Cambridge Analytica Scandal: Data Exploitation and the Ethics of Social Media Influence

In Partial Fulfillment of the Requirements for

IS181 – Social Issues and Professional Practices

Submitted by:

Mandap, Jomer R.

Submitted to:

Lisondra, Cherry B.

February 28, 2025

Introduction

The Cambridge Analytica Scandal of 2018 emerged as a defining incident in the debate over data privacy, ethical technology practices, and the impact of social media on democratic processes. This case involved Cambridge Analytica, a political consulting firm, that harvested the personal data of over 87 million Facebook users without explicit consent, using it for psychological profiling and targeted political advertising. These practices were primarily associated with the 2016 U.S. Presidential Election and the Brexit referendum, where microtargeted campaigns potentially swayed public opinion through manipulative data analytics.

The scandal highlighted significant ethical concerns, including the breach of user privacy, corporate negligence, and the responsibility of technology companies like Facebook in protecting user data. The incident prompted a global conversation about data governance, the ethical use of big data, and the regulatory frameworks needed to safeguard personal information. The objective of this research is to analyze the ethical, legal, and professional considerations of this scandal, employing ethical theories such as utilitarianism, deontology, Mill's Harm Principle, virtue ethics, and social contract theory, alongside regulatory insights from GDPR, CCPA, and industry ethical standards like ACM and IEEE.

This document is meticulously structured to align with the ethics worksheet framework, ensuring that each of the 13 questions is addressed in a detailed and systematic manner. The analysis will not only provide answers to these questions but will also weave them into a cohesive narrative that explores the ethical dimensions of the case study. By doing so, the document aims to present a comprehensive understanding of the ethical dilemmas at hand, while also highlighting the ambiguities that often arise when navigating complex issues in technology and society.

Case Study

The Cambridge Analytica Scandal, which surfaced in 2018, exposed how personal data of millions of Facebook users was exploited without consent, highlighting critical gaps in data privacy and corporate ethics. The scandal began in 2014 when academic researcher Aleksandr Kogan developed the app "This Is Your Digital Life." While the app had direct consent from around 270,000 users, Facebook's API at the time allowed the app to access the data of users'

friends, leading to a massive data breach affecting 87 million individuals globally (Arora & Zinolabedini, 2019).

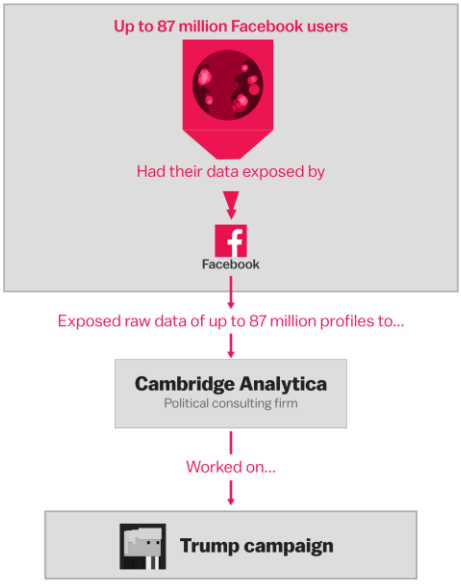

Figure 1. Cambridge Analytica Scandal Diagram

The data collected included personal information, likes, interactions, and psychological profiles, which were then sold to Cambridge Analytica. The firm used advanced data analytics and psychographic profiling to create targeted political ads, influencing voter behavior in the 2016 U.S. elections and the Brexit campaign (Wilson, 2019). This manipulation of personal data without informed consent raised serious ethical questions about user privacy, corporate transparency, and the ethical limits of data-driven marketing strategies.

The scandal had profound consequences. Facebook faced a $5 billion fine from the Federal Trade Commission (FTC) for privacy violations, while Cambridge Analytica filed for bankruptcy in 2018. The incident led to stricter data privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union, and changes in how technology companies handle user data.

Ultimately, the Cambridge Analytica scandal not only showcased the vulnerabilities of digital ecosystems but also served as a catalyst for redefining ethical standards in technology and data governance.

