified in Objective 6 of the project charter, our system is liable to significant ethical obligations, since children are a vulnerable group and require higher levels of protection. Any failure to properly vet or supervise

staff in these services risks serious harm, not only to the children directly but also to TRG's reputation and trustworthiness as a service provider.

Figure 4 shows that the greatest dangers often come from within an organisation, whether

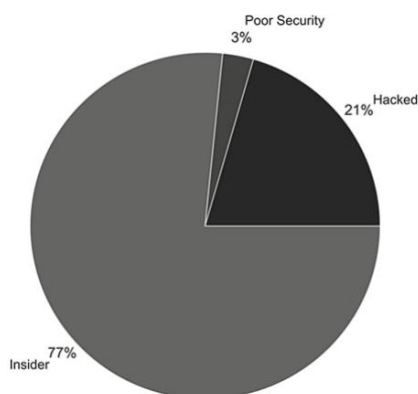


Figure 4 - Percent-based pie chart of subcategories of data breaches (Palacios & Morales-Rocha, 2021, p. 9).

through negligence, carelessness, or intent. In childcare, these risks are amplified as the existence of illicit financial markets for child exploitation material means that malicious insiders may have a stronger incentive to target them. Allowing unvetted or unqualified staff access to children is therefore not only a governance failure but a serious ethical breach that can result in lasting harm.

Australian regulations place a strong duty of care on organisations that work with children. In Queensland, the Blue Card scheme requires anyone in child-related roles to hold a valid clearance, following the rule of “No Card, No Start” (Queensland Government, 2024). Failures in this system show what is at stake. In 2025, ABC News reported on a childcare worker who kept clearance despite red flags and was later charged with dozens of offences (ABC News, 2025). This highlights how relying only on manual checks or assumptions of trust can end in disaster.

PMP and TRG must come together to ensure only accredited, cleared, and trained staff should ever be permitted to work with children. Without proper vetting and monitoring, our system could expose children to harm. Meeting this duty of care is not just about compliance, it is about safeguarding families and maintaining public trust in TRG's services.

5. Evaluation via Professional Codes of Ethics

5.1. ACS Code of Ethics

The ACS Code of Ethics is built on four key values: Honesty, Trustworthiness, Respect for Others, and Respect for the Profession. In practice, this means IT professionals are expected to protect people's privacy, reduce risks, work competently, and build systems that are secure, reliable, and user-friendly.

How the ACS Code applies to TRG's case study issues

- Data Collection and Retention

The Guest Hospitality System (GHS) will store names, payment details, itineraries, and childcare enrolments. Under the ACS principle of trustworthiness, PMP must collect only what is necessary, protect it, and delete it once no longer required. The ANU breach in 2019 showed the risks of holding excess data. Respect for others reinforces that over-retention increases harm, while honesty requires TRG to be transparent about collection and retention.

- RFID Tracking

RFID tracking can help families locate each other but also creates privacy risks if misused. The ACS Code requires professionals to reduce risks before harm occurs. For PMP, this means making RFID optional, requiring clear consent, and deleting logs quickly. Honesty demands transparent explanations of data use, while trustworthiness requires secure design that prevents linking to other records without permission.

- Child Safety

Since the GHS will support childcare, the ACS Code places strong responsibility on PMP to protect children. Respect for others means safety must come first, preventing unvetted staff from working with or accessing records. Respect for the profession requires PMP staff to only

take roles they are qualified for. This includes enforcing clearance checks, such as Queensland's Blue Card, through the system rather than relying only on manual oversight.

5.2. PMI / IEEE

PMI Code of Ethics

The Project Management Institute (PMI) Code is based on responsibility, respect, fairness, and honesty (*PMI, 2016*).

For data collection and retention, PMI would say that responsibility means only gathering information that is needed and deleting it once it is no longer required. The ANU breach showed the damage that can occur when this duty is ignored (*Palacios & Morales-Rocha, 2021*). Honesty also means we must be clear with guests about why data is collected and how long it will be kept.

For RFID tracking, PMI highlights respect and fairness. Guests should never feel pressured to use the feature, and those who opt out must not be disadvantaged. Honesty requires that we give accurate and easy-to-understand explanations about risks and safeguards so families can make an informed choice.

For childcare vetting, PMI expects us to act with responsibility and respect by ensuring only cleared and qualified staff work with children. The ABC childcare case in 2025 shows the serious harm that follows when these values are not upheld (*ABC News, 2025*).

