EAST WEST UNIVERSITY

Project 3 Report

Ethical Limits of Social Media Monitoring: Balancing User Privacy and Public Safety

Course Title: Cybersecurity, Law, and Ethics

Course Code: CSE487

Section: 04

Submitted to

Muhammed Yaseen Morshed Adib

Lecturer, Department of Computer Science & Engineering,

East West University

Submitted by

Group Member Name	ID
Shairin Akter Hashi	2022-2-60-102
Nushrat Jaben Aurnima	2022-2-60-146
Tahmina Ahmed	2022-2-60-151
Zihad Khan	2022-2-60-107
Md. Shahrukh Hossain Shihab	2022-1-60-372

Date of Submission: 27.12.2025

1. Introduction to the Ethical Dilemma

Social media sites have become an integral aspect of communication today, where individuals can express their views, opinions, and real-time updates. Social media sites produce a considerable amount of data that can be traced and extracted by governments, law enforcement organizations, and other private agencies. Social media monitoring is referred to as systematic observation or analysis of publicly available content on social media sites to trace potential risks or threats. Though this is practiced extensively in combating cyber-crimes, terrorism, hatred speeches, and circulation of misinformation, it still raises certain concerns related to personal rights.

The source of the ethical dilemma is based on the conflict between **two conflicting principles**: ***the right to privacy and freedom for individuals*** and ***the duty of institutions to safeguard public safety and order***. First, social media users should expect not to have their privacy seriously hampered, even for content they choose to upload on public sites. Second, an absence of regulation on social media activities could lead to damaging practices remaining unchecked on social media, causing potential risks to social welfare. Professionals such as software developers are faced with an ethical dilemma on how far they should go before they are deemed to be unnecessarily invading users' privacy on social media sites.

2. Stakeholder Analysis

Research on social media analytics and monitoring highlights the importance of considering diverse stakeholder perspectives-such as users, organizations, and institutions-when evaluating ethical implications and engagement outcomes **[2].**

1. **Social media users:** Users of the internet regularly experience having their private data tracked over time while using the internet. It may increase insecurity for some users in the name of safety and decrease the level of trust they have in the people responsible for protecting them.
2. **Government and law enforcement agencies:** Law enforcement uses social media to identify crime potential threats to public safety. But governing bodies cannot always keep law enforcement agencies from abusing their power while monitoring social media excessively.
3. **Social media companies:** User Data Management are platforms' follow legal uses and security requirements. However, weak control can increase misuse of their customer's data.
4. **Marginalized / targeted communities:** The People from marginalized communities are the least protected from these biased monitoring systems. As a result, they might have an unfair impact from inaccurate monitoring systems. Therefore, it is crucial to design a fair, transparent, and efficient method to remove biasness for targeted communities.
5. **The general public:** Government monitoring has more potential to reduce the risk and stop the flow of misinformation to society. But their large-scale surveillance could also potentially violate civil rights. So, it is important to implement ethical and proportionate monitoring practices.

With limited and legally authorized monitoring, privacy is better protected, governments can target real threats, platforms lower legal risks, and public safety is maintained without excessive surveillance.

3. Application of Ethical Frameworks

3.1 ACM Code of Ethics and Professional Conduct

This principle recognizes public good and social well-being by preventing threats like violent crime, coordinated misinformation for social media monitoring. The code signifies individuals' rights of autonomy, dignity, and fair treatment. Avoiding harm is another significant concern. Monitoring systems can cause privacy violations, misidentification, and psychological stress. This may unintentionally be due to biased algorithms and affect certain groups (gender, race, culture etc). The ACM Code stresses taking steps to reduce or correct them. Individuals deserve to know how, when, and why their information is collected as this code upholds honesty, transparency, and privacy.

All these considerations perfectly align with the ACM Code's **General Ethical Principles**, **1.1 (Contribute to society and human well-being)**, **1.2 (Avoid harm)**, **1.4 (Be fair and take action not to discriminate)**, and **1.6 (Respect privacy)**, to reduce harm, bias, and protect individual dignity. **[3]**

3.2 ACM/IEEE-CS Software Engineering Code of Ethics

This Code of Ethics prioritizes public interest above organizational interests. Engineers behind developing any social media monitoring systems must consider the broader impact that undermines privacy, freedom of expression, or equal treatment. It talks about professional responsibility and independent judgment. They are expected to approve systems only when risks do not affect the quality of life. If monitoring tools pose significant concerns, such as data breaches, professionals have a responsibility to find a solution rather than personal gains. They must understand the environment that the system needs before rush deployment.

