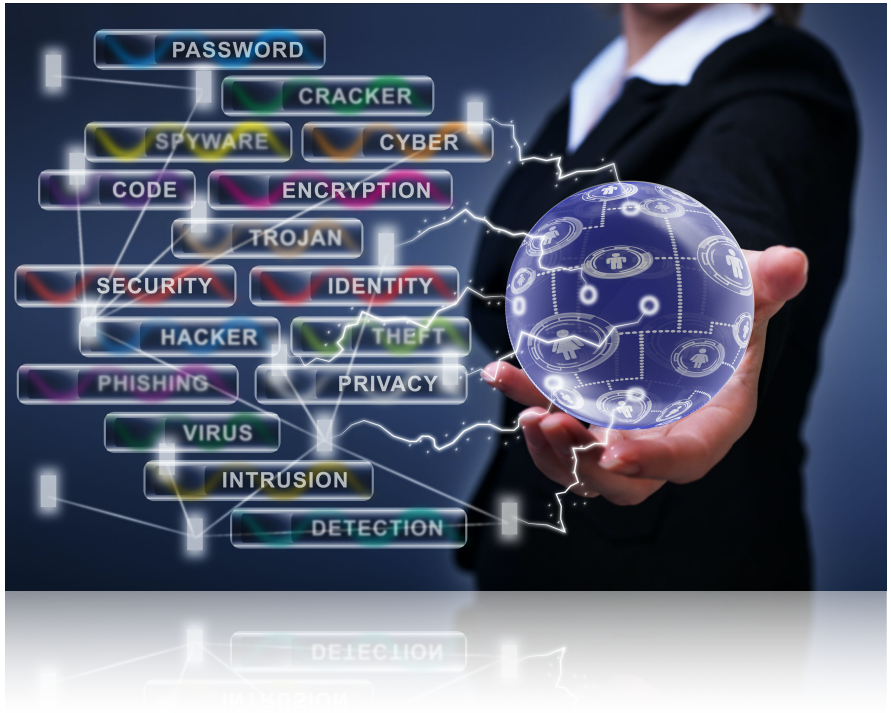
Information Technology Fundamentals

Mohammad Hossein Manshaei
manshaei@gmail.com



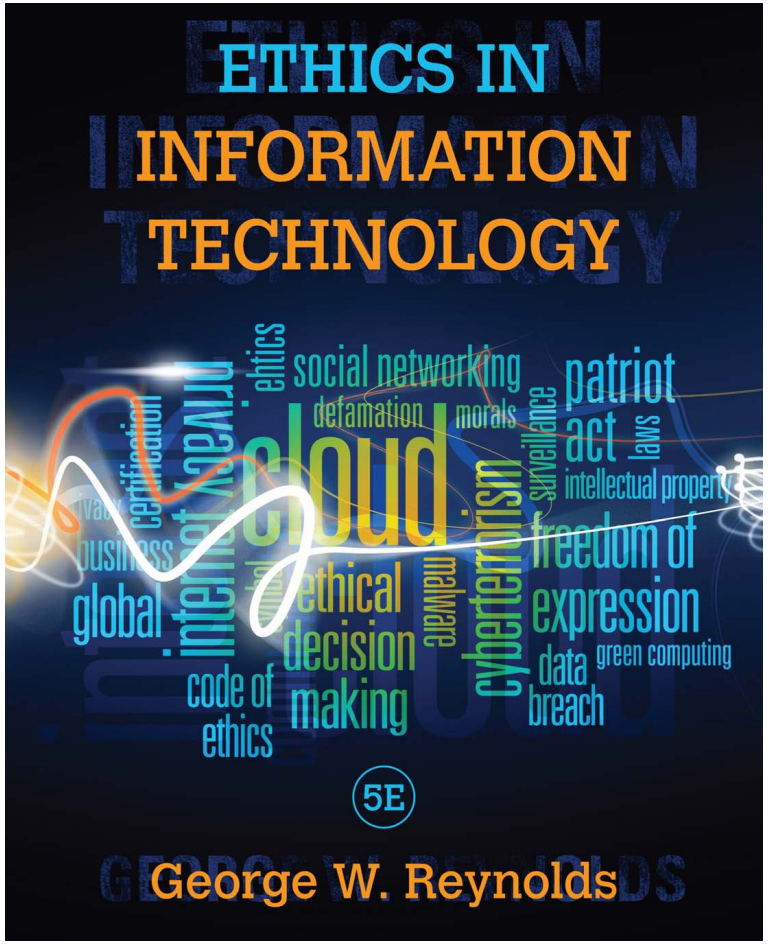
Information Assurance & Security: Privacy
Module 7: Part I

Module 7. Main Objectives

1. Define Main Concepts of Information Privacy
2. Review Privacy Laws, Applications, and Key issues

Main Reference

- George W. Reynolds, 2011. **Ethics in Information Technology.** Engage Learning.



