CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Security Auditing, Legal and Ethical Aspects

Privacy and Ethical Issues

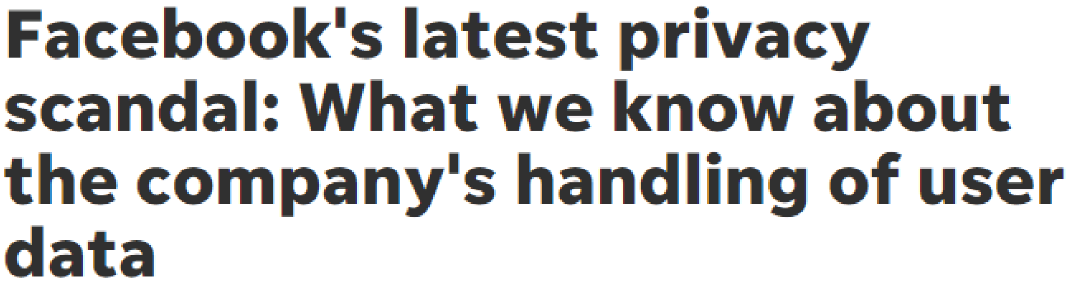
Video Summary

- Privacy Issues
- EU and US Privacy Initiatives
- Privacy Class Decomposition
- Ethics and Codes of Conduct

Privacy

- Dramatic increase in scale of information collected and stored
  - Motivated by law enforcement, national security, economic incentives
- Individuals have become increasingly aware of access and use of personal information and private details about their lives
- Concerns about extent of privacy compromise have led to a variety of legal and technical approaches to reinforcing privacy rights

Privacy



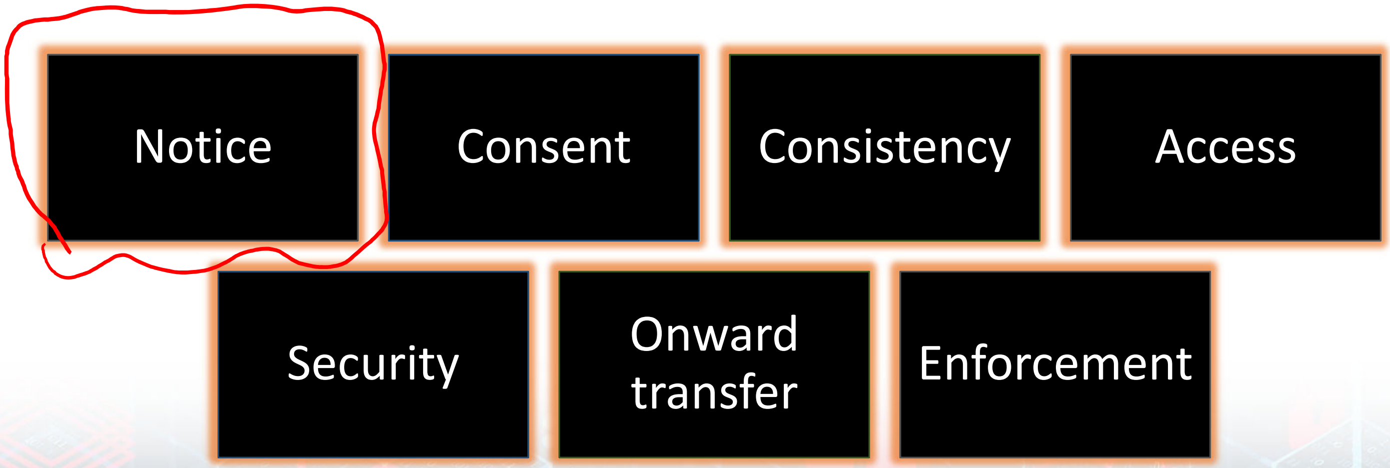
Facebook's latest privacy scandal: What we know about the company's handling of user data

- Dec. 2018
- Facebook gave technology companies like Microsoft, Netflix and Spotify special access to user's data without anyone else knowing.

