Chapter 19(19.1, 19.2, 19.3, 19.4)

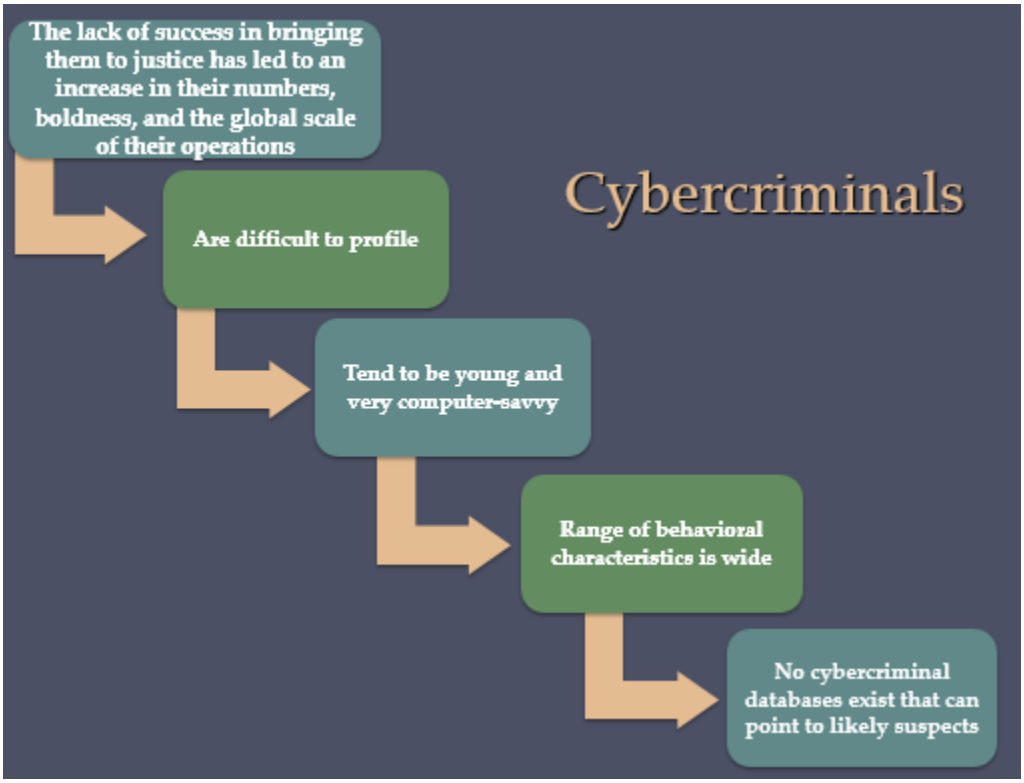
The term **cybercrime** has an implication of the use of networks specifically, whereas **computer crime** may or may not involve networks.

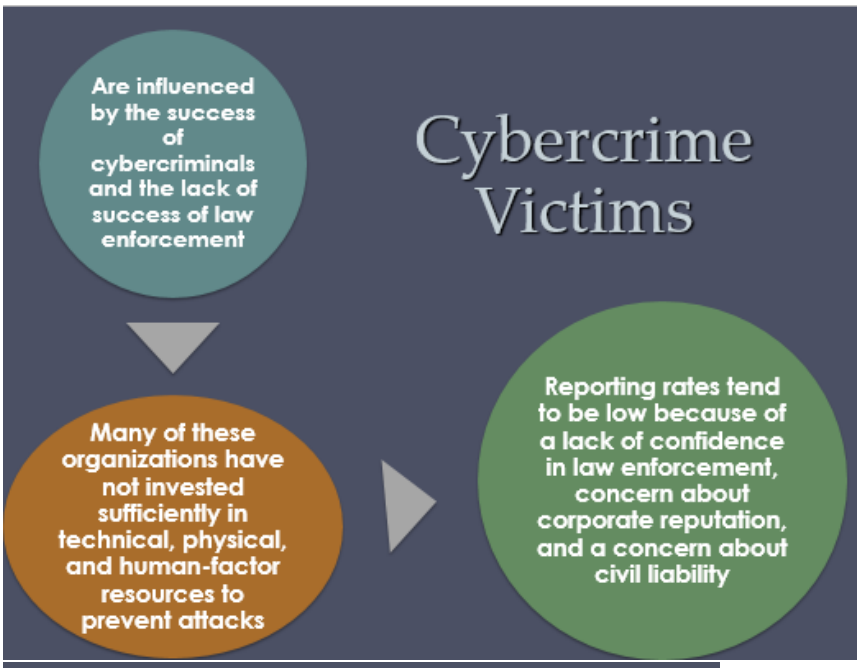
Types of Computer Crime:

1. **Computers as targets:** Involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability.
2. **Computers as storage devices:** using computers to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files or pirated commercial software
3. **Computers as communications tools:** crimes that are committed online such as illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography.

