SRINIVAS UNIVERSITY
INSTITUTE OF ENGINEERING & TECHNOLOGY
Srinivas Campus,Mukka,Surathkal,Mangaluru-574 146

"A Case Study on Data Misuse — Analysis, Governance, and Ethical Insights"

AN GROUP TASK

Submitted by:

NAME	TOTADA CHANDRASHEKAR
USN	01SU23CS214

Subject:

Fundamentales of AI and ML

Subject code:

24SBT110

Submitted to:

Prof,Mahesh Kumar

Academic Year 2026

Introduction

- **Data is a highly valuable asset in today's digital age.**
- **Social media platforms collect vast personal information, including:**
  - **Demographics (age, location, gender) o Interests and browsing habits o Social connections and interactions**
- **While data can improve services and innovation, it carries significant ethical responsibilities.**
- **Case focus: SocialConnect, a social media platform, had user data exploited by a third-party political consulting firm for targeted election campaigns.**
- **Key ethical issues include: o Lack of informed consent o Privacy violations o Use of personal data to influence political behavior**
- **Purpose of the study:**
  - **Analyze how better governance and ethical practices could prevent misuse o Provide practical lessons for organizations handling sensitive data**

Case Background

- **Platform: SocialConnect – a popular social media platform with millions of users.**
- **Third-Party App: "Personality Quiz" offered by a political consulting firm, VoteMax.**
- **Data Collected:**
  - **Users' personal information (name, age, location) o Friends' data without their knowledge o Likes, posts, and browsing behavior**
- **Purpose of Data Collection: Marketed as a fun quiz, but data was used to:**
  - **Build voter profiles**
  - **Target personalized political advertisements**
- **Method of Misuse:**

- **Users unknowingly granted permission for both their data and friends' data to be accessed o VoteMax analyzed this data to influence political opinions**

- **Outcome:**
  - **Massive exposure of personal data o Users unaware of the real purpose of the app o Platform reputation and trust severely impacted**
- **Regulatory Impact: Potential violation of privacy laws (e.g., GDPR, CCPA)**
- **Societal Concerns: Raised debates about ethics in digital political campaigns**
- **Lessons Highlighted: Showcases the risks of weak oversight and lack of transparency in data sharing**

Ethical Issues

- **Lack of Informed Consent:**
  - **Users were unaware that their data, and their friends' data, would be collected for political purposes.**
- **Third-Party Risk:**
  - **SocialConnect failed to properly audit or monitor third-party apps accessing user data.**
- **Manipulation of Behavior:**
  - **Personal data was used to influence political opinions, raising concerns about autonomy and fairness.**
- **Transparency Failure:**
  - **Users were not informed about how their data would be used, violating trust and privacy principles.**
- **Privacy Violations:**
  - **Sensitive information, such as user connections and interests, was shared without explicit permission.**
- **Accountability Gap:**
  - **No clear responsibility or governance structure existed to prevent misuse of data.**
- **Potential Legal Breach:**
  - **Actions could violate data protection laws such as GDPR and CCPA.**

Consequences

- **Loss of User Trust:**
  - **Users felt their personal information was exploited, damaging SocialConnect's reputation.**
- **Public Backlash:**
  - **Media coverage and social outrage highlighted the misuse of personal data.**
- **Regulatory Scrutiny:**
  - **Potential fines and legal actions under data protection laws (e.g., GDPR, CCPA).**
- **Political Controversy:**
  - **Raised ethical debates about the influence of social media on elections.**
- **Financial Impact:**
  - **Possible loss of users and advertisers due to damaged credibility.**
- **Operational Challenges:**
  - **Increased pressure to implement stricter data governance and monitoring systems.**
- **Long-term Ethical Implications:**
  - **Highlighted the need for stronger corporate responsibility in handling sensitive data.**
- **Erosion of Social Media Integrity:**
  - **Users may become skeptical of platforms, reducing engagement and participation.**
- **Potential Industry-Wide Effects:**
  - **Other companies may be forced to adopt stricter policies due to regulatory or public pressure.**
- **Reputational Damage for Third Parties:**
  - **VoteMax's credibility and trustworthiness also suffered due to unethical practices.**

Preventive Measures / Ethical Practices

- **Stronger Consent Mechanisms:**
  - **Implement clear, granular consent for all types of data collected.**
  - **Notify users when their friends' data may also be accessed.**
- **Robust Third-Party Auditing:**
  - **Require apps to undergo security and ethical audits before accessing user data.**
  - **Continuously monitor third-party apps for compliance and misuse.**
- **Data Minimization Principles:**
  - **Collect only data necessary for the app's stated purpose. o Avoid sharing sensitive data unless absolutely required.**
- **Transparency and Accountability:**
  - **Maintain public logs of third-party data access.**
  - **Allow users to view, export, and delete their data easily.**
- **Internal Ethical Review Board:**
  - **Evaluate high-risk data requests for potential societal harm before approval. o Ensure company decisions consider both legal and ethical implications.**
- **Regular Employee Training:**
  - **Train staff on ethical data handling, privacy laws, and responsible governance.**
- **Strong Regulatory Compliance:**
  - **Align company policies with GDPR, CCPA, and other relevant privacy regulations.**
- **User Awareness Campaigns:**
  - **Educate users about data sharing risks and safe online practices.**

Conclusion

- **Data ethics is critical in protecting user privacy, trust, and societal well-being.**
- **The SocialConnect case demonstrates the risks of weak governance and lack of transparency.**
- **Ethical data practices, such as informed consent, data minimization, and third-party auditing, are essential to prevent misuse.**
- **Companies must balance business goals with responsibility to users and society.**
- **Strong regulatory compliance, internal ethics boards, and user education can mitigate ethical risks.**
- **Lessons learned from this case can guide organizations in building trustworthy, responsible, and ethical data practices.**