European Union (EU) Directive on Data Protection

- Adopted in 1998 to:
  - Ensure member states protect fundamental privacy rights when processing personal information
  - Prevent member states from restricting the free flow of personal information within EU

- Organized around principles of:



Notice

Consent

Consistency

Access

Security

Onward transfer

Enforcement

United States Privacy Initiatives

Privacy Act of 1974

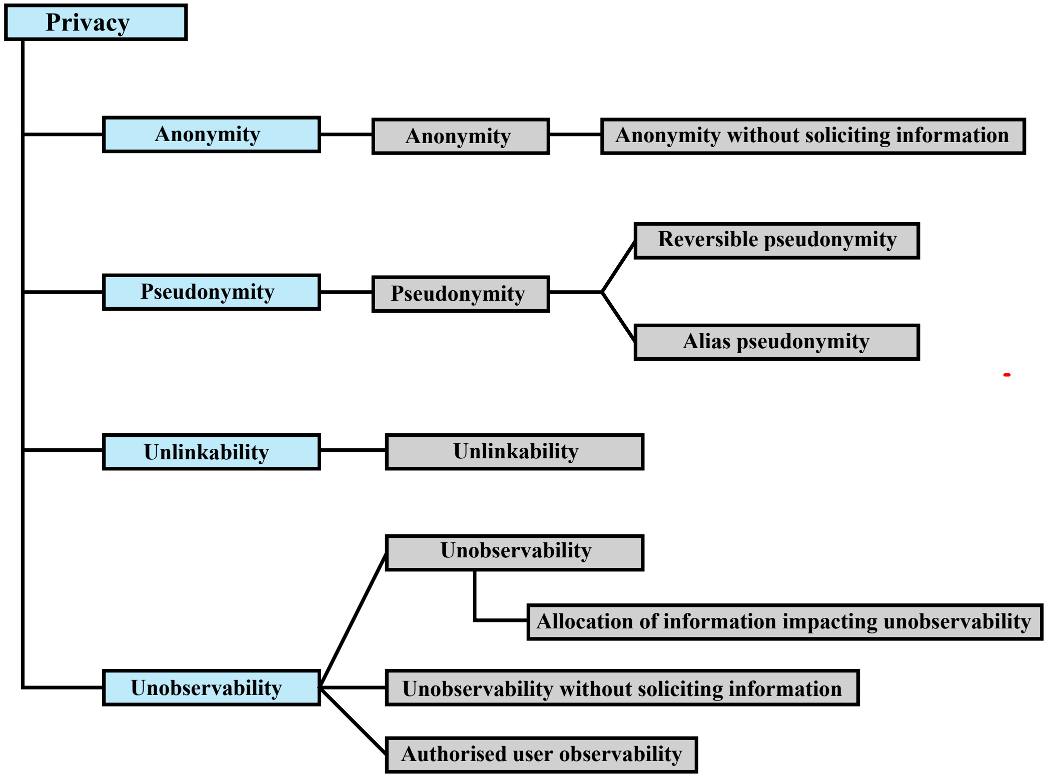
- Deals with personal information collected and used by federal agencies
- Permits individuals to determine records kept
- Permits individuals to forbid records being used for other purposes
- Permits individuals to obtain access to records and to correct and amend records as appropriate
- Ensures agencies properly collect, maintain, and use personal information
- Creates a private right of action for individuals

Also have a range of other privacy laws

ISO 27002 states . . .

“An organization’s data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information. Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented.”

Privacy Class Decomposition


Privacy
Anonymity
Anonymity
Anonymity without soliciting information
Pseudonymity
Pseudonymity
Reversible pseudonymity
Alias pseudonymity
Unlinkability
Unlinkability
Unobservability
Unobservability
Allocation of information impacting unobservability
Unobservability without soliciting information
Authorised user observability

Ethical Issues

- Many potential misuses and abuses of information and electronic communication that create privacy and security problems
- Basic ethical principles developed by civilizations apply
  - Unique considerations surrounding computers and information systems
  - Scale of activities not possible before
  - Creation of new types of entities for which no agreed ethical rules have previously been formed

- Ethics:

“A system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions.”

What is the main difference between Ethics and Laws?

