Case Study Report

Facebook–Cambridge Analytica Data Privacy Scandal (2018)

An Analysis of Data Privacy, Corporate Accountability, and Global Impact

Prepared by: *Tanvir Ahmed*

Date: *27 Aug 2025*

Executive Summary

In 2018, Facebook faced one of the most significant data privacy scandals in digital history when Cambridge Analytica, a political consulting firm, harvested data from up to **87 million users** without explicit consent. The information was exploited for psychographic profiling and political advertising, raising global concerns about privacy, transparency, and democratic integrity.

This report examines the scandal in detail, focusing on the **background, nature, impact, ethical/legal dimensions, and lessons learned**. It also includes visual data representations (charts and timelines) for clarity.

Case Study Report

Dedication

This case study is dedicated to everyone who values the right to privacy in the digital age. It is also dedicated to those individuals, such as whistleblowers and investigative journalists, whose efforts brought the Facebook–Cambridge Analytica scandal to light. Their work serves as a reminder that accountability and transparency are vital in protecting society from the misuse of technology.

Preface

The Facebook–Cambridge Analytica scandal of 2018 was a pivotal moment in the global discussion on data privacy and the ethical use of digital platforms. This report seeks to provide a comprehensive analysis of the scandal, covering its background, technical aspects, impact, ethical and legal considerations, and lessons learned.

The case study has been structured in a professional format to serve as both an academic analysis and a portfolio example of research and reporting skills. Visual elements, such as charts, graphs, and timelines, are included to illustrate the scale of the incident and its consequences more clearly.

By examining this case, the report aims to highlight the challenges faced by companies, regulators, and society at large in addressing issues of digital governance and accountability.

Acknowledgements

I would like to acknowledge the contributions of investigative journalists from *The Guardian* and *The New York Times*, whose groundbreaking reporting first brought the scope of the scandal to global attention.

I also extend gratitude to Christopher Wylie, the whistleblower whose courage and testimony exposed critical details of Cambridge Analytica's practices.

Additionally, appreciation is owed to the academic community, regulators such as the Federal Trade Commission, and the European Union for their detailed analyses and enforcement actions, which provide the foundation for understanding the scandal's lasting impact.

Case Study Report

How to Use This Report

This case study report is designed for students, professionals, and policymakers interested in understanding the implications of large-scale data privacy scandals. It may be used as:

- **An academic reference:** The report's structure, analysis, and references make it suitable for study in fields such as information systems, business ethics, and law.
- **A professional portfolio piece:** Its design and presentation demonstrate research, analytical, and reporting skills.
- **A policy and practice resource:** The lessons learned provide actionable insights for corporations, regulators, and individuals seeking to improve data privacy practices.

The report can be read in full for a comprehensive understanding, or by individual sections for targeted learning (e.g., ethical analysis, impact assessment, or technical background). Visual data elements supplement the written content for a more engaging experience.

About the Author

Tanvir Ahmed is a cybersecurity analyst, ethical hacker, and Linux enthusiast dedicated to advancing the field of information security. With professional training and global certifications from institutions such as **Google, Cisco, Harvard, Microsoft, IBM, and CompTIA**, he has developed deep expertise in **ethical hacking, penetration testing, network defense, and digital forensics**.

Currently pursuing a **Higher National Diploma (HND) in Cybersecurity** at Regent Middle East, Dubai, Tanvir combines academic knowledge with real-world experience gained through internships and hands-on projects and freelance bug buntry. His work includes designing **AI-powered incident response systems**, building **secure encryption frameworks**, and developing **malware detection tools** that leverage machine learning.

He is proficient in a wide range of tools and technologies, including **Kali Linux, Ubuntu, Nmap, Wireshark, Burp Suite, Metasploit, Hashcat, Splunk, ELK Stack**, and programming languages such as **Python, PHP, JavaScript, Ruby, C++, and React, C**.

Beyond technical expertise, Tanvir is passionate about **teaching, mentoring, and sharing knowledge**.

He strongly believes in the philosophy:

"Knowledge should empower, not destroy."

Case Study Report

Table of Contents

Case Study Report

Case Study Report

1. Introduction

In 2018, Facebook faced one of the largest data privacy scandals in modern digital history, when it was revealed that Cambridge Analytica, a political consulting and data analytics firm, had improperly accessed personal data from millions of Facebook users without their explicit consent. The incident raised global concerns about data security, digital ethics, and corporate accountability in the age of social media.