Similar Cases

The Cambridge Analytica scandal is not an isolated incident in the realm of data privacy and ethical breaches in the technology sector. Similar cases include:

- **Equifax Data Breach (2017):** One of the largest data breaches in history, exposing the personal information of 147 million individuals. Equifax failed to secure sensitive information, leading to identity theft and financial losses (Henriksen, 2019). IT experts criticized Equifax's lack of encryption and delayed response, suggesting stronger data protection measures and faster public notification (Hughes, 2024).
- **Yahoo Data Breaches (2013-2014):** Exposed the data of 3 billion user accounts, including names, email addresses, and security questions. Yahoo faced criticism for delayed disclosure and poor security practices (Christodoulou & Iordanou, 2021). Cybersecurity professionals pointed out Yahoo's inadequate security infrastructure and emphasized the need for proactive threat detection (Bromwich & Pope, 2024)
- **Google+ Data Exposure (2018):** A software vulnerability exposed personal data of up to 500,000 Google+ users. Google decided to shut down the platform due to security and user engagement concerns (Bromwich & Pope, 2024). IT analysts highlighted Google's responsible approach in promptly addressing vulnerability and prioritizing user safety by discontinuing the service (Hinds et al., 2020).

Incident	Year	Affected Users	Key Issues
Cambridge Analytica	2018	87 million	Privacy violations, unethical data use
Equifax	2017	147 million	Poor encryption, delayed notification
Yahoo	2013-14	3 billion	Weak security, delayed disclosure
Google+	2018	500,000	Software vulnerability, shutdown

Table 1. Comparison of Similar Data Breaches

These cases, alongside the Cambridge Analytica scandal, highlight systemic issues in data governance, corporate accountability, and the ethical responsibilities of technology companies in protecting user data.

Key Stakeholders Involved:

- **Facebook:** The platform responsible for data security and user privacy.
- **Cambridge Analytica:** The firm that exploited the data for political and commercial gains.
- **Users:** The individuals whose data was misused, often without their knowledge.
- **Governments and Regulatory Bodies:** Such as the Federal Trade Commission (FTC) and the UK Information Commissioner's Office (ICO).
- **Political Campaigns:** Benefited from microtargeting strategies based on user data.

Technologies Involved:

- **Big Data Analytics:** Utilized by Cambridge Analytica to create psychological profiles and target ads.
- **Facebook's API:** Provided access to user data through third-party apps without adequate safeguards.
- **Psychographic Profiling Tools:** Used to analyze personality traits and influence voter behavior.

Ethical Analysis

The ethical dilemma at the core of the Cambridge Analytica Scandal revolves around the question: **"Should Facebook be held accountable for the misuse of user data by Cambridge Analytica, despite users providing indirect consent through third-party applications?"**

This question underscores the tension between user autonomy, corporate responsibility, and the ethical boundaries of data analytics in social media platforms. The scandal raised significant ethical concerns about data privacy, transparency, and the ethical responsibilities of technology companies in protecting user information from exploitation by third parties (Hughes, 2024).

Key Ethical Questions:

1. What is the ethical issue/problem in one sentence?

The primary ethical issue is whether Facebook's data-sharing policies, which allowed Cambridge Analytica to harvest user data without explicit consent, represent a violation of ethical standards in data privacy and corporate governance.

2. What facts have the most bearing on the ethical decision? Several critical facts influence the ethical analysis of this case:

- **Data Collection Mechanism:** The app **"This Is Your Digital Life"** was initially designed for **academic research**, but **data collected** through it was **sold to Cambridge Analytica** for **political purposes** (Wilson, 2019).
- **Scope of Data Breach:** While only **270,000 users** directly **consented to share data**, **Facebook's API** allowed **Cambridge Analytica** to **access data from their friends**, leading to a **breach affecting 87 million users** (Arora & Zinolabedini, 2019).
- **Regulatory Violations:** The **FTC's $5 billion fine** and the **ICO's £500,000 penalty** highlighted **legal breaches**, including **violations of data protection laws** such as the **GDPR** and **CCPA** (Boerboom, 2020).
- **Lack of User Awareness:** Many **users were unaware** that their **data was being used** for **political profiling**, raising **concerns about informed consent** (Le Jeune, 2021).

