

Scenario 4: Social Media Privacy Concerns

Prem Joshi (2537632)

Manthan Siddhpura (2524128)

Dev Gajera (2538542)

Dharmikkumar Dabgar (2536691)

Scenario 4: Social Media Privacy Concerns

1. Legal Issues

a) Which Privacy Laws Are Potentially Violated?

The social media company may be violating multiple privacy and data protection laws by collecting user data without clearly informing users or obtaining valid consent. Privacy laws are designed to protect individuals' personal information and ensure organizations handle data responsibly.

1. General Data Protection Regulation (GDPR) – European Union and United Kingdom

The GDPR is one of the world's strongest privacy regulations and applies to organizations that process personal data of EU and UK residents. Key requirements include:

- Obtaining clear, informed, and freely given consent before collecting personal data.
- Informing users about what data is collected and why it is being collected.
- Allowing users to access, modify, and delete their personal information.
- Ensuring data is collected only for legitimate and specified purposes.
- Implementing appropriate security measures to protect personal data.

Potential GDPR violations include:

- Collecting personal data without explicit consent.
- Using personal information for purposes not disclosed to users.
- Sharing data with advertisers or third parties without authorization.
- Failing to provide users with access to their personal information.

2. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

These laws provide privacy rights to residents of California, United States. Businesses must:

- Inform consumers about the categories of personal information collected.
- Explain how the information is used and shared.
- Allow users to opt out of the sale or sharing of their data.
- Provide access to collected personal information upon request.

Violations may occur if the company secretly collects browsing habits, location data, or user interactions without proper disclosure.

3. Data Protection Act 2018 (United Kingdom)

The Data Protection Act complements the UK GDPR and governs the lawful processing of personal information within the UK. Organizations must ensure transparency, accountability, and lawful data processing.

4. Other International Privacy Laws

Depending on where users are located, additional laws may apply:

- Personal Information Protection and Electronic Documents Act (PIPEDA) – Canada

- Lei Geral de Proteção de Dados (LGPD) – Brazil
- Digital Personal Data Protection Act (DPDP Act) – India
- Privacy Act 1988 – Australia

Summary of Potential Legal Violations

The company may be violating privacy laws by:

- Collecting data without valid user consent.
- Failing to disclose data collection practices.
- Processing personal information beyond the original purpose.
- Sharing user information with third parties without permission.
- Failing to provide users with adequate privacy controls.
- Retaining user data longer than necessary.

b) What Legal Recourse Do Users Have?

Users affected by improper data collection practices have several legal options available.

1. Filing Complaints with Regulatory Authorities

Users can report privacy violations to relevant government agencies such as:

- The UK's Information Commissioner's Office (ICO)
- European Data Protection Authorities
- California Privacy Protection Agency (CPPA)
- Other national privacy regulators

Regulators can investigate complaints and impose substantial fines on organizations found guilty of violations.

2. Exercising Data Subject Rights

Many privacy laws grant users the right to:

- Access their personal information.
- Understand how their data is being processed.
- Correct inaccurate information.
- Restrict certain forms of processing.

3. Requesting Data Deletion

Users may invoke the "Right to be Forgotten" and request permanent deletion of personal information when there is no legitimate reason for its continued processing.

4. Seeking Financial Compensation

If privacy violations result in:

- Identity theft,

- Financial losses,
- Emotional distress,
- Reputational damage,

users may seek compensation through legal proceedings.

5. Participating in Class-Action Lawsuits

Where large numbers of users are affected, collective legal action may be taken against the company, increasing accountability and reducing litigation costs for individual users.

2. Ethical Issues

a) Evaluate the Ethicality of the Company's Data Collection Practices

The company's actions raise significant ethical concerns because they undermine user trust and violate fundamental principles of privacy and transparency.

Lack of Informed Consent

Ethically, users should understand:

- What information is being collected.
- Why it is being collected.
- How it will be used.

Collecting data without adequately informing users prevents them from making informed decisions.

Violation of Privacy

Privacy is considered a basic human right in many societies. Users reasonably expect their personal information, browsing behavior, messages, and preferences to remain protected unless they explicitly agree otherwise.

Exploitation of User Trust

Users often trust social media platforms to communicate and interact safely. Secretive data collection exploits this trust for commercial gain.