2. Background

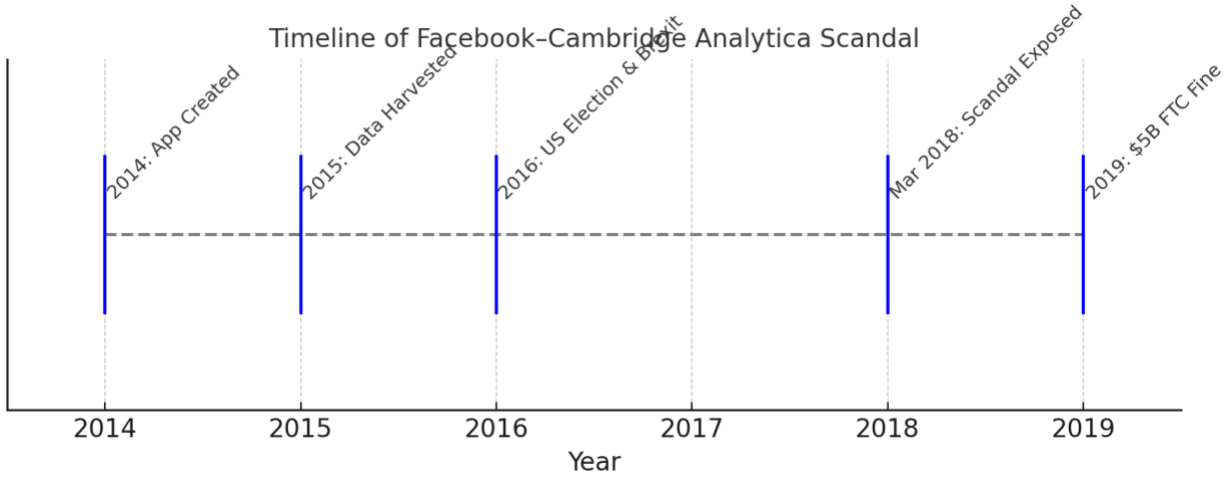
Company Involved

- **Facebook (Meta Platforms, Inc.)**: At the time of the incident, Facebook was the world's largest social media platform, with over 2 billion active users. Its Open Graph API allowed third-party developers to access user data with limited oversight, creating a vulnerability that was exploited.

Third-Party Actor

- **Cambridge Analytica**: A UK-based political data analytics and consulting firm, affiliated with the SCL Group. Known for its work in psychological profiling and microtargeting, Cambridge Analytica claimed to influence voter behavior using psychographic data.

Timeline of Events



Case Study Report

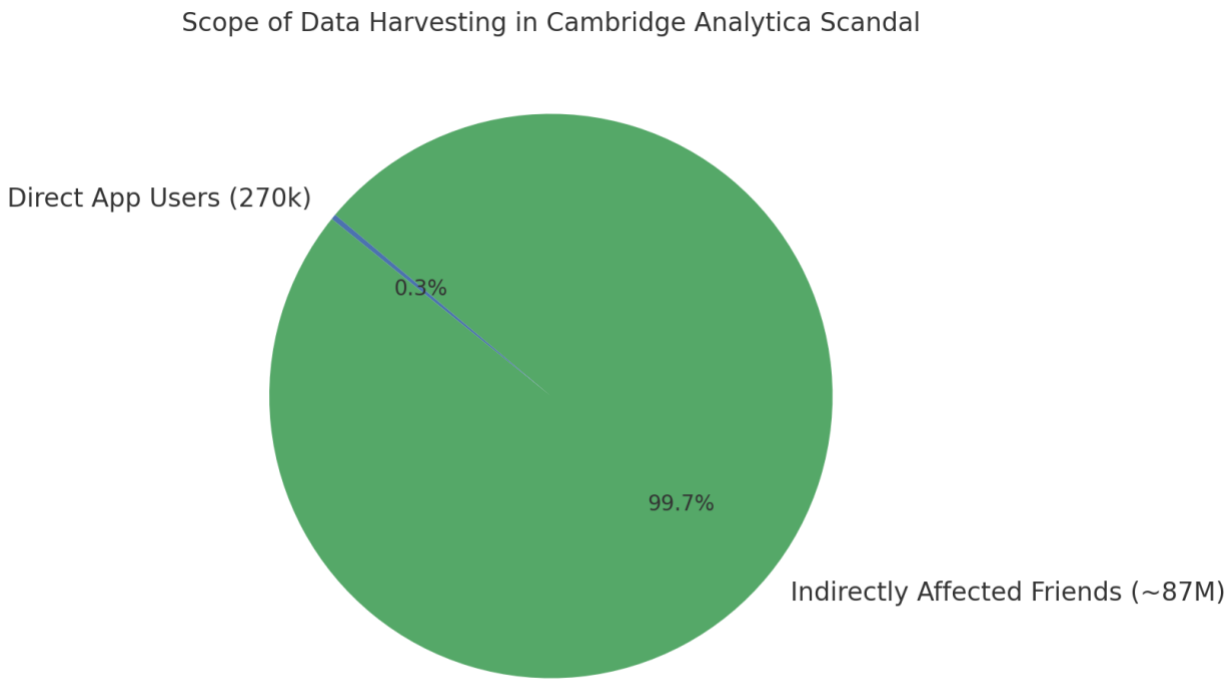
Year	Event
2013	Aleksandr Kogan, a Cambridge University researcher, founded Global Science Research (GSR) and partnered with Cambridge Analytica.
2014	Kogan developed a Facebook app called **"This Is Your Digital Life"**, a personality quiz that collected user data under the guise of academic research.
2014–2015	The app harvested data from approximately **270,000 users**, but due to Facebook's API permissions, it also accessed data from **up to 87 million users**, including friends of quiz participants.
2015	Facebook updated its API to restrict third-party access to friends' data, but the harvested data had already been transferred to Cambridge Analytica.
2016	Cambridge Analytica allegedly used the data to support political campaigns, including **Ted Cruz's** and **Donald Trump's** presidential bids, as well as the **Brexit Leave.EU** campaign.
March 2018	Whistleblower **Christopher Wylie**, a former Cambridge Analytica employee, revealed the data misuse to **The Guardian** and **The New York Times**, triggering global outrage.
April 2018	Facebook CEO **Mark Zuckerberg** testified before the U.S. Congress, acknowledging the company's failure to protect user data.
May 2018	Cambridge Analytica filed for bankruptcy amid mounting legal and public pressure.
July 2019	The **U.S. Federal Trade Commission (FTC)** fined Facebook **$5 billion**, the largest privacy-related fine in history at the time.
October 2019	The **UK Information Commissioner's Office (ICO)** fined Facebook **£500,000** for exposing users to "serious risk of harm".

