This course is not primarily a lecture course. It will rely heavily on a discussion of the issues presented in the textbook *Computer Ethics: A Global Perspective* by Giannis Stamatellos. These slides present ideas and quotes from the textbook primarily to inspire and promote discussions in class. A focus will be placed on

1) the local and global impact of computing on organizations and society as well as on

2) how ethical principles and leadership quality impact individuals, organizations and society.

Chapter 3: Privacy and Anonymity
Ch 3 – Privacy and Anonymity

“... privacy violation ... is one of the central issues of computer ethics.”

Needs and expectations of the individual.

conflict

Obligations of organizations that play key roles in our IT society.
Ch 3 – Privacy and Anonymity

Human dignity and freedom are key issues related to privacy concerns.

“In a computerized world where only information has value, individuals are usually treated more as the sum of data than as free human beings.”
Ch 3 – Privacy and Anonymity

“We are living in a computerized world where information is the most valuable commodity.”

“… our raw personal data is the lifeblood of a new information economy that is highly dependent on the collection, storage, and control of private information.”
Ch 3 – Privacy and Anonymity

Profit
“For some businesses, information is money, and for this reason they buy and sell information derived from personal data.”

Security
“... for some government and military organizations, information is security, and for this reason, they manipulate personal data in the name of safety and public security.”
Ch 3 – Privacy and Anonymity

Some types of sensitive personal data.

- banking records
- medical records
- military records
- police records
- insurance records
- phone calls
- airline reservations
- passport registrations
- credit card purchases
- ...
Ch 3 – Privacy and Anonymity

Some reasons governments collect personal data.

- identification (e.g., for emergency information)
- security (e.g., for criminal activities)
- information (e.g., national statistics like the census, etc.)
Ch 3 – Privacy and Anonymity

Privacy (a human right) involves four rights:

1. Solitude: the right to be alone/undisturbed.
2. Anonymity: the right to have no personal public identity.
3. Intimacy: the right to do things privately.
4. Reserve: the right to have control over your own personal information and control over how that information is disseminated.
Areas of concern regarding privacy:

1. Protection of privacy in domestic (e.g., homes), professional (e.g., workplace), civil (e.g., libraries, public streets, retail stores), and recreational environments.
   
   • Methods of intrusion include: authentication methods, video surveillance, ID checks, etc.

2. Location privacy (e.g., tracking the physical location of persons)
Ch 3 – Privacy and Anonymity

Privacy (a human right) has four rights (continued):

3. Bodily privacy (e.g., body search techniques, genetic and drug testing)

4. Personal privacy (e.g., physical searches and gathering information)

5. Communication privacy (e.g., telephone and other voice communications, email, postal mail)

6. Information privacy (e.g., related to the collection, manipulation, and dissemination of personal data)
Ch 3 – Privacy and Anonymity

Which of the six rights to privacy are associated with computer ethics?
Ch 3 – Privacy and Anonymity

“There is no doubt that the privacy of thoughts and actions must be an indefeasible right of human freedom. “

**Indefeasible**: Adjective: Not able to be lost, annulled, or overturned: "an indefeasible right". (Google online dictionary: )
“Privacy determines the freedom of an individual and identifies the personal space that one occupies and selects to share with others.

“On the other hand, privacy can produce a suspicious anonymity. Many computer criminals and terrorists hide behind their anonymity, with dangerous consequences to society.”
Ch 3 – Privacy and Anonymity

Anonymity and privacy as important protections for human freedom.

Conflict

Anonymity and privacy as protections of the guilty that shields deception and fraud.

personal freedom

public security
Ch 3 – Privacy and Anonymity

Australian Privacy Charter (1994) - “... the desire for privacy does not mean the individual has something to hide.”

Stamatellos interpretation: “Privacy protection is a fundamental human right, and its desire should not be justified nor negotiated.”
Ch 3 – Privacy and Anonymity

Alan Westin (1990) analyzed the balance in this way:

1. “Safeguarding personal and group policy in order to protect individuality and freedom against unjustified intrusions by authorities.”

2. “Collecting relevant personal information essential for rational decision-making in social, commercial and governmental life.”

3. “Conducting the constitutionally limited government surveillance of people and activities to protect public order and safety.”
Ch 3 – Privacy and Anonymity

Methods of privacy violation:

1. **Intrusion**: wrongful entry; obtaining property illegally

2. **Misuse of information**: illegal use of information

3. **Interception of information**: unauthorized eavesdropping on private information

4. **Data matching**: combining data from “unrelated databases” to produce new information that is unrelated to the various purposes for which the original data was provided

5. **Data mining**: use of large amounts of compiled data to get new information previously not identified or hidden
Ch 3 – Privacy and Anonymity

IT tools used to violate privacy:

• Database:
  • Mismanagement (e.g., incorrect or old data).
  • Data Theft
• Networks (e.g., the Internet):
  • Website with insufficient security procedures.
  • Provide direct access to personal data.
• Video cameras (e.g., closed circuit TV in public areas)
• Satellites (e.g., to track position, monitor home, etc.)
• Mobile (e.g., 3G phones & surveillance satellite, GPS, etc.)
• identification cards (smart cards, e-passports, RFID, etc.)
Ch 3 – Privacy and Anonymity

Protecting your own privacy and data:

Two forms of privacy to consider (applies at the individual, corporate and organizational levels):

1. Protecting the rights of the individual referred to by data.

2. Protecting the rights of the individual that owns data.
Ch 3 – Privacy and Anonymity

Protecting your own privacy and data: Issues related to the storage of personal data (questions to ask of organizations that have your data):

• Who collects your data and is the collection transparent and legal with respect to privacy rights?

• Is your stored data accurate and regularly updated and corrected?

• Who else is your data shared with and are you able to access and correct your own data?

• Is your data secure from unauthorized access and use? Are your individual rights protected as required by law?
Ch 3 – Privacy and Anonymity

Legislation in the United States
In the U.S. privacy issues relate to the first and fourth amendments to the U.S. Constitution.

1\textsuperscript{st} Amendment: freedom of religion, speech, the press, right of persons to peaceably assemble and “... to petition the government for a redress of grievances.”

4\textsuperscript{th} Amendment: “… the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures ... and no warrants shall issues, but upon probable cause ... “
Ch 3 – Privacy and Anonymity

Additional laws on the use of personal data.

1. The Privacy Act (1974): “restricts the collection, use, and disclosure of personal information and gives individuals the right to know and correct such information”.

Ch. 3 – Study Guide

• Name nine types of sensitive personal data.
• What are the four rights that involve privacy?
• What are the six areas of concern regarding privacy?
• Briefly describe the conflict between privacy and security.
• Name five methods of privacy violation.
• Name four questions to ask an organization collecting data on you?
• What two things does The Privacy Act of 1974 do?
• What does the Computer Matching and Privacy Protection Act of 1988 oblige government agencies to report in advance?
• Give an example of the local impact of IT-related privacy violations.
• Give an example of the global impact of IT-related privacy violations.
• Give an example of ethical principles related to privacy violations and their application in leadership. For example, in what context (education, government, business, etc.) might leadership be effective in preventing privacy violations?
• How does the ACM professional code address privacy violations?