Loss of User Autonomy

When users are unaware of data collection practices, they lose control over their personal information and cannot exercise meaningful choice regarding how their data is used.

Risk of Harm

Misuse of personal data can lead to:

- Identity theft
- Fraud
- Targeted manipulation
- Psychological profiling

- Discrimination
- Unauthorized surveillance

Ethical Analysis Using Different Ethical Theories

Rights-Based Ethics

This theory emphasizes individual rights. Privacy is a fundamental right, and unauthorized data collection violates that right.

Duty-Based (Deontological) Ethics

Organizations have a moral duty to act honestly and transparently. Concealing data practices violates this duty regardless of the business benefits obtained.

Utilitarian Ethics

Although collecting user data may improve advertising effectiveness and increase profits, the potential harm to millions of users may outweigh these benefits, making the practice ethically unacceptable.

Virtue Ethics

A responsible and ethical company should demonstrate honesty, integrity, accountability, and respect for users. Secretive data collection reflects poor corporate character.

b) How Should the Company Address User Privacy Concerns Ethically?

To act ethically and rebuild trust, the company should:

Obtain Genuine Consent

Consent requests should be:

- Clear
- Specific
- Easy to understand
- Free from manipulation

Increase Transparency

Privacy policies should explain:

- What data is collected
- Why it is collected
- Who receives the data
- How long it is stored

Adopt Data Minimization

Only collect information necessary to provide the service. Excessive data collection increases privacy risks and ethical concerns.

Provide User Control

Users should be able to:

- Manage privacy settings
- Opt out of data sharing
- Download their information
- Delete their accounts easily

Conduct Ethical Reviews

The company should regularly assess whether its data practices respect user rights and societal expectations.

Ensure Third-Party Accountability

Partners and advertisers receiving user data should be required to follow the same privacy standards.

3. Professional Issues

a) What Professional Standards Should Guide the Company's Data Handling Practices?

Technology professionals have ethical responsibilities that extend beyond legal compliance.

Respect for Privacy

Professionals must protect personal information and ensure users maintain control over their data.

Honesty and Transparency

Organizations should clearly communicate their data practices and avoid deceptive behavior.

Accountability

The company should take responsibility for how data is collected, processed, stored, and shared.

Security and Confidentiality

Appropriate technical safeguards should be implemented to prevent unauthorized access, breaches, and misuse.

Fairness and Non-Discrimination

Data should not be used in ways that unfairly discriminate against individuals or groups.

Prevention of Harm

Technology professionals should anticipate risks and take proactive steps to protect users from potential harm.

Relevant Professional Standards

ACM Code of Ethics

The ACM Code emphasizes:

- Avoiding harm
- Respecting privacy
- Being honest and trustworthy

- Maintaining professional competence

IEEE Code of Ethics

The IEEE Code requires professionals to:

- Act responsibly
- Protect public welfare
- Maintain integrity
- Respect privacy and confidentiality

ISO/IEC 27001

This international standard provides guidance for:

- Information security management
- Risk assessment
- Data protection controls
- Continuous security improvement

b) What Changes Can the Company Make to Ensure Transparency and User Trust?

To regain user confidence, the company should implement the following improvements:

1. Simplify Privacy Policies

Replace lengthy legal language with clear and understandable explanations.

2. Implement Transparent Consent Mechanisms

Users should know exactly what data is being collected before agreeing.

3. Create Privacy Dashboards

Users should be able to:

- View collected information
- Download their data
- Modify privacy settings
- Delete stored information

4. Adopt Privacy-by-Design Principles

Privacy protections should be built into products from the earliest stages of development.

5. Conduct Independent Audits

External experts should regularly evaluate compliance with privacy regulations and ethical standards.

6. Strengthen Security Measures

The company should implement:

- Encryption

- Multi-factor authentication
- Access controls
- Regular security testing

7. Publish Transparency Reports

Regular reports should disclose:

- Data collection activities
- Government requests
- Third-party data sharing
- Security incidents

8. Provide Meaningful User Choice

Users should be able to opt out of data collection and sharing as easily as they opt in.

9. Establish a Dedicated Privacy Governance Team

A specialized team should oversee privacy compliance, risk management, and user protection initiatives.

10. Promote a Culture of Ethical Data Use

Employees should receive ongoing training on privacy laws, ethical responsibilities, and data protection best practices.