Case Study: Inappropriate Use of Surveys

Introduction

Surveys are commonly used tools for collecting data in research, marketing, and social media contexts. However, when misused, they can lead to significant ethical, legal, social, and professional consequences. One of the most notorious examples is the Cambridge Analytica scandal, where surveys were employed to manipulate personal data for political purposes. This report explores the misuse of surveys in that case and other similar instances, analyzing their broader implications.

Cambridge Analytica and Facebook Surveys (2018)

In 2018, Cambridge Analytica, a political consultancy firm, was implicated in a major data privacy scandal involving the misuse of Facebook data. A third-party app, developed by researcher Dr. Aleksandr Kogan, distributed a seemingly harmless personality quiz titled “thisisyourdigitallife.” Though only 270,000 users completed the survey, the app harvested data from users’ Facebook friends without their knowledge or consent, amassing personal data from over 87 million users.

This data was used to construct psychographic profiles and target individuals with personalized political advertising, allegedly influencing major democratic processes such as the Brexit referendum and the 2016 U.S. presidential election. The data was not only collected without informed consent but was also shared and used for purposes entirely unrelated to the original survey.

Other Examples of Inappropriate Survey Use

1. TikTok Personality Quizzes

On TikTok, personality quizzes often go viral, appearing as harmless entertainment. However, some of these quizzes collect device data, track user behavior, or request access to contacts. This information can then be used for targeted advertising or even sold to third parties. Many users, especially minors, are unaware of the privacy risks involved.

2. Fake COVID-19 Health Surveys

During the COVID-19 pandemic, cybercriminals distributed fake health surveys impersonating authorities like the WHO or NHS. These surveys were used to gather sensitive health and personal information from respondents, which was later used in phishing attacks or sold on illicit marketplaces. Victims were often left vulnerable to identity theft and fraud.

Impact Analysis

Ethical Impact

- **Lack of Informed Consent:** Participants were misled about how their data would be used.
- **Deception:** Surveys presented themselves as tools for fun or public service, hiding commercial or political motives.
- **Breach of Trust:** Violated the ethical principles of transparency and respect for persons.

Social Impact

- **Public Mistrust:** Users became wary of digital platforms and online surveys.
- **Manipulation of Public Opinion:** Targeted ads contributed to political polarization and social division.
- **Vulnerable Populations Exploited:** Specific demographics were targeted based on emotional or psychological vulnerabilities.

Legal Impact

- **Violation of Privacy Laws:** The Cambridge Analytica case breached the UK Data Protection Act and, by extension, the EU GDPR.
- **Regulatory Action:** Facebook faced a $5 billion fine from the U.S. Federal Trade Commission (FTC), the largest ever at the time for privacy violations.
- **Strengthened Legislation:** Incidents led to global discussions about digital rights and stricter data regulations.

Professional Impact

- **Professional Misconduct:** Developers and researchers failed to adhere to professional standards of data handling.

- **Reputational Damage:** Facebook, Cambridge Analytica, and associated academic institutions suffered significant reputational harm.

- **Responsibility of Tech Workers:** Reinforced the importance of ethical responsibility among developers, data scientists, and researchers.

Conclusion

These cases demonstrate the dangers of misusing surveys in the digital age. What may appear as an innocent data collection tool can be repurposed to violate privacy, manipulate opinion, and cause widespread harm. Ethical, legal, and professional accountability is essential to ensure trust and integrity in data-driven practices. Moving forward, all stakeholders — from developers to platform owners — must prioritize transparency, consent, and responsible data use.