Contents

- ➢ Privacy Protection and the Law
  - ◇ Information Privacy
  - ◇ Privacy Laws, Applications, and Court Rulings
    - Financial Data
    - Health Information
    - Children Personal Data
    - Electronic Surveillance
    - Export of Personal Data and Access to Government Records

Privacy Protection and the Law

- Systems **collect** and **store** key data from every **interaction** with customers
- Many **object** to data collection policies of government and business
- Privacy
  - Key concern of Internet users
  - Top reason why some people still avoid the Internet
- Reasonable **limits** must be set
- Historical perspective on the right to privacy
  - Fourth Amendment - reasonable expectation of privacy

Definition of Privacy

- Right of Privacy:
  - "The right to be **left alone**—the most comprehensive of rights, and the right most valued by **a free people**"
- Information Privacy:
  - "The right of individuals to **control the collection** and use of **information about themselves**"

    - Communication Privacy

      +

    - Data Privacy

The Right of Privacy (continued)

- Legal aspects
  - Protection from unreasonable intrusion upon one's isolation
  - Protection from appropriation of one's name or likeness
  - Protection from unreasonable publicity given to one's private life
  - Protection from publicity that unreasonably places one in a false light before the public

Contents

- ➢ Privacy Protection and the Law
  - ◇ Information Privacy
  - ◇ Privacy Laws, Applications, and Court Rulings
    - Financial Data
    - Health Information
    - Children Personal Data
    - Electronic Surveillance
    - Export of Personal Data and Access to Government Records

Financial Data

Individuals **must reveal** much of their personal financial data in order to take advantage of the wide range of **financial products and services available**

(credit cards, checking and savings accounts, loans, payroll direct deposit, and brokerage accounts.)

Fair Credit Reporting Act (1970)

- The act outlines:
  - Who may access your credit information
  - How you can find out what is in your file
  - How to dispute inaccurate data
  - How long data is retained
  - …
- Ensure accuracy, fairness, and privacy of information gathered by the credit-reporting companies

Gramm-Leach-Bliley Act (GLBA- 1999)

- Glass-Steagall (1933): Prohibited any one institution from offering investment, commercial banking, and insurance services

- GLBA: Enabled such entities to merge (e.g., Bank of America, Citigroup, and JPMorgan Chase)

GLBA and Privacy Concerns

1. Financial Privacy Rule
   - Mandatory guidelines for the collection and disclosure of personal financial information by financial organizations
   - Must provide a privacy notice to each consumer
     - What data about the consumer is gathered
     - With whom that data is shared
     - How the data is used
     - How the data is protected
   - Opt out and Opt In policy
2. Safeguards Rule
   - Document a data security plan describing its plans for the ongoing protection of clients' personal data
3. Pretexting Rule

Contents

- ➢ Privacy Protection and the Law
  - ◇ Information Privacy
  - ◇ Privacy Laws, Applications, and Court Rulings
    - Financial Data
    - Health Information
    - Children Personal Data
    - Electronic Surveillance
    - Export of Personal Data and Access to Government Records

Health Information

1. The use of **electronic medical records**

2. Subsequent **interlinking**

3. Transferring of this electronic information among different organizations.

Health Insurance Portability and Accountability Act (HIPAA-1996)

- Healthcare organizations must
  - Employ **standardized electronic** transactions
  - Obtain written consent from patients prior to disclosing any information in their medical records
  - Appoint a **privacy officer** to develop privacy policies and procedures
- Misuse data may be **fined $250,000** and serve up to **10 years in prison**

Contents

- ➢ Privacy Protection and the Law
  - ◇ Information Privacy
  - ◇ Privacy Laws, Applications, and Court Rulings
    - Financial Data
    - Health Information
    - Children Personal Data
    - Electronic Surveillance
    - Export of Personal Data and Access to Government Records

Children's Personal Data

Need to **protect children** from being exposed to **inappropriate material** and **online predators**

Children's Online Privacy Protection Act (COPPA-1998)

Web site that caters to children must:

- Offer comprehensive privacy policies
- Notify parents or guardians about its data-collection practices
- Receive parental consent before collecting any personal information from children under 13.

COPPA- Case Study

- In 2006, the FTC charged **Bonzi Software**, Inc., and **UMG Recordings**, Inc., with collecting personal information from children online without their parents' consent,
  - Bonzi Software: A free software download called BonziBUDDY, was the first company charged for privacy violations over a download. (**fined** $75,000)
  - UMG Recordings, which operates music-related Web sites, was charged with collecting birth dates from children through its online registration process. (fined $400,000)
- The social networking Web site **Xanga.com** was also fined **$1 million** for allowing preteens to sign up for the service without gaining a parent's consent