These discussions align with the Software Engineering Code of Ethics**, 1 (Public)**, **3 (Product)**, and **4 (Judgment)** so that engineers prioritize social welfare, assess system risks, and avoid rushed deployment that may cause significant ethical or social harm. **[4]**

3.3 Web 2.0 Ethical Decision-Making Principles

This discussion is about **rights and fairness-based ethical approach commonly applied to Web 2.0 platforms**, where user participation, trust, and consent are essential for legitimate decision-making. **[5]**

In this Web 2.0 environment, social media users play active roles rather than just passive. Here users are the key concerns. By monitoring user-generated content without consent weakens the trust in the system. Web 2.0 systems require balancing threat detection with preserving communication for ethical decision making. It involves data collection policies, security implementations and regulatory compliances.

4. Group's Justified Ethical Decision

After analyzing the ethical dilemma by relating to relevant ethical frameworks, our group concludes that social media monitoring is only acceptable when it is limited, purpose specified and clearly justifies public safety concerns. Monitoring should focus on recognizing threats and crimes that harm society. We believe that restrictions are ethically preferable to unrestricted data collection. Therefore, practices such as legal authorization, data minimization, storage specifications (data retention and deletion timeline) and accountability mechanisms must be followed for monitoring.

These approaches are ethically justified by ACM principles on avoiding harm and respecting privacy, the ACM/IEEE-CS requirement to prioritize public interest and responsible judgment, and Web 2.0 ethics emphasizing user trust, consent, and fair participation.

5. Criticism and Defence of Our Decision

Criticism 1: Limiting monitoring may reduce public safety and increase dangerous behavior.

Defense: Rather than applying broader method, monitoring for serious public safety risks can be done. It can lessen privacy violations, misidentification, and psychological stress of users in automated monitoring.

Criticism 2: Data minimization and deletion rules may lessen the amount of evidence needed for investigating a crime.

Defense: Only necessary data can be collected and kept rather than everyone's data as excessive storage raises the danger of data breach and abuse especially for large scale monitoring systems.

Criticism 3: Transparency and consent might disclose vulnerability to hackers.

Defense: Transparency does not require revealing technical information. Platforms can be transparent about what information are being stored, why it is being stored, how it is stored, and user rights while keeping detection methods confidential.

Criticism 4: Audits and accountability are expensive for companies.

Defense: If monitoring brings predictable risks such as misuse, data breaches, or biased targeting on certain groups and organizations cannot provide basic protection to users; it becomes unethical to increase surveillance. For protecting user's rights and trust it is not an option but necessity to have clear policies, reviews, and reporting.

Our decision tries to prioritize user privacy and trust while maintaining public safety. This aligns with both the ACM and ACM/IEEE-CS codes, as well as transparency focused Web 2.0 principles.

6. Conclusion

Social media monitoring creates a conflict between ensuring public safety and user privacy. Although monitoring can help lessen harms such as cyber-crime, terrorism, hate speech, and misinformation, excessive or biased surveillance can make users' uncomfortable. Therefore, ethical principles require minimizing harm, ensuring fairness, and employing surveillance only when there is public safety risk.

Our group concludes that social media monitoring is permissible only when it is restricted, purpose-specified, supported by legal authorization, data minimization, deletion rules, and accountability through supervision. This approach meets stakeholder interests by enabling threat detection while preventing monitoring from becoming unjustified excessive surveillance.

References

[1] Duplicitous social media and data surveillance: An evaluation of privacy risk. (2020). *Computers & Security, 94*, 101822.

[2] Consumers' ethical perceptions of social media analytics practices: Risks, benefits and potential outcomes. (2019). *Journal of Business Research.*

[3] Association for Computing Machinery. *ACM Code of Ethics and Professional Conduct.*

[4] Association for Computing Machinery & IEEE Computer Society. *Software Engineering Code of Ethics and Professional Practice.*

[5] Impact of social media and Web 2.0 on decision-making. *ResearchGate.*