Chapter 12

Ethical and Social Issues in Information Systems
STUDENT OBJECTIVES

• What ethical, social, and political issues are raised by information systems?

• What specific principles for conduct can be used to guide ethical decisions?
STUDENT OBJECTIVES

• Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?

• How have information systems affected everyday life?
**Problem:** inability to efficiently target online ads.

**Solutions:** behavioral targeting allows businesses and organizations to more precisely target desired demographics.
• Google monitors user activity on thousands of sites; businesses monitor activity on their own sites to better understand customers.

• Demonstrates IT’s role in organizing and distributing information.

• Illustrates the ethical questions inherent in online information gathering.
Behavioral Targeting and Your Privacy: You’re the Target

- Develop expertise
- Develop information policies
- Combine search engine firms with advertising networking firms
- Develop strategies to fend off privacy critics and federal government legislation
- Coordinate industry-wide responses to claims of privacy invasion
- Develop huge databases to track individual behavior online
- Develop software to profile individuals

Business Challenges
- Display ads decline in utility and price
- Desire to monetize huge collections of Web behavioral data

People

Organization

Technology

Information System

Business Solutions
- Advertising networks track and profile individuals online
- Display ads become more relevant, effective, and valuable
- Invades the privacy of 200 million individuals

Develop digital profiles on millions of Web users and target "relevant" ads to them
• Recent cases of failed ethical judgment in business
  • Bear Stearns, Galleon Group, Pfizer
  • In many, information systems used to bury decisions from public scrutiny

• Ethics
  • Principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors
Information systems and ethics

Information systems raise new ethical questions because they create opportunities for:

- Intense social change, threatening existing distributions of power, money, rights, and obligations
- New kinds of crime
A Model for Thinking About Ethical, Social, and Political Issues

- Society as a calm pond
- IT as rock dropped in pond, creating ripples of new situations not covered by old rules
- Social and political institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, laws
  - Requires understanding of ethics to make choices in legally gray areas
The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

Figure 12-1
Five Moral Dimensions of the Information Age

1. Information rights and obligations
2. Property rights and obligations
3. Accountability and control
4. System quality
5. Quality of life
Key Technology Trends That Raise Ethical Issues

- Doubling of computer power
  - More organizations depend on computer systems for critical operations
- Rapidly declining data storage costs
  - Organizations can easily maintain detailed databases on individuals
- Networking advances and the Internet
  - Copying data from one location to another and accessing personal data from remote locations are much easier
Key Technology Trends That Raise Ethical Issues

• Advances in data analysis techniques
  • Companies can analyze vast quantities of data gathered on individuals for:
    • Profiling
      • Combining data from multiple sources to create dossiers of detailed information on individuals
    • Nonobvious relationship awareness (NORA)
      • Combining data from multiple sources to find obscure hidden connections that might help identify criminals or terrorists
Credit card purchases can make personal information available to market researchers, telemarketers, and direct-mail companies. Advances in information technology facilitate the invasion of privacy.
NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

Figure 12-2
• Basic concepts for ethical analysis
  • Responsibility:
    • Accepting the potential costs, duties, and obligations for decisions
  • Accountability:
    • Mechanisms for identifying responsible parties
  • Liability:
    • Permits individuals (and firms) to recover damages done to them
  • Due process:
    • Laws are well known and understood, with an ability to appeal to higher authorities
Ethical analysis: A five-step process

1. Identify and clearly describe the facts.

2. Define the conflict or dilemma and identify the higher-order values involved.

3. Identify the stakeholders.

4. Identify the options that you can reasonably take.

5. Identify the potential consequences of your options.
Candidate Ethical Principles

- **Golden Rule**
  - Do unto others as you would have them do unto you.

- **Immanuel Kant’s Categorical Imperative**
  - If an action is not right for everyone to take, it is not right for anyone.

- **Descartes’ Rule of Change**
  - If an action cannot be taken repeatedly, it is not right to take at all.
• Candidate Ethical Principles (cont.)

• Utilitarian Principle
  • Take the action that achieves the higher or greater value.

• Risk Aversion Principle
  • Take the action that produces the least harm or least potential cost.

• Ethical “No Free Lunch” Rule
  • Assume that virtually all tangible and intangible objects are owned by someone unless there is a specific declaration otherwise.
• Professional codes of conduct
  • Promulgated by associations of professionals
    • E.g., AMA, ABA, AITP, ACM
  • Promises by professions to regulate themselves in the general interest of society

• Real-world ethical dilemmas
  • One set of interests pitted against another
  • E.g., right of company to maximize productivity of workers versus workers right to use Internet for short personal tasks
Information Rights: Privacy and Freedom in the Internet Age

• Privacy:
  • Claim of individuals to be left alone, free from surveillance or interference from other individuals, organizations, or state. Claim to be able to control information about yourself.

• In the United States, privacy protected by:
  • First Amendment (freedom of speech)
  • Fourth Amendment (unreasonable search and seizure)
  • Additional federal statues (e.g., Privacy Act of 1974)
The Moral Dimensions of Information Systems

- **Fair information practices:**
  - Set of principles governing the collection and use of information
  - Basis of most U.S. and European privacy laws
  - Based on mutuality of interest between record holder and individual
  - Restated and extended by FTC in 1998 to provide guidelines for protecting online privacy
  - Used to drive changes in privacy legislation
    - COPPA
    - Gramm-Leach-Bliley Act
    - HIPAA
The FTC FIP principles:

- **Notice/awareness (core principle):**
  - Web sites must disclose practices before collecting data.

