Ethical and Social Issues in Information Systems


Learning Objectives

• Identify the ethical, social, and political issues that are raised by information systems.
• Identify the principles for conduct that can be used to guide ethical decisions.
• Evaluate the impact of contemporary information systems and the Internet on the protection of individual privacy and intellectual property.
• Assess how information systems have affected everyday life.

Ethical and Social Issues Related to Systems (1/4)

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

Ethical and Social Issues Related to Systems (2/4)

• A model for thinking about ethical, social, and political issues
  • Society as a calm pond
  • IT as a 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.

Key Technology Trends That Raise Ethical Issues (1/3)

- Four key technology trends that raise ethical issues
  - Computing power doubles every 18 months
    - Increased reliance on, and vulnerability to, computer systems
  - Data storage costs rapidly declining
    - Multiplying databases on individuals

Key Technology Trends That Raise Ethical Issues (2/3)

- Four key technology trends that raise ethical issues (cont.)
  - Data analysis advances
    - Greater ability to find detailed personal information on individuals
    - Profiling and nonobvious relationship awareness (NORA)
  - Networking advances and the Internet
    - Enables moving and accessing large quantities of personal data

- Five moral dimensions of information age
  - Major issues raised by information systems include:
    - Information rights and obligations
    - Property rights and obligations
    - Accountability and control
    - System quality
    - Quality of life

Figure 4-1
Nonobvious Relationship Awareness (NORA)

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.

Figure 4-2

• Basic concepts form the underpinning of an ethical analysis of information systems and those who manage them
  • 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
Ethics in an Information Society (4/5)

- **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

Ethics in an Information Society (5/5)

- **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 vs. workers right to use Internet for short personal tasks

Information rights and obligations (1/9)

- **Privacy**
  - Claim of individuals to be left alone, free from surveillance or interference from other individuals, organizations, or the state.
  - Ability to control information about yourself
  - In U.S., privacy protected by:
    - First Amendment (freedom of speech)
    - Fourth Amendment (unreasonable search and seizure)
    - Additional federal statues
    - Privacy Act of 1974

Information rights and obligations (2/9)

- **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
Information rights and obligations (3/9)

- 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
  - Security: Data collectors must take steps to ensure accuracy, security of personal data
  - Enforcement: Must be mechanism to enforce FIP principles

Information rights and obligations (4/9)

- 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 (not true in the U.S.)
  - EU member nations cannot transfer personal data to countries without similar privacy protection (e.g. U.S.)
  - 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.

Information rights and obligations (5/9)

- 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 a message and transmitting that information to another computer on the Internet
  - Spyware
    - Surreptitiously installed on user’s computer
    - May transmit user’s keystrokes or display unwanted ads

Information rights and obligations (6/9)

How Cookies Identify Web Visitors

- Figure 4-3
  - How Cookies Identify Web Visitors
    1. The Web server reads the user’s Web browser and determines the operating system, browser name, version number, Internet address, and other information.
    2. The server transmits a tiny text file with user identification information called a cookie, which the user’s browser receives and stores on the user’s computer hard drive.
    3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user’s computer.
    4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

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.
Information rights and obligations (7/9)

• U.S. allows businesses to gather transaction information and use this for other marketing purposes
• Online industry promotes self-regulation over privacy legislation
• Self regulation has proven highly variable
  • Statements of information use are quite different
  • Some firms offer opt-out selection boxes
  • Online “seals” of privacy principles
• Most Web sites do not have any privacy policies
• Many online privacy policies do not protect customer privacy, but rather protect the firm from lawsuits

Information rights and obligations (8/9)

• 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.

Information rights and obligations (9/9)

The P3P Standard

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, the user or rejects the cookies from the Web site. Otherwise, the Web page loads normally.

Figure 4-4

The P3P Standard 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.

Property Rights: Intellectual Property (1/3)

• Intellectual property: Intangible property of any kind created by individuals or corporations
• Three 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
Property Rights: Intellectual Property (2/3)

- 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 Millenium Copyright Act (DMCA)
  - Makes it illegal to circumvent technology-based protections of copyrighted materials

System Quality: Data Quality and System Errors (1/4)

- 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)

Property Rights: Intellectual Property (3/3)

- Accountability, Liability, Control
  - Computer-related liability problems
    - If software fails, who is responsible?
      - If seen as a part of a machine that injures or harms, software producer and operator may be liable
      - If seen as similar to a book, difficult to hold software author/publisher responsible
    - What should liability be if software is seen as service? Would this be similar to telephone systems not being liable for transmitted messages (so-called “common carriers”)

System Quality: Data Quality and System Errors (2/4)

- Quality of Life: Negative social consequences of systems
  - Balancing power: Although computing power is decentralizing, key decision-making power remains centralized
  - Rapidity of change: Businesses may not have enough time to respond to global competition
  - Maintaining boundaries: Computing and Internet use lengthens the work-day, infringes on family, personal time
  - Dependence and vulnerability: Public and private organizations ever more dependent on computer systems
System Quality: Data Quality and System Errors (3/4)

- **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

System Quality: Data Quality and System Errors (4/4)

- **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