3. Nature of the Scandal

3.1 Scope of the Breach

The breach was not a traditional cybersecurity incident involving malware or unauthorized system access—it was a **data exploitation scandal** rooted in weak API governance and deceptive data collection practices.

Case Study Report



- **App Involved**: "This Is Your Digital Life," created by Cambridge academic Aleksandr Kogan through Global Science Research (GSR).
- **User Base**: ~270,000 users voluntarily downloaded the app and completed personality quizzes.
- **Facebook API Loophole**: At the time, Facebook's Open Graph API allowed apps to access not only the data of consenting users, but also the data of their **entire friend networks**—without those friends' knowledge or consent.
- **Total Reach**: This cascading access led to the harvesting of data from **up to 87 million users globally**.

Types of Data Collected

- **Demographics**: Age, gender, location, language.
- **Behavioral Data**: Facebook "likes," page interactions, and activity logs.
- **Social Graph**: Friend connections, mutual interests, and network structure.
- **Psychographic Attributes**: Personality traits, political leanings, emotional triggers—derived using psychological models like OCEAN (Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism).

This data was not encrypted or anonymized in a way that prevented individual profiling. It was stored and processed in violation of Facebook's policies, and later weaponized for political influence.

Case Study Report

3.2 Use of Data

Cambridge Analytica's core business model revolved around **psychographic microtargeting**—a technique that goes beyond demographics to predict and influence behavior based on personality and psychological traits.

🎯 Political Applications

- **2016 U.S. Presidential Election**:
  - Data was allegedly used to support **Donald Trump's campaign**.
  - Voters were segmented into psychological categories (e.g., neurotic, agreeable, skeptical) and targeted with tailored political ads designed to evoke emotional responses.
  - Ads were deployed across Facebook, YouTube, and other platforms using dark posts (non-public ads visible only to targeted users).
- **2016 Brexit Referendum**:
  - Cambridge Analytica was linked to the **Leave.EU** campaign, although official investigations found limited direct involvement.
  - Nonetheless, the scandal raised concerns about foreign influence and unregulated data use in democratic processes.

Psychological Manipulation

- Ads were crafted to exploit cognitive biases:
  - Fear-based messaging for neurotic profiles.
  - Patriotism and tradition for conservative profiles.
  - Disruption and change for openness-driven profiles.

This marked a shift from **mass communication** to **individual persuasion**, blurring ethical lines between marketing and manipulation.

3.3 Disclosure and Fallout

The scandal broke in **March 2018**, when:

- **Christopher Wylie**, a former Cambridge Analytica employee, leaked internal documents and gave interviews to *The Guardian* and *The New York Times*.
- Wylie described the operation as "a full-service propaganda machine," revealing how data was weaponized to sway elections.

