Somaiya Vidyavihar University
K J Somaiya School of Engineering

Course Name:	**Information Security (116U01L602)**	**Semester:**	VI
Date of Performance:	03 / 04 / 2025	**DIV/ Batch No:**	A-4
Student Name:	Hyder Presswala	**Roll No:**	16010122151

Title: Report writing on legal issues and ethics with respect to some case study.

Objectives:

Expected Outcome of Experiment:

CO5 :- Interpret legal and ethical issues in security

Books/ Journals/ Websites referred:

1. Security in Computing
2. Cryptography and Network Security
3. Cryptography and Network Security: Principles and Practice

Pre Lab/ Prior Concepts:

New Concepts to be learned:

Implementation Details:

Scenario Description:-

Your group has been hired by a technology firm to develop a facial recognition system for public spaces. The system is meant to enhance security by identifying individuals from a government watchlist and providing alerts to security personnel. However, the company also wants to collect and analyze data on all individuals passing through the monitored areas, including demographic information, movement patterns, and purchasing behaviors. This data will be sold to third-party companies for targeted advertising.

Additionally, the company wants to integrate the system with law enforcement databases, allowing authorities to track individuals in real-time without their knowledge or consent. Some of the people being tracked might not have any criminal record but are flagged based on predictive analytics that suggests they could engage in unlawful activities.

Ethical Decision-Making Model

1. Ethical Dilemma

The ethical concerns in this scenario revolve around:

- Privacy violations: People are being monitored and tracked without consent.
- Data misuse: Information collected is being sold to third parties for profit.
- Potential discrimination: Predictive analytics could lead to biased profiling.
- Surveillance state concerns: Individuals may be tracked in real time without their knowledge.

2. Stakeholders

- **General Public**: People who pass through public spaces and are unknowingly monitored.
- **Government & Law Enforcement**: Using the system for tracking and security.
- **Technology Firm**: Developing and profiting from the system.
- **Third-Party Advertisers**: Buying and using collected data for targeted marketing.
- **Civil Rights Organizations**: Concerned about ethical and legal implications.

3. Options & Effects on Stakeholders

Option	Impact on Stakeholders
Develop the system as requested	**Violates public privacy, enables government overreach, and risks unethical use of data. Benefits law enforcement, the tech firm, and advertisers.**
Implement ethical safeguards	**Protects public privacy by requiring consent and anonymization of data. Limits unethical use but may reduce profitability.**
Reject the project	**Maintains ethical integrity but loses business**

	opportunity. May result in another team developing an unethical version.
Modify the system to allow only security alerts without tracking or selling data	**Balances security and privacy concerns but may reduce commercial value for third parties.**

4. Decision & Justification

Our team decides to **modify the system to allow only security alerts without tracking or selling data**. The system will:

- Only flag individuals **on a verified criminal watchlist**.
- **Anonymize** all other collected data.
- **Require user consent** for non-security-related tracking.
- **Not sell data to third parties** without explicit consent.
- Implement **bias detection algorithms** to prevent discriminatory profiling.

ACM Code of Ethics Analysis

How Our Decision Aligns with the ACM Code of Ethics:

1. **Public Interest First (1.1 – Contribute to Society and Human Well-Being)**
   - By limiting tracking and ensuring transparency, we prioritize the public's privacy rights.
2. **Avoid Harm (1.2 – Avoid Harm to Others)**
   - We prevent privacy violations and the misuse of sensitive personal data.
3. **Honesty & Fairness (1.3 – Be Honest and Trustworthy, 1.4 – Be Fair and Take Action to Not Discriminate)**
   - We ensure ethical implementation, prevent biased tracking, and do not sell data unethically.
4. **Respect Privacy (1.6 – Respect Privacy, 1.7 – Honor Confidentiality)**
   - We anonymize data and require user consent, respecting individual rights.

Legal & Ethical Compliance Fixes

- **Transparency & Consent**: Inform individuals about data collection and allow them to opt out.
- **No Third-Party Sales**: Ensure data is not misused for profit without user consent.
- **Government Oversight**: Require legal authorization for tracking individuals in real-time.
- **Bias Checks**: Regularly audit the system to prevent discrimination.

Conclusion:
We learned about the Ethics & Laws for coding and the difference between them.