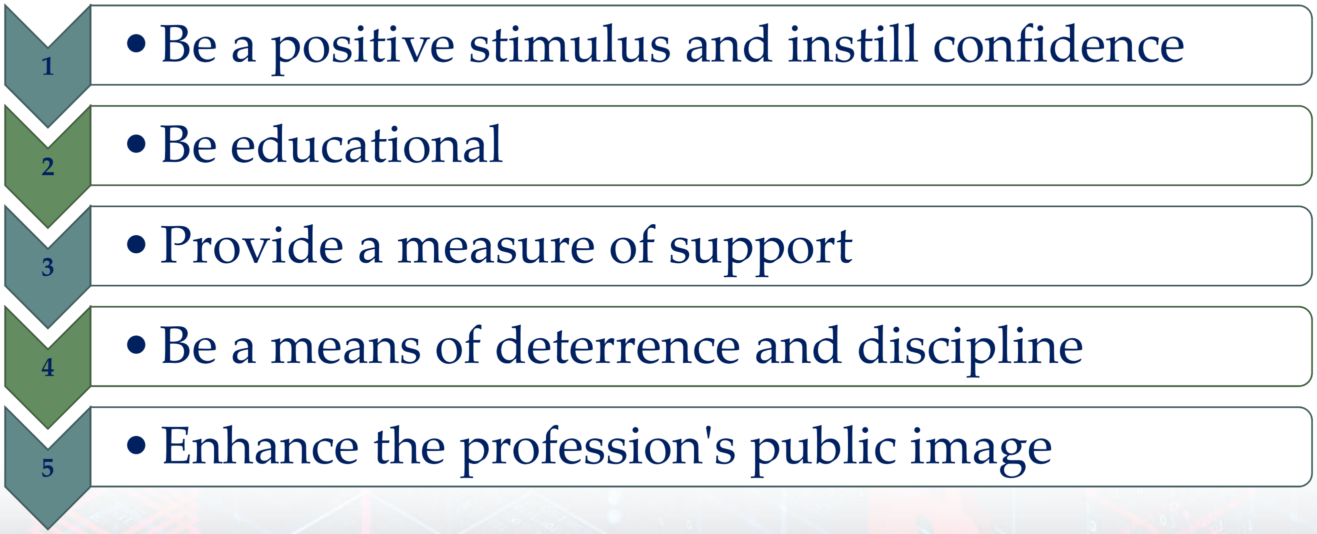
Judgment?

Professional/Ethical Responsibilities

- Types of ethical areas a computing or IT professional may face:
  - Ethical duty as a professional may come into conflict with loyalty to employer
  - “Blowing the whistle” or exposing a situation that can harm the company’s customers
  - Potential conflict of interest
- Organizations have a duty to provide alternative, less extreme opportunities for the employee
  - In-house person coupled with a commitment not to penalize employees for exposing problems
- Professional societies should provide a mechanism whereby society members can get advice on how to proceed

Codes of Conduct

- Ethics are not precise laws or sets of facts
- Many areas may present ethical ambiguity
- Many professional societies have adopted ethical codes of conduct which can:



1 • Be a positive stimulus and instill confidence

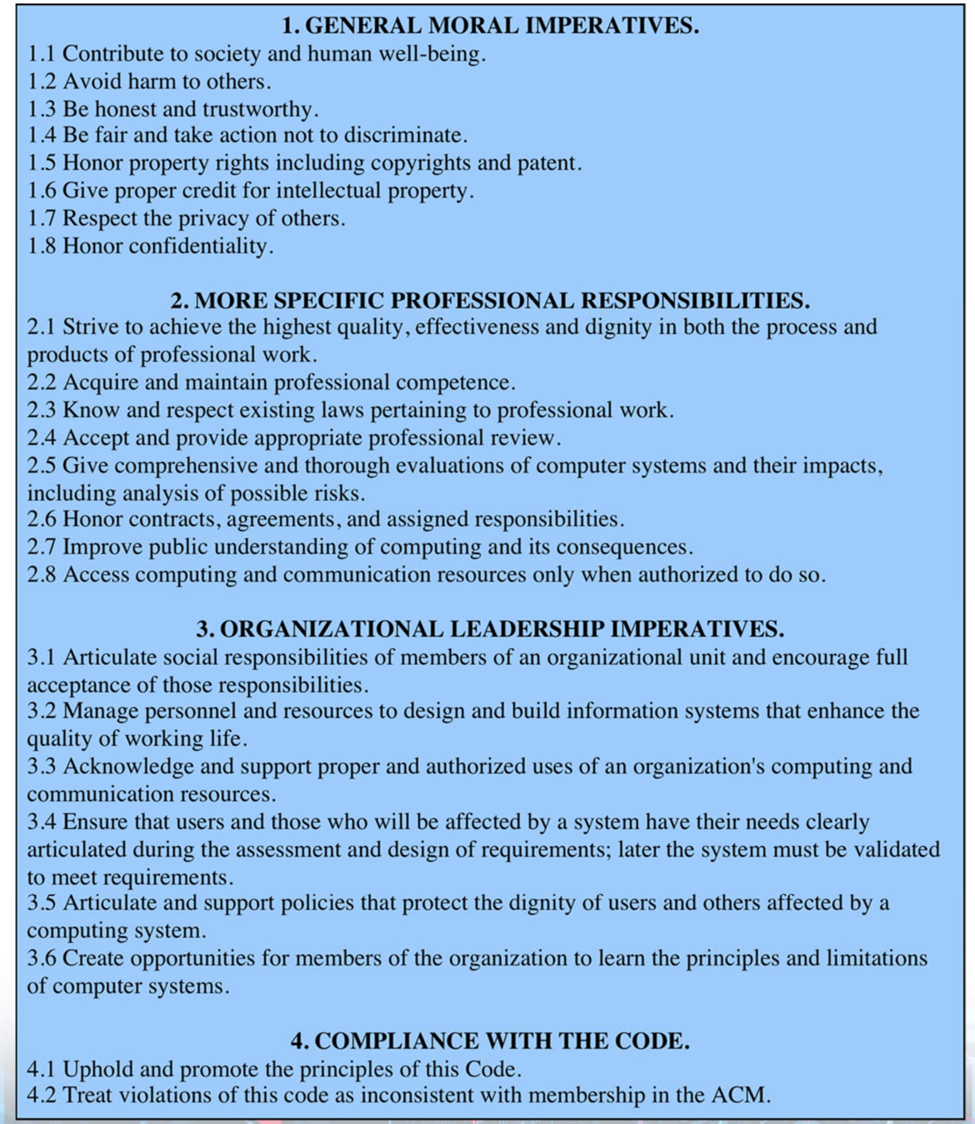
2 • Be educational

3 • Provide a measure of support

4 • Be a means of deterrence and discipline

5 • Enhance the profession's public image

Association for Computing Machinery (ACM) Code of Ethics



1. GENERAL MORAL IMPERATIVES.

1.1 Contribute to society and human well-being.
1.2 Avoid harm to others.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Honor property rights including copyrights and patent.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
2.2 Acquire and maintain professional competence.
2.3 Know and respect existing laws pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
2.6 Honor contracts, agreements, and assigned responsibilities.
2.7 Improve public understanding of computing and its consequences.
2.8 Access computing and communication resources only when authorized to do so.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