Key Revelations

- Facebook had known about the data misuse since **2015**, but failed to notify affected users or verify that Cambridge Analytica deleted the data as promised.
- The breach was not disclosed until media investigations forced public accountability.
- Facebook CEO **Mark Zuckerberg** testified before U.S. Congress in **April 2018**, acknowledging the platform's failure to protect user privacy.

Public Reaction

- The hashtag **#DeleteFacebook** trended globally.
- Facebook's stock dropped significantly.
- Governments worldwide began drafting stricter data protection laws.

4. Technical Aspects of Data Collection

4.1 Facebook's Open Graph API (Pre-2014)

The **Open Graph API**, launched in 2010, was designed to allow third-party developers to integrate deeply with Facebook's social graph. It enabled apps to access user data and interact with Facebook features like likes, shares, and friend lists.

Key Features Before 2014

- **OAuth-based permissions**: Users granted apps access to their data via login prompts.
- **Extended permissions**: Apps could request access to friends' data—without those friends ever interacting with the app.
- **Default scope**: Included profile info, likes, photos, check-ins, and even chat status.
- **Graph structure**: Facebook modeled relationships as nodes (users) and edges (friendships), allowing traversal across the graph.

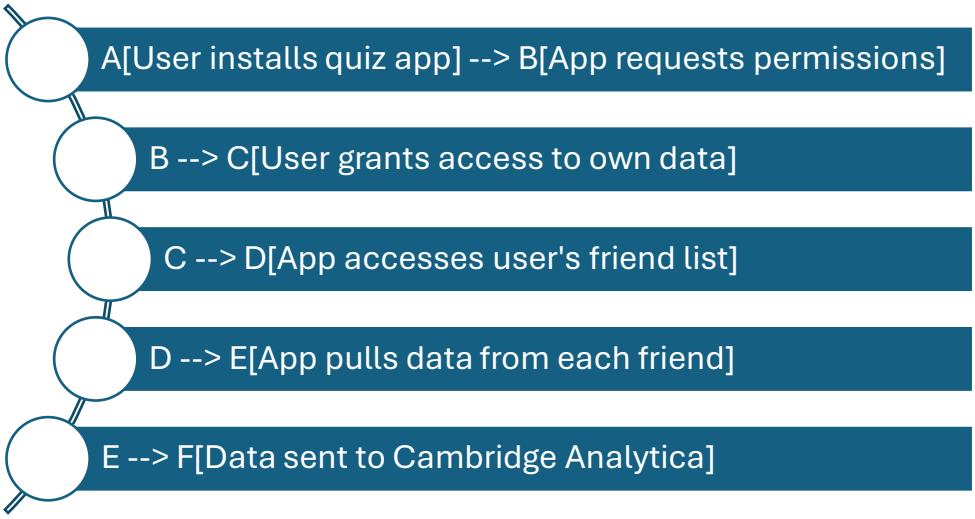
This design prioritized developer flexibility over user privacy. It treated **friend data as an extension of the user's consent**, which created a massive surface for indirect data harvesting.

4.2 How "Friend Data" Was Exposed

The app "This Is Your Digital Life" exploited this architecture to harvest data far beyond its direct user base.

Step-by-Step Breakdown

Case Study Report



What Was Collected from Friends

- **Name, gender, location**
- **Likes and interests**
- **Relationship status**
- **Education and work history**
- **Political and religious views**
- **Social connections and group memberships**

None of these friends had installed the app or given explicit consent. The API treated them as passive data sources.

4.3 Facebook's Enforcement Failures

Despite knowing about the abuse as early as **2015**, Facebook failed to take meaningful action until public pressure mounted in **2018**.

