CHAPTER **6**

Ethics and Privacy

DR. JAMIL S. ALAGHA

1. Ethical Issues
2. Privacy

1. Describe ethics, its three fundamental tenets, and the four categories of ethical issues related to information technology.

2. Discuss at least one potential threat to the privacy of the data stored in each of three places that store personal data.

6.1 Ethical Issues

- Ethical Frameworks
- Ethics in the Corporate Environment
- Ethics and Information Technology

Ethical Frameworks

- Utilitarian Approach
- Rights Approach
- Fairness Approach
- Common Good Approach
- Five Steps of the General Ethical Framework

Five Steps of the General Ethical Framework

1. Recognize the Issue
2. Get the Facts
3. Evaluate Alternative Actions
4. Make a Decision and Test It
5. Act and Reflect on the Outcome of Your Decision

Ethics in the Corporate Environment

- Code of Ethics
- Fundamental Tenets of Ethics
  - Responsibility
  - Accountability
  - Liability

Ethics and Information Technology

- Privacy Issues
- Accuracy Issues
- Property Issues
- Accessibility Issues

6.2 Privacy

- Electronic Surveillance
- Personal Information in Databases
- Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites
- Privacy Codes and Policies
- International Aspects of Privacy

Privacy: Two Rules

- Court decisions in many countries have generally followed two rules
  1. The right to privacy is not absolute. Privacy must be balanced against the needs of society.
  2. The public's right to know supersedes the individual's right to privacy.

Electronic Surveillance

- ACLU – Electronic surveillance is rapidly increasing
- Emerging Technologies increase monitoring of human activity
  - Your SmartPhone has become a Sensor
- Facial Recognition by Google & Facebook
- Tagging (Photos & Geotagging)

Personal Information in Databases

- Major Concerns:
  - Do you know where the records are?
  - Are the records accurate?
  - Can you change inaccurate data?
  - How long will it take to make a change?
  - Under what circumstances will the personal data be released?

Personal Information in Databases (continued)

- Major Concerns:
  - How are the data used?
  - To whom are the data given or sold?
  - How secure are the data against access by unauthorized people?

Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

- Weblog
- Free Speech versus Privacy

Privacy Codes and Policies

- Opt-in Model
- Opt-out Model
- Platform for Privacy Preferences (P3P)

Table 6.2: Privacy Policy Guidelines: A Sampler

Data collection

Data should be collected on individuals only for the purpose of accomplishing a legitimate business objective.

Data should be adequate, relevant, and not excessive in relation to the business objective.

Individuals must give their consent before data pertaining to them can be gathered. Such consent may be implied from the individual's actions (e.g., applications for credit, insurance, or employment).

Data accuracy

Sensitive data gathered on individuals should be verified before they are entered into the database.

Data should be kept current, where and when necessary.

The file should be made available so that the individual can ensure that the data are correct.

In any disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.

Data confidentiality

Computer security procedures should be implemented to ensure against unauthorized disclosure of data. These procedures should include physical, technical, and administrative security measures.

Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.

Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.

Data should not be disclosed for reasons incompatible with the business objective for which they are collected.

International Aspects of Privacy

- Inconsistent Privacy and Security Laws
- Transborder data flow
- European Community Commission
- Safe Harbor framework for European citizen personal data