

Arooj Arif Maqray

Technology is a threat to Privacy

Outline:

1. Introduction

- Meaning of privacy as a basic human right
- Rise of technology and digital dependency
- Thesis statement: despite its benefits, technology has become a major threat to personal and collective privacy.

2. Historical Background

- Pre-digital era: limited data collection
- Growth of computers and internet
- Shift from simple devices to smart, connected devices.
- Data is the new oil.

3. Major ways technology threatens privacy

A. Excessive data collection

- Apps demanding unnecessary permissions.
- Social media harvesting personal details

B. Surveillance and tracking

- Expanding CCTV and facial recognition systems
- Government surveillance under security
- Mobile phones tracking locations.

C. Gadgets and Appliances

- Smart TVs, cameras, appliances collecting audio/video.

- storage of household data by private companies.
- hacking risks.
- d. social media oversharing and algorithmic profiling
 - People share personal information voluntarily
 - Algorithms predicting behavior, choices, relationships
 - Used for targeted advertising and political manipulation.
- e. biometric data misuse
 - Fingerprints, facial scans, voice data.
 - Permanent biometrics, cannot be changed once stolen.
 - corporate misuse of biometric data.
- f. data breaches and weak cybersecurity
 - Massive leaks of financial, medical, personal information.
 - Increased identity theft and cybercrimes
 - Irreversible impact of leaked data.

Impacts of Privacy Loss

- a. Personal harm
 - Emotional distress, humiliation
 - Cyberbullying, blackmail
- b. Economic damage
 - Financial fraud, identity theft
 - Long term financial insecurity
- c. social and political consequences.
 - People are afraid to express opinions
 - Manipulation of public opinion via data profiling
 - Discrimination based on digital footprint

d. threat to democratic rights

- Mass surveillance reducing freedom.
- state misuse of data.
- weakening trust in institutions.

5. Who gains and who suffers?

a. Tech companies

Profits from user data.

b. Governments

surveillance for law enforcement and control

c. ordinary citizens

convenience but severe loss of privacy.

d. criminals and hackers

exploit data theft.

6. Current Efforts to protect privacy

a. legal Measures

Data Protection Acts

b. corporate Measures

Privacy settings, transparency reports

c. individual Measures

strong passwords, VPNs, restricted sharing.

7. Practical solutions and recommendations

a. Stronger Privacy laws

limits data collection.

b. Privacy by design.

minimum data collection in devices.

c. Public awareness

digital literacy campaigns

- d. Secure technologies
encryption, regular updates.
- e. corporate accountability.
Penalties, independent oversight

8. Ethical Considerations:

- a. Informed consent
Simple terms, no manipulative patterns
- b. Fairness
Ensuring algorithms do not discriminate
- c. balance
National security vs individual Privacy.

9. Conclusion:

Practical solutions and recommendations