Key Failures

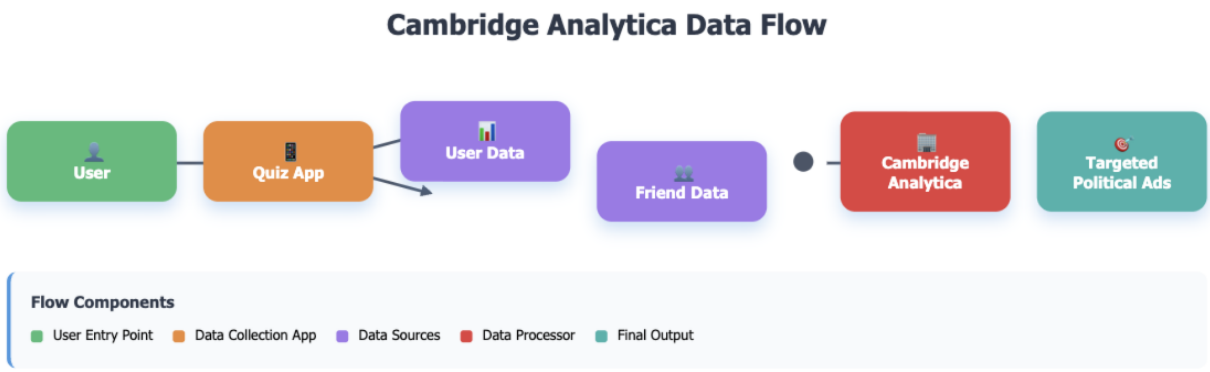
- **Lack of audit trails**: Facebook did not proactively monitor how third-party apps used data post-collection.
- **No real-time anomaly detection**: There were no automated systems to flag suspicious data access patterns (e.g., exponential friend data harvesting).
- **Weak contractual enforcement**: Facebook relied on developers to self-certify compliance with data deletion requests.
- **Delayed API updates**: Although Graph API v2.0 (2014) restricted friend data access, older apps were grandfathered in until **April 30, 2015**, giving them a full year to continue harvesting.

Case Study Report

Strategic Oversight Gaps

- Facebook prioritized **platform growth and developer engagement** over privacy safeguards.
- Internal documents later revealed that Facebook executives were aware of the risks but chose not to disrupt app ecosystems.

Summary Diagram: Data Flow & Exploitation



5. Impact

5.1 Impact on Users

Privacy Breach

- **Nature of Violation**: The personal data of up to **87 million Facebook users** was harvested without informed consent. This included not only direct quiz participants but also their friends, whose data was accessed via Facebook's permissive API.
- **Depth of Exposure**: Data points ranged from basic demographics to psychographic profiles, enabling highly granular behavioral predictions.
- **Rights Infringement**: This violated fundamental privacy rights under emerging global standards, such as the principles later enshrined in the **GDPR** — specifically, the right to be informed, the right to consent, and the right to restrict processing.