- **Choice/consent (core principle):**
  - Consumers must be able to choose how information is used for secondary purposes.

- **Access/participation:**
  - Consumers must be able to review, contest accuracy of personal data.
• FTC FIP principles (cont.)

• Security:
  • Data collectors must take steps to ensure accuracy, security of personal data.

• Enforcement:
  • Must be mechanism to enforce FIP principles.
European Directive on Data Protection:
- Requires companies to inform people when they collect information about them and disclose how it will be stored and used.
- Requires informed consent of customer.
- EU member nations cannot transfer personal data to countries without similar privacy protection (e.g., the United States).
- U.S. businesses use safe harbor framework.
  - Self-regulating policy and enforcement that meets objectives of government legislation but does not involve government regulation or enforcement.
Internet Challenges to Privacy:

- **Cookies**
  - Tiny files downloaded by Web site to visitor’s hard drive.
  - Identify visitor’s browser and track visits to site.
  - Allow Web sites to develop profiles on visitors.

- **Web bugs**
  - Tiny graphics embedded in e-mail messages and Web pages
  - Designed to monitor who is reading message and transmit information to another computer

- **Spyware**
  - Surreptitiously installed on user’s computer
  - May transmit user’s keystrokes or display unwanted ads
How Cookies Identify Web Visitors

Cookies are written by a Web site on a visitor’s hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.

Figure 12-3
• The United States allows businesses to gather transaction information and use this for other marketing purposes.

• Online industry promotes self-regulation over privacy legislation.

• However, extent of responsibility taken varies:
  • Statements of information use
  • Opt-out selection boxes
  • Online “seals” of privacy principles

• Most Web sites do not have any privacy policies.
• Technical solutions
  • The Platform for Privacy Preferences (P3P)
    • Allows Web sites to communicate privacy policies to visitor’s Web browser—user
    • User specifies privacy levels desired in browser settings
    • E.g., “medium” level accepts cookies from first-party host sites that have opt-in or opt-out policies but rejects third-party cookies that use personally identifiable information without an opt-in policy.
Web sites are posting their privacy policies for visitors to review. The TRUSTe seal designates Web sites that have agreed to adhere to TRUSTe’s established privacy principles of disclosure, choice, access, and security.
The P3P Standard

P3P enables Web sites to translate their privacy policies into a standard format that can be read by the user’s Web browser software. The user’s Web browser software evaluates the Web site’s privacy policy to determine whether it is compatible with the user’s privacy preferences.

1. The user with P3P Web browsing software requests a Web page.
2. The Web server returns the Web page along with a compact version of the Web site’s policy and a pointer to the full P3P policy. If the Web site is not P3P compliant, no P3P data are returned.
3. The user’s Web browsing software compares the response from the Web site with the user’s privacy preferences. If the Web site does not have a P3P policy or the policy does not match the privacy levels established by the user, it warns the user or rejects the cookies from the Web site. Otherwise, the Web page loads normally.

Figure 12-4
Property Rights: Intellectual Property

- Intellectual property: intangible property of any kind created by individuals or corporations
- Three main ways that intellectual property is protected
  - Trade secret: intellectual work or product belonging to business, not in the public domain
  - Copyright: statutory grant protecting intellectual property from being copied for the life of the author, plus 70 years
  - Patents: grants creator of invention an exclusive monopoly on ideas behind invention for 20 years
• Challenges to intellectual property rights
  • Digital media different from physical media (e.g., books)
    • Ease of replication
    • Ease of transmission (networks, Internet)
    • Difficulty in classifying software
    • Compactness
    • Difficulties in establishing uniqueness

• Digital Millennium Copyright Act (DMCA)
  • Makes it illegal to circumvent technology-based protections of copyrighted materials
• Accountability, liability, control

• Computer-related liability problems

• If software fails, who is responsible?
  • If seen as part of machine that injures or harms, software producer and operator may be liable.
  • If seen as similar to book, difficult to hold author/publisher responsible.
  • What should liability be if software seen as service? Would this be similar to telephone systems not being liable for transmitted messages?
System quality: data quality and system errors

- What is an acceptable, technologically feasible level of system quality?
  - Flawless software is economically unfeasible.

- Three principal sources of poor system performance:
  - Software bugs, errors
  - Hardware or facility failures
  - Poor input data quality (most common source of business system failure)
Quality of Life: Equity, Access, and Boundaries

• Negative social consequences of systems
  • Balancing power: although computing power decentralizing, key decision making remains centralized
  • Rapidity of change: businesses may not have enough time to respond to global competition
  • Maintaining boundaries: computing, Internet use lengthens work-day, infringes on family, personal time
  • Dependence and vulnerability: public and private organizations ever more dependent on computer systems
• **Computer crime and abuse**
  - Computer crime: commission of illegal acts through use of compute or against a computer system—computer may be object or instrument of crime
  - Computer abuse: unethical acts, not illegal
    - Spam: high costs for businesses in dealing with spam
• **Employment:**
  - Reengineering work resulting in lost jobs
• **Equity and access—the digital divide:**
  - Certain ethnic and income groups in the United States less likely to have computers or Internet access
Health risks:

- Repetitive stress injury (RSI)
  - Largest source is computer keyboards
  - Carpal Tunnel Syndrome (CTS)
- Computer vision syndrome (CVS)
- Technostress
- Role of radiation, screen emissions, low-level electromagnetic fields
Although some people enjoy the convenience of working at home, the do anything anywhere computing environment can blur the traditional boundaries between work and family time.
Repetitive stress injury (RSI) is the leading occupational disease today. The single largest cause of RSI is computer keyboard work.