IEEE Code of Ethics

The Institute of Electrical and Electronics Engineers (IEEE) Code stresses avoiding harm, protecting privacy, being honest, and acting responsibly.

For data collection, IEEE would expect us to limit what we store, protect it securely, and remove it quickly when no longer needed (*IEEE, 2023*). For RFID tracking, IEEE would require honest

communication about risks and strong technical safeguards to protect privacy. For childcare, IEEE's duty to avoid harm makes proper checks and competent staff non-negotiable (*IEEE, 2023*).

Both PMI and IEEE reinforce that responsibility, honesty, and the prevention of harm must guide how we design and operate the GHS (*PMI, 2016; IEEE, 2023*).

5.3. Comparative Analysis

The ACS, PMI, and IEEE codes all guide ethical practice, but each emphasises different dimensions that reflect their professional concerns (*ACS, 2023; PMI, 2016; IEEE, 2023*).

- Similarities

All three codes demand honesty as foundational. Guests must be told what data is collected, why, and how long it is kept. Each also emphasises avoiding harm: ACS via respect and trustworthiness, PMI via responsibility and fairness, and IEEE through privacy and safety. Competence or professional capability is likewise common: ACS expects practitioners to be trustworthy and skilled, PMI expects accountability in project decisions, and IEEE demands accurate, safe engineering practices (*ACS, 2023; PMI, 2016; IEEE, 2023*).

- Differences

ACS is tailored to the Australian ICT context and ties into community trust and legal norms (*ACS, 2023*). It frames ethical obligations in terms of public interest and respect for users. PMI is process- and stakeholder-oriented; it frames ethics around how projects are run, how decisions are made, and how stakeholders are treated (*PMI, 2016*). IEEE is more technical: it pays special attention to system design, safety, disclosures of risk, and the engineering integrity of solutions (*IEEE, 2023*).

- Why those differences

They come from professional roles. ACS serves ICT professionals (software, systems) with a local legal/social lens. PMI works with project managers who must balance competing stakeholder demands and procedural fairness. IEEE addresses engineers and designers whose decisions have technical consequences. Each code emphasises what matters most to its field while still promoting overall ethical alignment (*ACS, 2023; PMI, 2016; IEEE, 2023*).

- Case study application

On data collection, ACS would focus on public trust and data minimisation, PMI on responsibility to stakeholders, and IEEE on safe architecture. On RFID, ACS would stress consent and respect, PMI fairness and stakeholder choice, IEEE system security and privacy safeguards. On childcare, ACS sees it as duty of care, PMI as stakeholder responsibility, and IEEE as a design-safety issue (*ACS, 2023; PMI, 2016; IEEE, 2023*).

6. Recommendations

Based on the ethical issues reviewed in this report, three key recommendations are made for the Guest Hospitality System (GHS).

- Limit data collection and retention

Only gather the information that is essential for bookings, payments, and childcare. Set strict retention periods and delete or de-identify data once it is no longer needed. This reduces the risk and impact of any future breach (*OAIC, 2019*).

- Strengthen RFID tracking security and transparency.

Although this feature is optional, it carries high privacy risks. TRG must ensure the system is secure against hacking or misuse, that location logs are deleted quickly, and that guests are given clear information about how the data is used and who can access it **(IEEE, 2023)**.

- Enforce strict childcare vetting.

The system must include controls to prevent unvetted staff from working with children or accessing their records. Clearances such as the Queensland Blue Card should be checked automatically before staff can be scheduled **(Queensland Government, 2024)**.

By following these recommendations, TRG can strengthen guest trust, meet legal and ethical standards, and reduce the risks of harm **(ACS, 2023; PMI, 2016)**.

7. Conclusion

The Guest Hospitality System (GHS) can make TRG resorts easier to use and more enjoyable for guests, but it also brings serious ethical responsibilities. If personal data is mishandled, if location tracking is misused or if childcare checks are weak, the impact on guests and community trust could be severe. In this report we examined three main areas: data collection and retention, RFID tracking, and childcare vetting. We showed how each issue can be managed through professional standards and practical safeguards. We also reviewed real-world breaches that highlight the harm caused when these responsibilities are ignored. By learning from these examples and applying professional codes of ethics, we can design and deliver a system that protects privacy, keeps families safe and strengthens trust in TRG's services.

8. References

ABC News. (2025, February 14). *Childcare worker kept clearance despite red flags before being charged with offences*. Australian Broadcasting Corporation.