3. Are there any other external or internal factors to be considered?

The ethical evaluation of the Cambridge Analytica Scandal requires consideration of external and internal factors:

External Factors:

- **Economic Ramifications:** Facebook faced financial repercussions, including a $5 billion FTC fine and a decline in stock value (Henriksen, 2019).

- **Political Impact:** The scandal influenced key democratic processes, raising concerns about electoral integrity in the 2016 U.S. elections and the Brexit referendum (González-Pizarro et al., 2022).
- **Regulatory Environment:** The scandal accelerated the adoption of stricter data privacy laws, such as the GDPR and CCPA, highlighting the need for robust legal frameworks (Shaw, 2018).
- **Public Opinion:** The scandal led to a global outcry over data privacy, exemplified by movements like #DeleteFacebook.

Internal Factors:

- **Corporate Culture:** Facebook's internal policies prioritized business growth over user privacy, allowing third-party apps to access extensive user data with minimal oversight (Hu, 2020).
- **Data Management Practices:** Ineffective data governance within Facebook led to misuse of user data, emphasizing corporate negligence (Christodoulou & Iordanou, 2021).
- **Organizational Ethics:** The absence of robust ethical guidelines within Facebook regarding data use and sharing.

4. Who are the claimants, and in what way are you obligated to each of them?

Primary Claimants and Obligations:

- **Facebook Users:** Obligation to protect user privacy, ensure transparency, and maintain trust (Hinds et al., 2020).
- **Regulatory Bodies:** Compliance with laws such as GDPR, CCPA, and FTC guidelines, ensuring ethical data practices (Bromwich & Pope, 2024).
- **Cambridge Analytica:** Despite its role in the scandal, an ethical obligation existed to prevent data misuse through contractual safeguards (Wagner, 2021).
- **Public and Democratic Institutions:** Duty to uphold the integrity of democratic processes and prevent data-driven manipulation (Marinescu, 2024).

5. What are the operant ideals?

- **For IT Professionals:**
    - **Integrity:** Maintain ethical standards in data management.
    - **Accountability:** Acknowledge responsibility for protecting user data.
    - **Respect for Privacy:** Handling user data with explicit consent.
    - **Professionalism:** Adhering to industry standards (e.g., ACM, IEEE).

- **For Facebook (Client/Organization):**
    - **Trustworthiness:** Building user trust through transparent data practices.
    - **Compliance:** Following legal frameworks like GDPR and CCPA.
    - **User-Centric Approach:** Prioritizing data protection over profits.

6. Do any of these ideas conflict? In what order would you honor them?

Conflicting Ideals:

• **Business Growth vs. User Privacy:** Facebook's focus on data-driven business strategies conflicted with ethical obligations to protect user data (Hughes, 2024).

• **Political Influence vs. Democratic Fairness:** Cambridge Analytica's practices challenged ethical norms of fairness and transparency in elections (Shaw, 2018).

Priority Order:

1. **User Privacy and Consent:** Legal and ethical priority under GDPR and CCPA (Boerboom, 2020).
2. **Democratic Fairness:** Safeguarding electoral integrity is critical for social stability (Wilson, 2019).

3. **Regulatory Compliance:** Ensuring adherence to legal standards and ethical codes (Marinescu, 2024).
4. **Business Objectives:** While important, they must not override ethical responsibilities (Hu, 2020).

7. What are your options, and which would be favored by each affected party? (List at least three.)

Option 1: Strengthen Data Governance Policies

Description: Facebook could implement stricter data-sharing policies, including limiting third-party access to user data, enhancing consent mechanisms, and conducting regular audits of data practices (Henriksen, 2019).

