

Key Privacy and Anonymity Issues

Consumer profiling

- Consumer profiling is the process of collecting and analyzing data about consumers in order to create a detailed profile of their characteristics, behaviors, and preferences.
- This information is used to segment consumers into different groups and to target marketing efforts more effectively.
- Companies openly collect personal information about users when they register at websites, complete surveys, fill out forms, follow them on social media, or enter contests online.
- Companies also use tracking software to allow their websites to analyze browsing habits and deduce personal interests and preferences.
- The use of cookies and tracking software is controversial because companies can collect information about consumers without their explicit permission.
- Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data.
- Companies that can't protect or don't respect customer information often lose business, and some become defendants in class action lawsuits stemming from privacy violations.

Electronic Discovery

- Electronic discovery (e-discovery) refers to the process of identifying, collecting, and producing electronically stored information (ESI) that is relevant to a legal case.
- ESI can include a wide range of digital information such as emails, text messages, social media posts, documents, and other electronic files.
- The purpose of discovery is to ensure that all parties go to trial with as much knowledge as possible.
- Under the rules of discovery, neither party is able to keep secrets from the other.
- It is important to note that e-discovery can be a complex and time-consuming process, and it is important to use experienced e-discovery professionals who have the necessary training and experience to conduct a thorough and accurate e-discovery process.
- Collecting, preparing, and reviewing the tremendous volume of ESI kept by an organization can involve significant time and expense.
- As a result, e-discovery can become so expensive and time consuming that some cases are settled just to avoid the costs

Workplace Monitoring

- Cyberloafing is defined as using the Internet for purposes unrelated to work such as posting to Facebook, sending personal emails or Instant messages, or shopping online
- Some surveys reveal that the least productive workers cyberloaf more than 60 percent of their time at work.

- Many organizations have developed policies on the use of IT in the workplace in order to protect against employee's abuses that reduce worker productivity or that expose the employer to harassment lawsuits.
- The potential for decreased productivity and increased legal liabilities has led many employers to monitor workers to ensure that corporate IT usage policies are being followed.
- Almost 80 percent of major companies choose to record and review employee communications and activities on the job, including phone calls, email, and web surfing.
- Some are even videotaping employees on the job
- Some employer may legally monitor your use of any employer-provided mobile phone or computing device including contact lists, call logs, email, location, photos, videos, and web browsing.
- Many employers permit their employees to use their own personal mobile phones or computing devices for work purposes in a policy called Bring Your Own Device (BYOD).
- Such a policy should spell out the degree to which use of such devices may be monitored.

Surveillance

- A number of advances in information technology—such as surveillance cameras and satellite-based systems that can pinpoint a person's physical location—provide amazing new data-gathering capabilities.
- However, these advances can also diminish individual privacy and complicate the issue of how much information should be captured about people's private lives.
- Advocates of advanced surveillance technology argue that people have no legitimate expectation of privacy in a public place and thus privacy rights do not apply
- Critics raise concerns about the use of surveillance to secretly store images of people, creating a new potential for abuse, such as intimidation of political dissenters or blackmail of people caught with the “wrong” person or in the “wrong” place.

Freedom expression

Key issues:

- a. **Controlling Access to Information on the Internet**