Law enforcement agency difficulties:

- Lack of investigators knowledgeable and experienced in dealing with this kind of crime
- Required technology may be beyond their budget
- The global nature of cybercrime
- Lack of collaboration and cooperation with remote law enforcement agencies





Some types of cybercrimes under the Act:

- **Access or interfere the data** or information system and copying or transmission of data; (Section 3, 4 and 5 of the Act).
- **Unauthorized access, unauthorized copying, unauthorized transmitting or unauthorized interfering** with the critical infrastructure.
- Prepare or disseminate information through any information system or device with the intent to **glorify an offence relating to terrorism.**
- Whosoever prepares or disseminates any **Hate Speech**, information that invites motivation of people to fund or recruits for terrorism through any information system or device (Sections 11 & 12 of the Act).
- **To make any illegal claim**; or title or to cause any person to part with property; or to enter into a contract; to **commit fraud**; alteration, deletion or suppression of data etc. (Sections 13 & 14 of the Act).

- **Unauthorized use of another person's identity** information or to obtain, sell, possess or transmit such information. (Sections 16 of the Act).
- **Child Pornography**
- **Doing Cyber Stalking** with an intent **to coerce or intimidate or harass any person** by using information system, information system network, internet website, electronic mail or any similar means of communication.
- **Spamming**: A person commits the offence of spamming who with an intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain. (Section 25 of the Act).

Privacy:

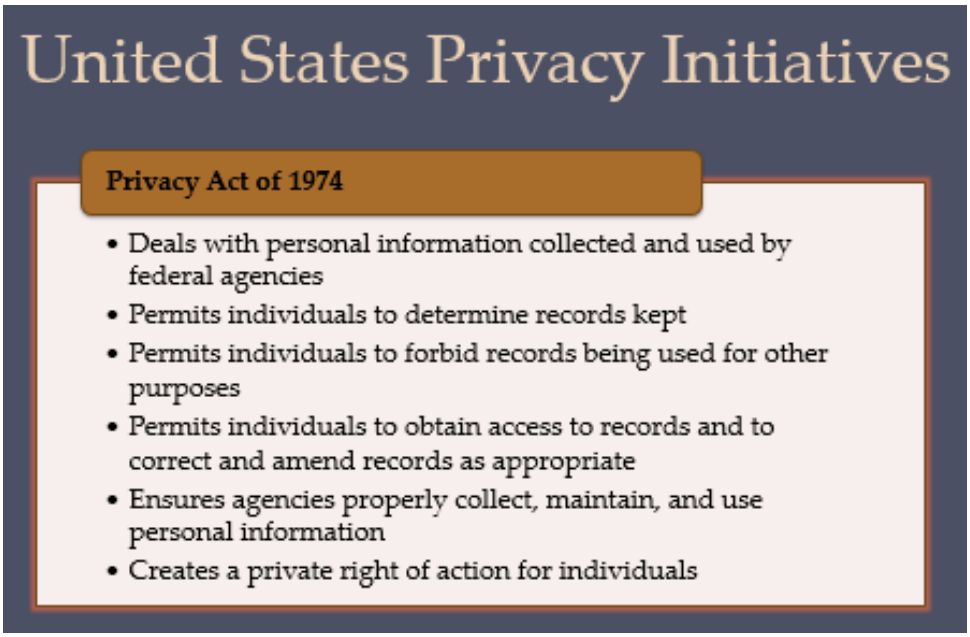
The scale of personal information collected and stored in information systems has increased dramatically, it is likely that the most economically valuable electronic asset is aggregations of information on individuals.