Loss of Trust

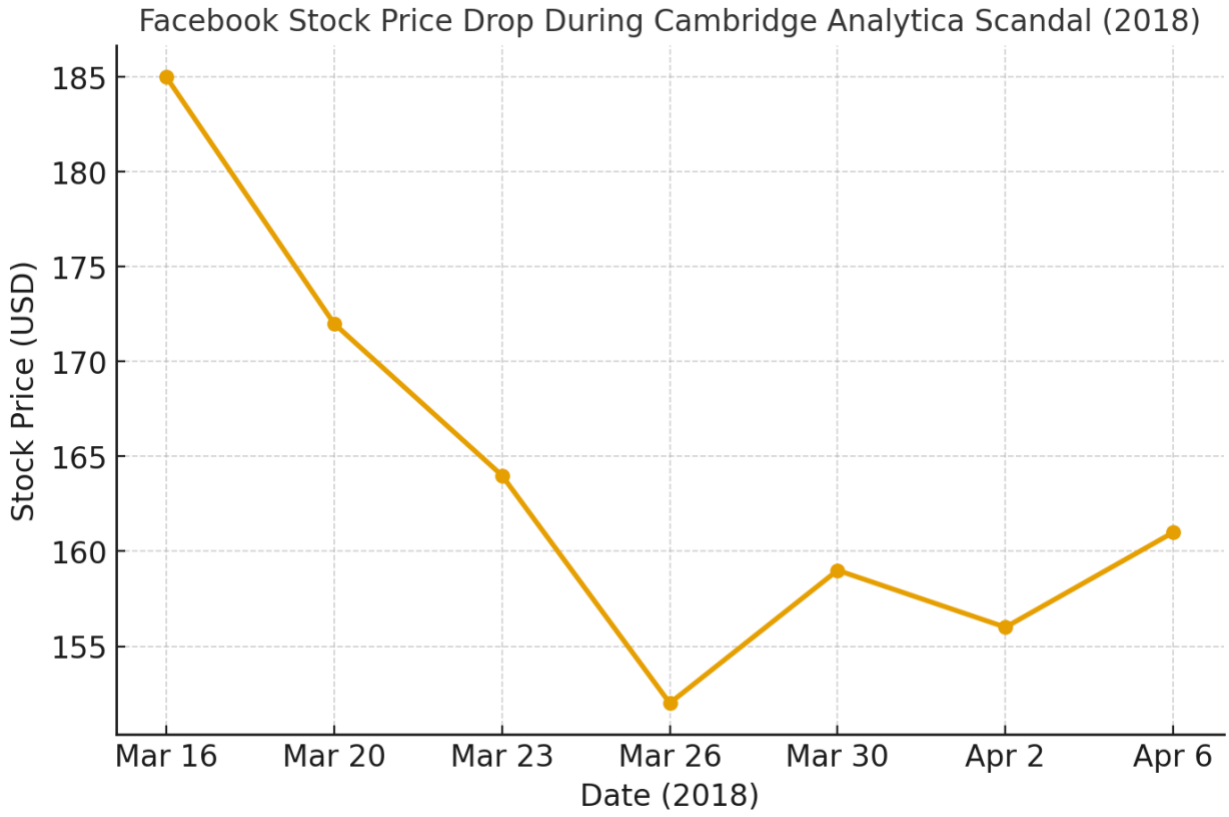
Case Study Report

- **User Sentiment Shift**: The scandal triggered a **global trust crisis**. Many users felt betrayed, believing Facebook had failed in its duty of care.
- **#DeleteFacebook Movement**: This grassroots campaign encouraged users to deactivate accounts, symbolizing a broader rejection of opaque data practices.
- **Behavioral Change**: Surveys post-scandal showed a measurable decline in user engagement and a rise in privacy-conscious behaviors, such as adjusting settings, limiting app permissions, and using privacy-focused platforms.

5.2 Impact on Facebook

Financial Repercussions

- **Market Capitalization Drop**: Within days of the scandal breaking in March 2018, Facebook's market value fell by nearly **$100 billion**, reflecting investor fears over regulatory risk, user attrition, and reputational damage.



- **Advertising Concerns**: Advertisers temporarily paused campaigns, wary of brand association with a platform under intense scrutiny.

Legal Penalties

Case Study Report

- **FTC Fine (2019)**: The U.S. Federal Trade Commission imposed a **$5 billion penalty** — the largest privacy-related fine in history at that time — for violating a 2011 consent decree that required Facebook to protect user data and be transparent about sharing practices.
- **Other Jurisdictions**: The UK's Information Commissioner's Office fined Facebook **£500,000** (the maximum under pre-GDPR law), citing "serious breaches" of data protection principles.

Reputational Harm

- **Congressional & EU Hearings**: CEO Mark Zuckerberg's testimony before the U.S. Congress and the European Parliament became defining moments, symbolizing the global backlash against Big Tech.
- **Public Perception**: Facebook's brand shifted from an innovative social connector to a cautionary tale of unchecked data monetization.

5.3 Impact on Society and Regulation

Political Integrity

- **Election Fairness Concerns**: The scandal amplified fears that **psychographic microtargeting** could distort democratic processes by delivering manipulative, unverified, and hyper-personalized political messages.
- **Foreign Interference Risks**: It highlighted how social media platforms could be exploited by both domestic and foreign actors to influence public opinion at scale.

Regulatory Shifts

- **GDPR Acceleration**: Although the EU's General Data Protection Regulation was already in development, the scandal heightened urgency for enforcement and public awareness.
- **Global Ripple Effect**: Inspired similar laws, such as the **California Consumer Privacy Act (CCPA)**, Brazil's **LGPD**, and India's draft data protection bill.
- **Political Ad Transparency**: Sparked new rules requiring disclosure of political ad sponsors and targeting criteria.

Corporate Accountability

- **Governance Debate**: The incident became a case study in the dangers of self-regulation for tech giants.
- **Industry Response**: Other companies, including Apple and IBM, publicly called for stronger privacy laws.
- **Shift in Business Models**: The scandal forced a re-examination of ad-driven revenue models that depend on extensive personal data collection.

Case Study Report

Strategic Insight for Cybersecurity & Governance

From a cybersecurity governance perspective, the impact underscores:

- The **interdependence of technical safeguards and ethical oversight**.
- The **need for proactive compliance** with emerging privacy laws, not reactive damage control.
- The **business risk of privacy negligence**, where reputational harm can outweigh immediate legal penalties.

6. Ethical and Legal Considerations

6.1 Ethical Concerns

Consent and Autonomy

- **Core Issue**: Users who installed the "This Is Your Digital Life" app consented to share their own data, but **were never informed** that their friends' data would also be harvested.
- **Breach of Autonomy**: Friends of quiz participants had **no opportunity to opt in or out**, stripping them of control over their personal information.
- **Ethical Principle Violated**: The **right to informed consent**, a cornerstone of both medical ethics and digital privacy, was ignored.
- **Why It Matters**: Without informed consent, individuals cannot make meaningful choices about their participation in data-driven systems — undermining personal agency.