<https://www.abc.net.au/news/2025-02-14/childcare-worker-charged-despite-blue-card-red-flags/>

ABC News. (2025, August 13). *Sacked childcare worker was allowed to keep Working with Children Check*. Australian Broadcasting Corporation.

<https://www.abc.net.au/news/2025-08-13/childcare-worker-to-lose-working-with-children/105646976>

Australian Computer Society. (2023). *ACS Code of Professional Ethics*. Australian Computer Society. <https://www.acs.org.au/governance/rules-and-regulations.html>

IEEE. (2023). *IEEE Code of Ethics*. Institute of Electrical and Electronics Engineers.

<https://www.ieee.org/about/corporate/governance/p7-8.html>

Karam v. Tea Dating Advice, Inc., No. 2:25-cv-01790 (E.D. La. filed 2025). *CourtListener*.

<https://www.courtlistener.com/docket/71252481/karam-v-tea-dating-advice-inc/>

Office of the Australian Information Commissioner. (2019, July). *Australian Privacy Principles guidelines* (Combined ed.). Australian Government.

https://www.oaic.gov.au/_data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf

Office of the Australian Information Commissioner. (2023). *Guide to securing personal information*. Australian Government. <https://www.oaic.gov.au/privacy/privacy->

[guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information](https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information)

Office of the Australian Information Commissioner. (n.d.). *Retention and deletion of personal information collected during COVID-19*. Australian Government.

<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/covid-19/retention-and-deletion-of-personal-information-collected-during-covid-19>

Palacios, R., & Morales-Rocha, V. (2021). Cybersecurity and data breaches: Case studies and analysis. In *Computational intelligence for business analytics*. Springer.

https://cathi.uacj.mx/bitstream/handle/20.500.11961/19686/483702_1_En_17_version_Author%20%281%29.pdf?sequence=1&isAllowed=y

Project Management Institute. (2016). *PMI Code of Ethics and Professional Conduct*. Project Management Institute. <https://www.pmi.org/>

[/media/pmi/documents/public/pdf/ethics/pmi-code-of-ethics.pdf](https://www.pmi.org/-/media/pmi/documents/public/pdf/ethics/pmi-code-of-ethics.pdf)

Queensland Government. (2024). *Working with children (Blue Card) system*. Queensland Government. [https://www.qld.gov.au/law/laws-regulated-industries-and-](https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/regulated-industries-and-licensing/blue-card)

[accountability/queensland-laws-and-regulations/regulated-industries-and-licensing/blue-card](https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/regulated-industries-and-licensing/blue-card)

Queensland Government. (2025). *Changes to the blue card system*. Queensland Government.

<https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/regulated-industries-and-licensing/blue-card/system/changes-to-the-blue-card-system>

Queensland Government. (n.d.). *Blue cards – No Card, No Start: Frequently asked questions*.

Queensland Government.

https://www.qld.gov.au/_data/assets/pdf_file/0026/158444/faq-no-card-no-start.pdf

Reyes v. Tea Dating Advice, Inc., No. 3:25-cv-06321 (N.D. Cal. filed July 28, 2025). *Justia*.

<https://dockets.justia.com/docket/california/candce/3:2025cv06321>

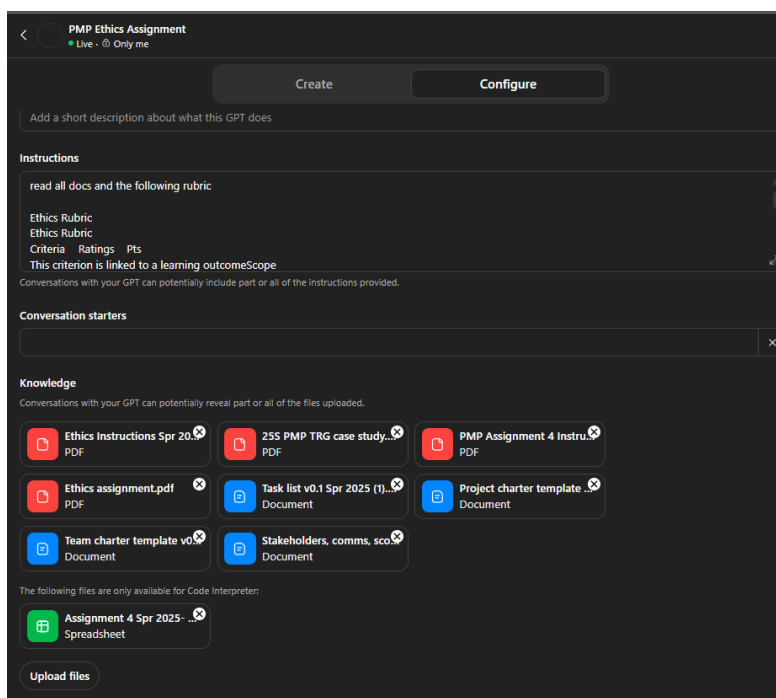
Spaniard Reject [@spaniard_reject]. (2025, July 25). Even worse than this, the images have location in the metadata. People are making maps of all the users. The lawsuit for this is gonna be insane. X. https://x.com/spaniard_reject/status/1948807698947981486

