Daffodil International University

Ashulia, Savar, Bangladesh.

Department of Computer Science and Engineering

Assignment

Course Code: CSE498
Course Title: Social and Professional Issues in Computing
Assignment Number: 01
Date of Submission: 10-10-2025

Submitted by,	Submitted to,
Jannatul Ferdaus Sumaiya ID: 222-15-6423 Section: 62_E Dept. of CSE, DIU	Indrani Sen Toma Lecturer Dept. of CSE, DIU.

1. Privacy as a Social Value vs. Privacy as an Individual Right

Answer:

Privacy is often viewed through two major perspectives, as a social value and as an individual right. Although they are interconnected, the two concepts emphasize different aspects of human interaction and societal structure.

Privacy as an Individual Right focuses on personal autonomy and control over one's information. It is based on the idea that every person has the right to decide what personal data they share and with whom. For example, in the context of government surveillance, individuals expect that their private conversations, locations, and online activities will not be monitored without consent or a legal warrant. When the government collects phone records or tracks social media communications in the name of national security, it raises concerns about the violation of individual rights to privacy and freedom.

In contrast, Privacy as a Social Value views privacy not just as a personal matter, but as something essential for maintaining trust, social balance, and democracy. A society that respects privacy promotes mutual respect and freedom of expression. For instance, when corporations engage in data mining—such as social media platforms analyzing user behavior to predict trends or influence public opinion—the impact goes beyond individuals. It affects how society functions by shaping opinions, manipulating elections, or deepening inequalities through targeted advertisements. Therefore, privacy as a social value emphasizes the collective importance of safeguarding information to maintain fairness and trust within communities.

In summary, privacy as an individual right protects personal freedom and dignity, while privacy as a social value ensures a healthy, trustworthy, and democratic society. Both dimensions are crucial in addressing modern challenges of surveillance and corporate data exploitation.

2. Ethical Violations Through Secondary Use of Data

Answer:

Secondary use of data refers to the practice of using data for purposes other than the original reason it was collected. Even when the initial data collection is lawful, secondary use can lead to serious ethical violations if it breaches consent, context, or fairness.

For example, consider a healthcare system that legally collects patient information for medical treatment. If that data is later sold to an insurance company or used for targeted pharmaceutical advertising without patient consent, it violates ethical principles of confidentiality and informed consent. The patients may face discrimination or increased insurance rates based on private medical conditions they never agreed to disclose.

Similarly, in the corporate world, social media platforms collect user data to improve user experience. However, when the same data is repurposed for political campaigning or behavioral prediction—like in the Cambridge Analytica case—it leads to manipulation and misinformation. Although the data was collected lawfully, its secondary use became unethical because users were unaware of the new purposes and potential harm.

Thus, ethical data handling requires that any secondary use be transparent, consent-based, and aligned with the original intent of collection. Failing to do so undermines public trust and violates core ethical standards in computing and information systems.