Transparency

- **Facebook's Role**: The platform failed to clearly communicate:
  - What data was being collected.
  - How it would be used.
  - Who it would be shared with.
- **Delayed Disclosure**: Facebook learned of the misuse in **2015** but did not inform affected users until **2018**, after media exposure.
- **Ethical Principle Violated**: **Duty of candor** — organizations have a moral obligation to be open and honest about risks and breaches.

Manipulation

- **Psychographic Targeting**: Data was used to craft **emotionally manipulative political ads** tailored to individual psychological profiles.
- **Democratic Risk**: This practice blurred the line between persuasion and coercion, potentially **distorting electoral outcomes**.

Case Study Report

- **Ethical Principle Violated**: **Respect for autonomy in decision-making** — individuals were nudged or pressured toward political choices without realizing they were being targeted in this way.

6.2 Legal Dimensions

U.S. Regulation

- **FTC Enforcement**: The **$5 billion fine** in 2019 was for violating a **2011 consent decree** that required Facebook to:
  - Obtain clear user consent before sharing data.
  - Maintain a comprehensive privacy program.
- **Significance**: This was the largest privacy-related fine in U.S. history at the time, signaling that regulators were willing to impose **record-breaking penalties** for systemic privacy failures.

European Regulation

- **GDPR Context**: The **General Data Protection Regulation** came into force in May 2018, shortly after the scandal broke.
- **Key Protections Relevant to the Case**:
  - **Right to be informed**: Users must know how their data is collected and used.
  - **Right to consent**: Consent must be explicit, informed, and freely given.
  - **Right to erasure**: Users can request deletion of their data.
- **UK ICO Fine**: Facebook was fined **£500,000** — the maximum under pre-GDPR law — for exposing users to "serious risk of harm."

Global Precedent

- **Catalyst for Reform**: The scandal accelerated the creation and enforcement of privacy laws worldwide, including:
  - **California Consumer Privacy Act (CCPA)** in the U.S.
  - **Lei Geral de Proteção de Dados (LGPD)** in Brazil.
  - Draft **Personal Data Protection Bill** in India.
- **Political Ad Transparency**: Many jurisdictions introduced rules requiring disclosure of political ad sponsors and targeting criteria.
- **Corporate Governance Shift**: Boards and executives began treating **data ethics** as a core compliance and reputational risk area.

6.3 Legal Analysis — Intersection of Ethics and Law

- **Ethics vs. Compliance**: While Facebook may have technically complied with its own (flawed) policies at the time, it **failed ethically** by not safeguarding user autonomy and transparency.

Case Study Report

- **Regulatory Lag**: The case exposed how **laws often trail behind technology**, allowing harmful practices to persist until public outrage forces change.
- **Long-Term Implications**:
  - Strengthened **cross-border cooperation** between regulators.
  - Increased **corporate liability** for third-party misuse of data.
  - Elevated **data protection officers (DPOs)** and privacy teams to strategic roles within organizations.

Ethical–Legal Comparative Analysis

Category	Ethical Concern	Legal Framework / Response	Global / Long-Term Implications
Consent & Autonomy	Users and their friends' data were harvested without explicit permission, violating the right to informed consent.	**FTC (U.S.)** – 2011 consent decree required clear, affirmative user consent before data sharing; breached by Facebook. **GDPR (EU)** – Requires explicit, informed, freely given consent for each purpose of data processing.	Set a precedent for stronger consent rules worldwide (e.g., CCPA in California, LGPD in Brazil, India's DPDP Bill). Increased global emphasis on opt-in models over opt-out defaults.
Transparency	Facebook failed to clearly inform users about what was collected, how it was used, and by whom. Disclosure was delayed for years.	**FTC (U.S.)** – Obligation to be truthful about data collection and sharing practices. **GDPR (EU)** – "Right to be informed" obligates timely, clear disclosure of data handling.	Drove legislative focus on mandatory breach notifications and plain-language privacy policies. Sparked ad transparency requirements in political campaigns.
Manipulation & Integrity of Decision-Making	Psychographic targeting used to influence voter behavior, potentially undermining democratic processes.	No explicit global law banning psychographic political targeting at the time. GDPR limits automated profiling with significant effects on individuals. Some national election laws (e.g., Canada, France) have since tightened rules on digital political advertising.	Initiated debate on whether manipulative targeting should be regulated or banned outright. Encouraged adoption of political

Case Study Report

Category	Ethical Concern	Legal Framework / Response	Global / Long-Term Implications
			ad registries and oversight mechanisms.
Corporate Accountability	Failure to oversee third-party app compliance; weak enforcement of data use agreements.	**FTC (U.S.)** – Holds companies accountable for third-party misuse if within scope of consent decree. **GDPR (EU)** – Data controllers remain responsible for compliance of processors/subcontractors.	Triggered corporate governance reforms: appointment of Data Protection Officers (DPOs), mandatory third-party risk audits, and increased board-level oversight of privacy.