Favored by:

- **Users:** As it enhances privacy and control over personal data.
- **Regulatory Bodies:** Demonstrates compliance with GDPR, CCPA, and FTC guidelines.
- **IT Professionals:** Aligns with ACM and IEEE ethical standards, promoting integrity and accountability.

Option 2: Improve User Consent Mechanisms

Description: Develop transparent consent mechanisms, providing users with detailed information about how their data will be used, and offering granular choices for sharing data with third parties (González-Pizarro et al., 2022).

Favored by:

- **Users:** Empowers them to make informed decisions about their data.
- **Regulators:** Aligns with legal requirements for informed consent under the GDPR.
- **Public and Democratic Institutions:** Helps maintain trust in social media platforms by preventing data misuse.

Option 3: Increase Transparency and Communication

Description: Facebook could introduce regular transparency reports, notifying users of how their data is being used, including disclosure of third-party data partnerships (Shaw, 2018).

Favored by:

- **Users:** Builds trust through openness and honesty.
- **Regulatory Bodies:** Shows proactive compliance with data protection standards.
- **IT Industry:** Sets a benchmark for transparency, encouraging ethical practices across the technology sector.

8. Which options could cause harm to any claimant?

- **Option 1:** Might limit the functionality of third-party apps, potentially affecting businesses that rely on Facebook's API, including small app developers (Arora & Zinolabedini, 2019).
- **Option 2:** Could lead to reduced user engagement, impacting Facebook's advertising revenue and profitability (Bromwich & Pope, 2024).
- **Option 3:** Over-communicating through transparency reports might overwhelm users with complex data policies, leading to confusion and misinterpretation (Hu, 2020).

9. Would honoring any of the ideals listed above invalidate any of your options?

- **Honoring user privacy** might **restrict business growth strategies (Option 1)**, potentially leading **to financial losses for Facebook** (Wilson, 2019).
- **Ensuring democratic fairness could limit the use of advanced data analyt**ics for **political campaigns**, affecting **business models** that **rely on political advertising** (Marinescu, 2024).
- **Transparency efforts** might **conflict with business interests** if Facebook is **forced to disclose commercially sensitive data practices** (Hinds et al., 2020).

10. Are there any rules, principles, or codes (legal, professional, organizational, or other) that automatically invalidate any of your options?

- **GDPR and CCPA** mandate **explicit consent**, supporting **Options 1 and 2** by reinforcing the need for robust consent mechanisms (Boerboom, 2020).
- **ACM and IEEE ethical codes** advocate **transparency and user autonomy**, validating **Option 3** (Henriksen, 2019).
- No **legal or ethical standards invalidate these options**, provided **implementation is aligned** with **regulatory requirements** and **ethical principles** (Christodoulou & Iordanou, 2021).

11. Which ethical theories support or reject which options? Explain.

To evaluate the ethical implications of the proposed solutions, it is essential to examine them through the lens of established ethical theories.

Consequential Theories:

• Mill's Harm Principle: Supports Options 1 and 2, as they minimize harm to user privacy and protect individuals from exploitation (Shaw, 2018).

• Utilitarianism: Favors Option 1, promoting the greatest good through enhanced data security and reducing potential harm from data misuse (Hu, 2020).

• Ethical Egoism: Might justify Facebook's original actions, prioritizing corporate gain over ethical responsibilities, but is ethically weak in balancing stakeholder interests (Hughes, 2024).

Nonconsequential Theories:

• Kant's Categorical Imperative: Strongly supports Options 1 and 2, as they respect users as ends, not merely means for data monetization (González-Pizarro et al., 2022).

• Ross's Duties: Aligns with transparency and fidelity, validating Option 3, as it maintains honesty and keeps promises to protect user data (Wagner, 2021).

12. Determine a course of action based on your analysis.

Recommended Approach:

- Implement Option 1 (Strengthen Data Governance) and Option 2 (Improve User Consent Mechanisms) as primary strategies.
- Supplement with Option 3 (Increase Transparency) to enhance user trust and comply with ethical standards.