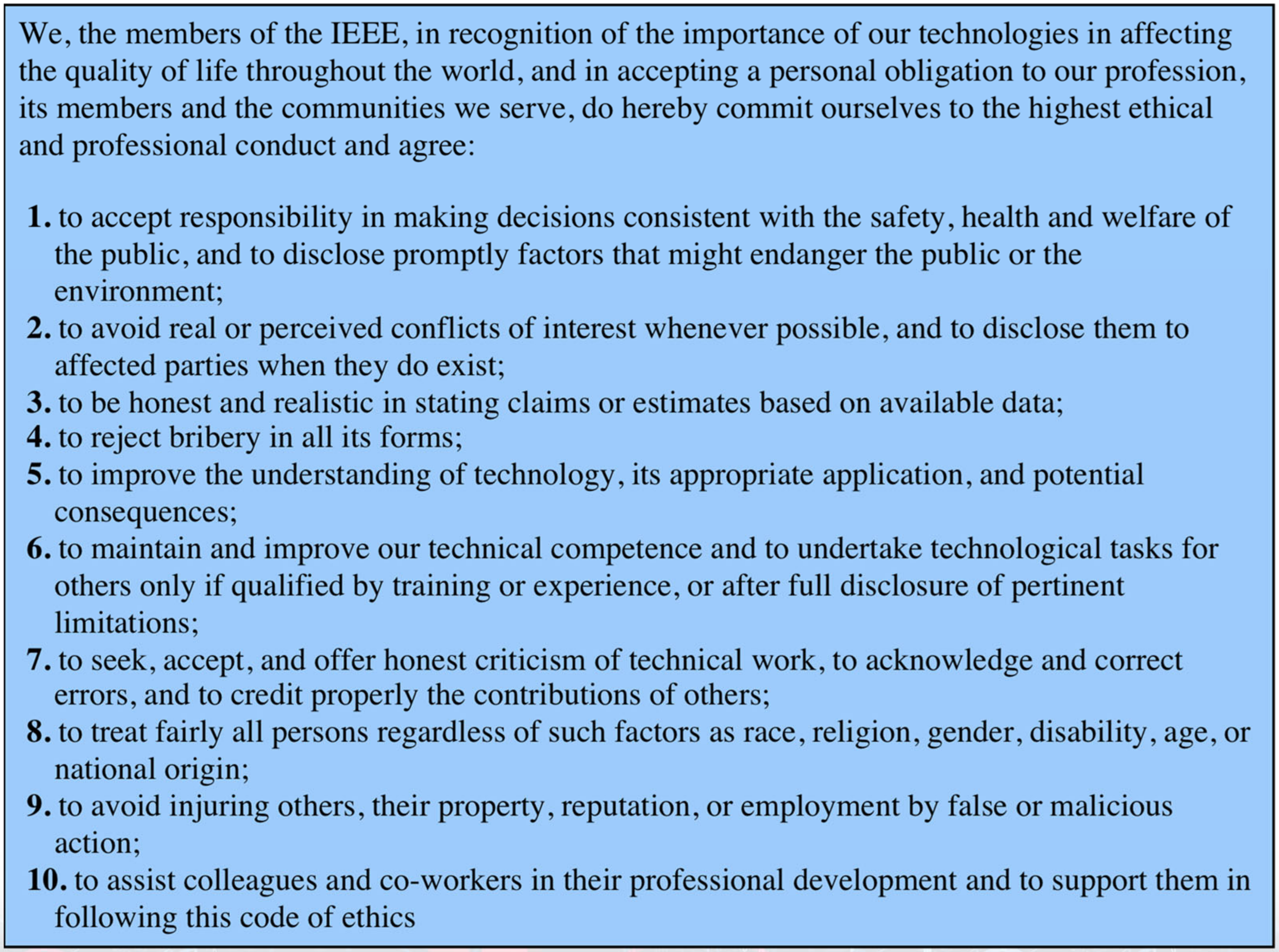
3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.
3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.
3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

4. COMPLIANCE WITH THE CODE.

4.1 Uphold and promote the principles of this Code.
4.2 Treat violations of this code as inconsistent with membership in the ACM.