7. Lessons Learned

7.1 Consent & Transparency — *The Foundation of Trust*

- **Informed Consent**:
  - Data collection must be based on **explicit, informed, and freely given consent**.
  - Consent requests should be **clear, concise, and specific** — avoiding vague "catch-all" terms buried in lengthy privacy policies.
  - Users must know **exactly** what data is collected, **why** it's collected, **how** it will be used, and **who** it will be shared with.
- **Transparency in Practice**:
  - Platforms should provide **real-time dashboards** showing active data-sharing permissions and allow users to revoke them instantly.
  - Breach notifications must be **timely and detailed**, outlining the scope, risks, and remediation steps.

7.2 Third-Party Accountability — *Closing the Backdoor*

- **Stricter Oversight of External Apps**:
  - Platforms must **vet developers** before granting API access, including background checks and compliance certifications.
  - Implement **least-privilege access** — apps should only access the minimum data necessary for their function.
- **Continuous Auditing**:
  - Automated monitoring systems should flag unusual data access patterns (e.g., mass friend data harvesting).

    - Regular compliance reviews and **mandatory deletion certifications** for unused or expired data.
- **Enforcement Mechanisms**:
    - Immediate suspension of non-compliant apps.
    - Legal action against developers who misuse data.

7.3 Stronger Governance — *From Self-Regulation to Enforceable Law*

- **Government Enforcement**:
    - Privacy laws must include **meaningful penalties** that outweigh the financial benefits of non-compliance.
    - Regulators should have **real-time audit powers** for high-risk platforms.
- **Global Harmonization**:
    - Cross-border data flows require **international cooperation** to prevent jurisdictional loopholes.
    - Aligning standards like **GDPR**, **CCPA**, and **LGPD** can create a unified privacy baseline.

7.4 Corporate Accountability — *Owning the Risk*

- **Responsibility Beyond Compliance**:
    - Companies must treat privacy as a **core business value**, not just a legal checkbox.
    - Establish **Data Ethics Boards** to review high-impact projects.
- **Security-by-Design**:
    - Embed privacy and security controls into product architecture from the start.
    - Conduct **Privacy Impact Assessments (PIAs)** before launching new features.

7.5 User Empowerment — *Raising Digital Literacy*

- **Awareness Campaigns**:
    - Public education on how data is collected, traded, and used for targeting.
    - Teach users to recognize manipulative content and adjust privacy settings.
- **Control Tools**:
    - Easy-to-use privacy settings with **one-click opt-outs**.
    - Clear explanations of the trade-offs between personalization and privacy.
- **Collective Action**:
    - Movements like **#DeleteFacebook** show that user behavior can pressure companies into reform.

7.6 Summary Table — Lessons by Stakeholder

Case Study Report

Stakeholder	Key Lesson	Actionable Measures
Companies	Corporate Responsibility	Vet third-party apps, embed privacy-by-design, conduct regular audits, enforce strict API controls.
Regulators	Laws & Enforcement	Impose meaningful penalties, mandate breach notifications, harmonize global privacy laws.
Users	Digital Literacy & Privacy Awareness	Learn privacy settings, understand consent, participate in awareness campaigns, demand transparency.

8. Conclusion

The Facebook–Cambridge Analytica scandal was a watershed moment in the history of digital privacy. It revealed how personal data could be weaponized for political gain and underscored the weaknesses of existing regulatory frameworks. While Facebook has since implemented stronger data protection policies, the case continues to serve as a cautionary tale of the ethical, legal, and societal challenges posed by big data and social media.

As technology continues to evolve, the lessons from this scandal highlight the importance of balancing innovation with privacy, transparency, and accountability. The incident remains a pivotal case study for policymakers, businesses, and academics alike in the ongoing global discourse on digital ethics and governance.

9. References

- Cadwalladr, C., & Graham-Harrison, E. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian.
- Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018). *How Trump Consultants Exploited the Facebook Data of Millions*. The New York Times.
- Federal Trade Commission (2019). *FTC Imposes $5 Billion Penalty on Facebook for Privacy Violations*.
- European Commission (2018). *General Data Protection Regulation (GDPR)*.
- Wylie, C. (2019). *Mindf*ck: Cambridge Analytica and the Plot to Break America*. Random House.