Rationale:

- Aligns with ethical theories, such as utilitarianism and deontology, promoting user autonomy, privacy, and fairness (Henriksen, 2019).
- Addresses legal requirements, ensuring compliance with GDPR, CCPA, and ACM/IEEE codes (Hinds et al., 2020).
- Balances business interests with ethical obligations, helping Facebook rebuild its reputation while maintaining user engagement (Marinescu, 2024).

13. Defend your decision in writing to your most adamant detractor.

To the most adamant detractor, who might argue that stricter data policies could limit innovation and harm business growth, I would respond:

"The ethical responsibility of technology companies extends beyond profitability to include the protection of user privacy and the preservation of democratic integrity. By implementing stronger data governance, enhancing consent mechanisms, and increasing transparency, Facebook can demonstrate corporate accountability, restore public trust, and set a precedent for ethical practices in the digital age. This approach not only complies with global regulations but also aligns with the core values of integrity, respect, and fairness as outlined by leading ethical frameworks and industry standards."

Conclusion

The Cambridge Analytica Scandal serves as a clear example of the ethical challenges in managing user data in the information technology sector, especially within social media platforms. The scandal exposed serious ethical issues such as privacy violations, lack of transparency, and

the use of data analytics to influence political outcomes. It also showed how these practices could harm democratic institutions and reduce public trust.

This analysis used ethical theories like utilitarianism, deontology, Mill's Harm Principle, Kant's Categorical Imperative, and Ross's duties to understand the complex ethical issues related to data privacy and the duties of IT organizations. The findings showed that Facebook's weak data governance and Cambridge Analytica's unethical actions broke both ethical and legal standards. This situation highlights the need for better corporate accountability, more transparency, and stronger data protection.

The proposed actions, such as improving data governance, enhancing consent mechanisms, and boosting transparency, match well with regulatory frameworks like the GDPR and CCPA. They also align with professional standards from ACM and IEEE. These steps offer a balanced way to combine ethical practices with business stability, making sure that technology development does not ignore ethical responsibilities.

The scandal also shows the need to balance business goals with ethical duties. As technology grows, the potential of data analytics and social media influence increases, but so do the risks if not managed properly. IT professionals need to focus on ethical decision-making, maintain integrity, and protect user privacy in a world driven by data.

Moving forward, technology companies should adopt ethical frameworks that guide data management practices, support transparency, and follow global standards. By promoting trust, protecting user rights, and showing corporate responsibility, companies like Facebook can handle ethical challenges properly and make a positive impact in the digital world.

References

1. Arora, N., & Zinolabedini, D. (2019). *The Ethical Implications of the 2018 Facebook-Cambridge Analytica Data Scandal*. University of Texas Repository.
2. Boerboom, C. (2020). *Cambridge Analytica: The Scandal on Data Privacy*. Augustana Digital Commons.
3. Bromwich, R. J., & Pope, N. (2024). *Private Risk Assessment Instruments*. De Gruyter.
4. Christodoulou, E., & Iordanou, K. (2021). *Democracy Under Attack: Ethical Issues of Big Data*. Frontiers in Political Science.
5. González-Pizarro, F., Figueroa, A., & López, C. (2022). *Regional Differences in Information Privacy Concerns After the Facebook-Cambridge Analytica Data Scandal*. Springer.
6. Henriksen, E. E. (2019). *Big Data, Microtargeting, and Governmentality in Cyber-Times: The Case of the Facebook-Cambridge Analytica Data Scandal*. University of Oslo.
7. Hinds, J., Williams, E. J., & Joinson, A. N. (2020). *Privacy Concerns and Perspectives Following the Cambridge Analytica Scandal*. Elsevier.
8. Hughes, L. (2024). *The Fight for Privacy: Facebook's Failure to Secure User Data*. Shawnee Digital Commons.
9. Shaw, D. (2018). *The Cambridge Analytica Affair and Internet-Mediated Research*. EMBO Reports.
10. Wilson, R. (2019). *Cambridge Analytica, Facebook, and Influence Operations: A Case Study and Anticipatory Ethical Analysis*. ProQuest.