European Union (EU) Directive on Data Protection:

1. Ensure member states protect fundamental privacy rights when processing personal information
2. Prevent member states from restricting the free flow of personal information within EU

The Directive is organized around the following principles of personal information use:

1. **Notice:** Organizations must notify individuals what personal information they are collecting, the uses of that information, and what choices the individual may have.
2. **Consent:** Individuals must be able to choose whether and how their personal information is used by, or disclosed to, third parties.
3. **Consistency**: Organizations may use personal information only in accordance with the terms of the notice given the data subject and any choices with respect to its use exercised by the subject.
4. **Access:** Individuals must have the right and ability to access their information and correct, modify, or delete any portion of it.
5. **Security**: Organizations must provide adequate security, using technical and other means, to protect the integrity and confidentiality of personal information.
6. **Onward transfer:** Third parties receiving personal information must provide the same level of privacy protection as the organization from whom the information is obtained.
7. **Enforcement:** The Directive grants a private right of action to data subject when organizations do not follow the law. In addition, each EU member has a regulatory enforcement agency concerned with privacy rights enforcement.



Privacy and Data Surveillance:

The demands of big business, government and law enforcement have created new threats to personal privacy

- Scientific and medical research data collection for analysis
- Law enforcement data surveillance
- Private organizations profiling
- This creates tension between enabling beneficial outcomes is areas including scientific research, public health, national security, law enforcement and efficient use of resources, while still respecting an individual's right to privacy

Another areas of particular concern is the rapid rise in the use of public social media sites

- These sites **gather, analyze, and share large amounts of data on individuals** and their interactions with other individuals and organizations
- Many people **willingly upload large amounts of personal information**, including photos and status updates
- This data could potentially be used by current and **future employers, insurance companies, private investigators**, and others, in their interactions with the individual

Privacy Protection:

- **Encryption**: This involves using mathematical algorithms to encode information so that it can only be accessed by authorized individuals who have the correct decryption key. This can help protect sensitive information from being accessed by unauthorized parties.
- **Anonymization:** This involves removing personally identifiable information from data sets, so that individuals can no longer be identified. This can help protect individuals' privacy while still allowing the data to be used for research or other purposes.
- **Access control:** This involves restricting access to personal information to only those who have a legitimate need to access it. This can be accomplished through the use of passwords, security tokens, or other forms of authentication.

- **Data minimization**: This involves collecting only the minimum amount of personal information necessary for a specific purpose. This can help reduce the risk of that information being misused or accidentally disclosed.
- **Privacy policies**: Developing and implementing clear, concise, and easy-to-understand privacy policies can help ensure that individuals understand how their personal information will be used, and can help prevent misunderstandings or misuse of that information.

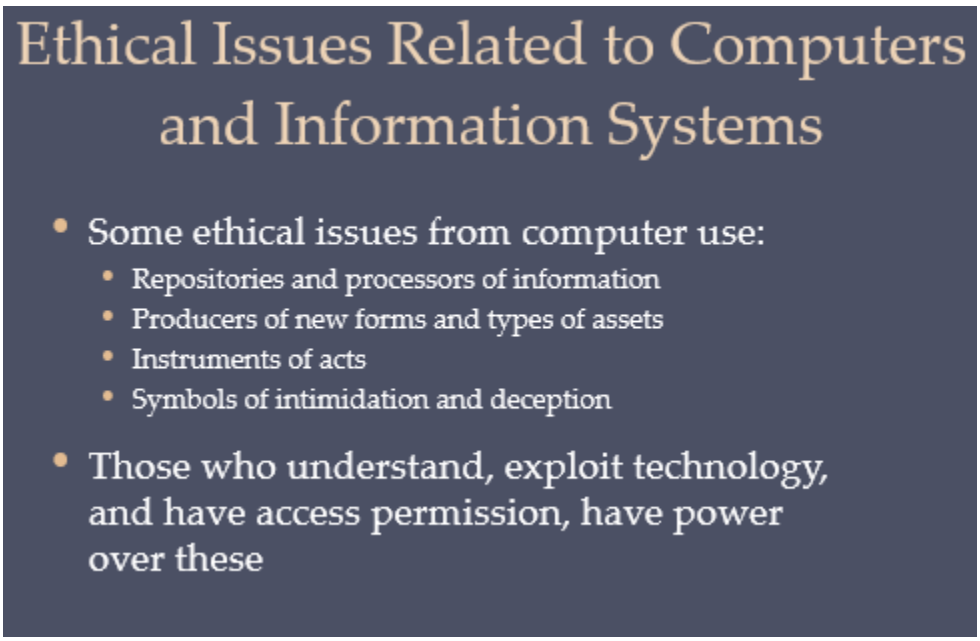
Data Privacy:

In terms of policy, guidelines are needed to manage the use and reuse of big data, ensuring suitable constraints are imposed in order to preserve privacy