TeaSpill. (2025). *TeaSpill website*. <https://teaspill.games/>

9. Appendix

Use of Gen AI

I began by creating a custom GPT with files provided which were pertinent to the assignment. This helped ensure that I didn't miss anything in the rubric or any of the instructions so that no marks are unnecessarily dropped without realising.



Following this I asked chatgpt to generate a skeleton so I can get an understanding of what subjects I am required to discuss throughout the assignment as seen in the snippet.

Executive Summary (not counted in word count)

- Short overview of system and key issues
- Summary of findings and recommendations

1. Introduction

- Brief description of TRG Guest Hospitality System (GHS)
- Purpose of the report
- Identification of three key ethical issues (data, RFID, childcare)

2. Scope

- SMART objectives (Specific, Measurable, Achievable, Relevant, Time-bound)
- Scope boundaries (what is and isn't covered)
- Note that focus is on ethics, not technical design

3. Ethical Considerations

3.1 Data Collection and Retention

- Risks of over-collection and long retention
- APP 3 and APP 11.2
- Example: ANU breach (2019)
- Why it matters ethically and legally

3.2 RFID Tracking and Consent

- Benefits vs privacy risks
- APP requirements for consent and deletion
- Example: Tea app breach (2025), map and TeaSpill site
- Ethical implications

After that for the sections I needed to find sources and articles pertinent to the points I wanted to make, to do that I tried to use Google's Gemini to access articles on Google Scholar, but it didn't have access to Google Scholar and some cursory tests revealed it couldn't guide me to the things I needed so I had to manually do some research.

are you good at using google scholar to find relevant information on things?

◆ I don't directly "use" Google Scholar in the way a human does. I don't have a web browser to navigate to the site, type in queries, or click on links.

Instead, I have access to the same vast amount of information that Google Scholar indexes, and I can search through it very quickly and efficiently using my underlying architecture. Think of it like this: a human uses a tool (Google Scholar) to access a database, while I am directly connected to a similar, or even more comprehensive, database.

With stuff like the Tea app, Optus breach, and other examples in the ethical considerations section I already had prior knowledge about them however to find direct sources it was slightly more difficult but the hardest one was the Tea app. When I couldn't find anything on Google Scholar, I asked ChatGPT for alternatives as I didn't want to use Reddit or News articles as they aren't trustworthy when ChatGPT suggested legal aspects that might be pertinent to the Tea app which is how I found the ongoing lawsuits.

I cant find anything about the Tea App data breach on google scholar is there another way to get reliable articles about it or something that can be used in my ethics report because news and reddit arent reliable

Yes — in cases like the **Tea app breach**, when peer-reviewed material isn't yet available on Google Scholar, a solid alternative is to rely on **legal and regulatory sources**. These are considered reliable and citable in academic work because they are primary documents.

For example:

- **Court filings and dockets:** The lawsuits *Reyes v. Tea Dating Advice, Inc.* (N.D. Cal.) and *Karam v. Tea Dating Advice, Inc.* (E.D. La.) are public records. You can access them through **Justia**, **CourtListener**, or **PACER**.
- **Regulatory body statements:** If any US state or federal regulator investigates, their press releases or official findings would be trustworthy.
- **Industry legal reporting:** Sites like Law360 or Bloomberg Law sometimes provide summaries of ongoing tech/data cases, which are more reliable than blogs or Reddit.

By citing the **federal lawsuits**, you can ground your report in verifiable, primary legal sources instead of relying only on news or social media. This is the same approach you took when you added *Reyes v. Tea Dating Advice, Inc.* and *Karam v. Tea Dating Advice, Inc.* into your references.

ChatGPT also helped summarise some of the documents such as PMI and IEEE and create APA7th references as it was time consuming to individually do each one