Figure 19.6 ACM Code of Ethics and Professional Conduct

IEEE Code of Ethics



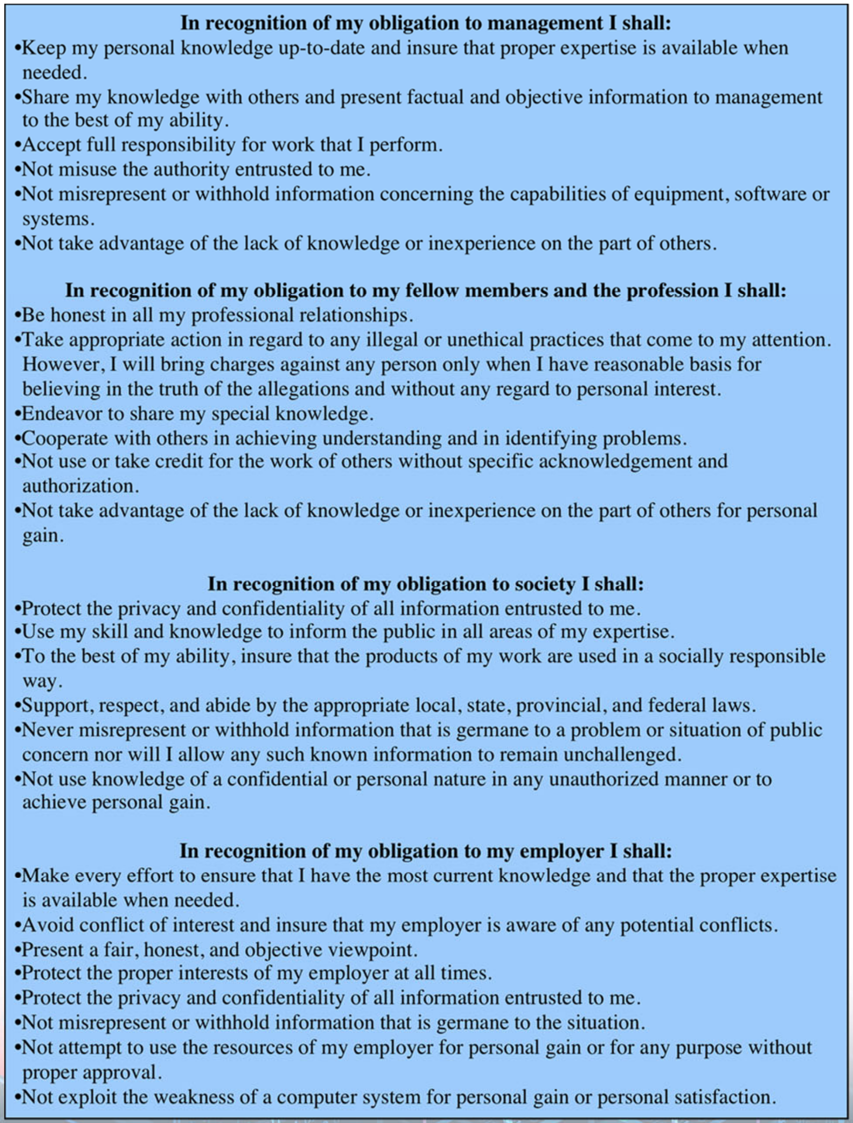
We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics

Figure 19.7 IEEE Code of Ethics

(Copyright ©2006, Institute of Electrical and Electronics Engineers)

Association of Information Technology Professionals (AITP) Standard of Conduct



In recognition of my obligation to management I shall:

- Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.
- Share my knowledge with others and present factual and objective information to management to the best of my ability.
- Accept full responsibility for work that I perform.
- Not misuse the authority entrusted to me.
- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.
- Not take advantage of the lack of knowledge or inexperience on the part of others.

In recognition of my obligation to my fellow members and the profession I shall:

- Be honest in all my professional relationships.
- Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without any regard to personal interest.
- Endeavor to share my special knowledge.
- Cooperate with others in achieving understanding and in identifying problems.
- Not use or take credit for the work of others without specific acknowledgement and authorization.
- Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

In recognition of my obligation to society I shall:

- Protect the privacy and confidentiality of all information entrusted to me.
- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Support, respect, and abide by the appropriate local, state, provincial, and federal laws.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

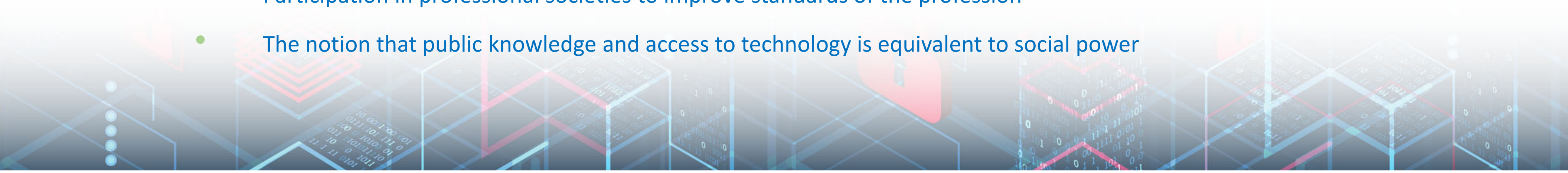
In recognition of my obligation to my employer I shall:

- Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.
- Avoid conflict of interest and insure that my employer is aware of any potential conflicts.
- Present a fair, honest, and objective viewpoint.
- Protect the proper interests of my employer at all times.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Figure 19.8 AITP Standard of Conduct

Comparison of Codes of Conduct

- All three codes place their emphasis on the responsibility of professionals to other people
- Do not fully reflect the unique ethical problems related to the development and use of computer and IT technology
- 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



Video Summary

- Privacy Issues
- EU and US Privacy Initiatives
- Privacy Class Decomposition
- Ethics and Codes of Conduct