- **Consent:** Ensuring participants can make informed decisions about their participation in the research
- **Privacy and confidentiality:** Privacy is the control that individuals have over who can access their personal information. Confidentiality is the principle that only authorized persons should have access to information
- **Ownership and authorship**: Addresses who has responsibility for the data, and at what point does an individual give up their right to control their personal data
- **Data sharing – assessing the social benefits of research:** The social benefits that result from data matching and reuse of data from one source or research project in another
- **Governance and custodianship**: Oversight and implementation of the management, organization, access, and preservation of digital data

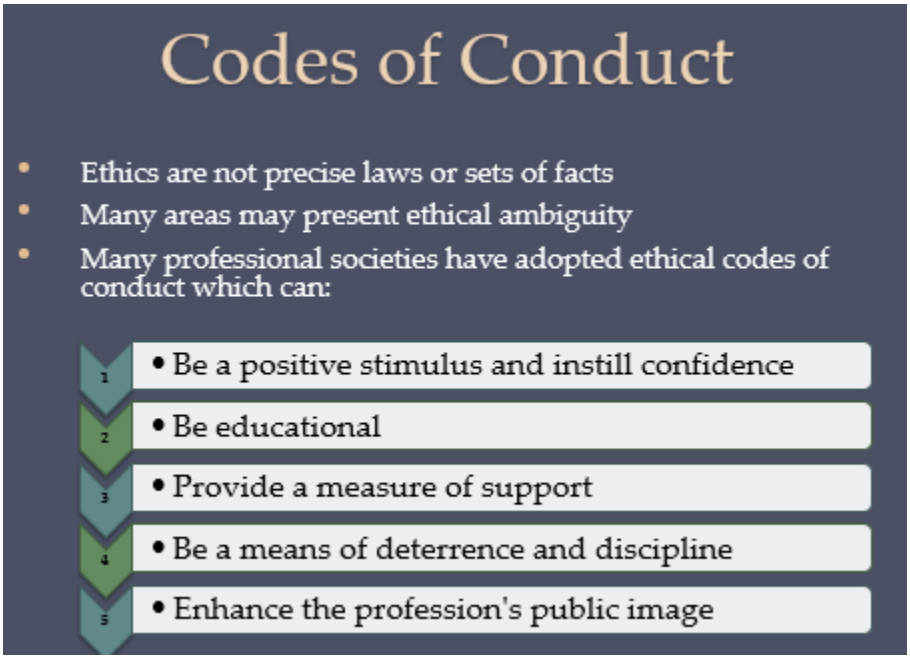
Ethical Issues:

Ethics refers to the principles and values that guide behavior. In other words, ethics is about determining what is right and wrong, and making choices that align with those values. Ethics is often associated with moral principles, and can be used to help individuals and organizations make decisions that are fair, just, and respectful of others.



Two types of ethical questions that IT professional faces:

1. The first is that IT professionals may find themselves in situations where their ethical duty as professionals comes into conflict with loyalty to their employer. Such a conflict may give rise for an employee to consider "**blowing the whistle**," or exposing a situation that can harm the public or a company's customers. Organizations have a duty to provide alternative, less extreme opportunities for the employee, such as not to penalize employees for exposing problems in-house.
2. **Potential conflict of interest.** For example, if a consultant has a financial interest in a certain vendor, this should be revealed to any client if that vendor's products or services might be recommended by the consultant.



Comparison of Code of Conduct of ACM, IEEE, AITP:

Common themes:

- Dignity and worth of other people
- Personal integrity and honesty
- Responsibility for work
- Confidentiality of information
- Public safety, health, and welfare
- Participation in professional societies to improve standards of the profession
- The notion that public knowledge and access to technology is equivalent to social power

The Rules:

Collaborative effort to develop a short list of guidelines on the ethics of computer systems. The guidelines, which continue to evolve, are the product of the Ad Hoc Committee on Responsible Computing. Anyone can join this committee and suggest changes to the guidelines

The Rules apply to:

1. Any artifact that includes an executing computer program.
2. Software that is commercial, free, open source, recreational, an academic exercise or a research tool.

The Rules are as follows:

1) The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system.
2) The shared responsibility of computing artifacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying, or using the artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.
3) People who knowingly use a particular computing artifact are morally responsible for that use.
4) People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded.
5) People who design, develop, deploy, promote, or evaluate a computing artifact should not explicitly or implicitly deceive users about the artifact or its foreseeable effects, or about the sociotechnical systems in which the artifact is embedded.