

Chapter 4

Ethical and Social Issues in Information Systems

Learning Objectives

- 4.1 Describe IT/IS-related ethical, social, and political issues.
- 4.2 Describe principles for ethical conduct.
- 4.3 Discuss information rights and privacy issues.
- 4.4 Discuss intellectual property issues.
- 4.5 Discuss system quality issues.
- 4.6 Discuss accountability and control issues.
- 4.7 Discuss quality of life issues
- 4.8 Understand how the information in this chapter can help your career.

Video Cases

- Case 1: What Net Neutrality Means for You
[What Net Neutrality Means For You - YouTube](#)
- Case 2: Facebook and Google Privacy: What Privacy?
- Case 3: United States v. Terrorism: Data Mining for Terrorists and Innocents
- Instructional Video: Viktor Mayer-Schönberger on the Right to Be Forgotten

The Double-Edged Nature of Currencies of the Future: Central Bank Digital Currencies

- Problem
 -
- Solutions
 -
- Results
 -
 -

Describe IT/IS-related ethical, social, and political issues (1 of 2)

- Recent cases of failed ethical judgment in business
 - Volkswagen AG, Wells Fargo, FX, Robinhood
 - 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

* The Madoff Ponzi scheme is instructive: systems were used for more than twenty years to fool investors, regulators, and investigators about the true nature of Madoff's business.

Describe IT/IS-related ethical, social, and political issues (2 of 2)

- Information systems raise new ethical questions because they create opportunities for:
 - Intense social change, threatening existing distributions of power, money, rights, and obligations
- New opportunities for crime
- New kinds of crimes

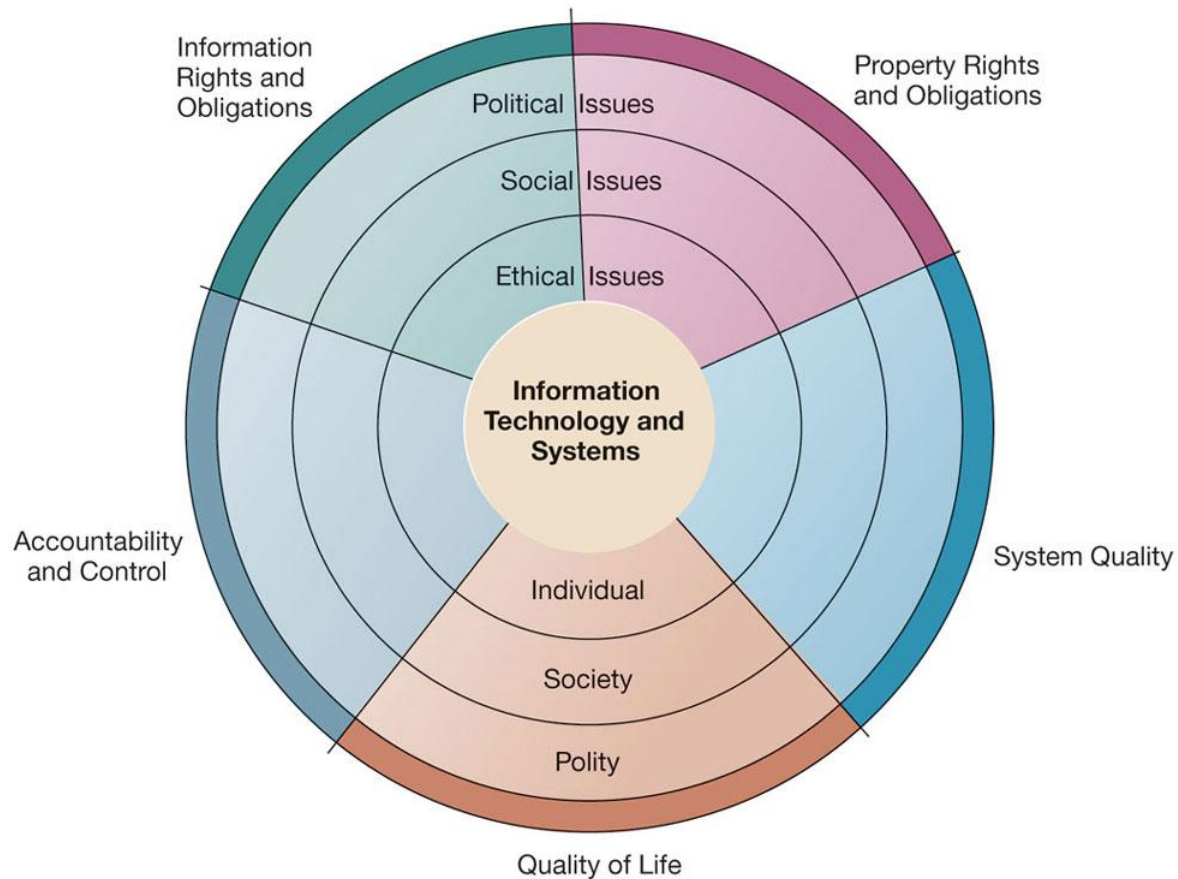
* Consider some of the ethical dilemmas that are presented by information systems and new developments in technology. Privacy is an important issue—understand that the business models of Google, Facebook, and many other sites depend on getting users to give up their personal information so it can be used to market and sell them products.

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

Figure 4.1 The Relationship Between Ethical, Social, and Political Issues in an Information Society

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.



Five Moral Dimensions of the Information Age

- Information rights and obligations
- Property rights and obligations
- Accountability and control
- System quality
- Quality of life

Consider examples of each of the five major issues. **For example**, an issue dealing with information rights might be, what rights do individuals possess with respect to themselves? What do they have a right to protect? An issue dealing with quality of life might be: what values should be preserved in an information- and knowledge-based society? An issue dealing with system quality might be: what standards of data and system quality should we demand to protect individual rights and the safety of society?

Key Technology Trends That Raise Ethical Issues

- Ever-increasing rise in computing power
 - More organizations depend on computer systems for critical operations.

* Moore's law
- Rapid decline of data storage costs
 - Organizations can easily maintain detailed databases on individuals.
- Advances in data analysis and networking advances and the Internet
 - Copying data from one location to another and accessing personal data from remote locations are much easier.
- Mobile device growth impact
 - Tracking of individual cell phones
- **AI:** may violate ethical and moral standards; challenges to privacy and intellectual property rights

Advances in Data Analysis Techniques

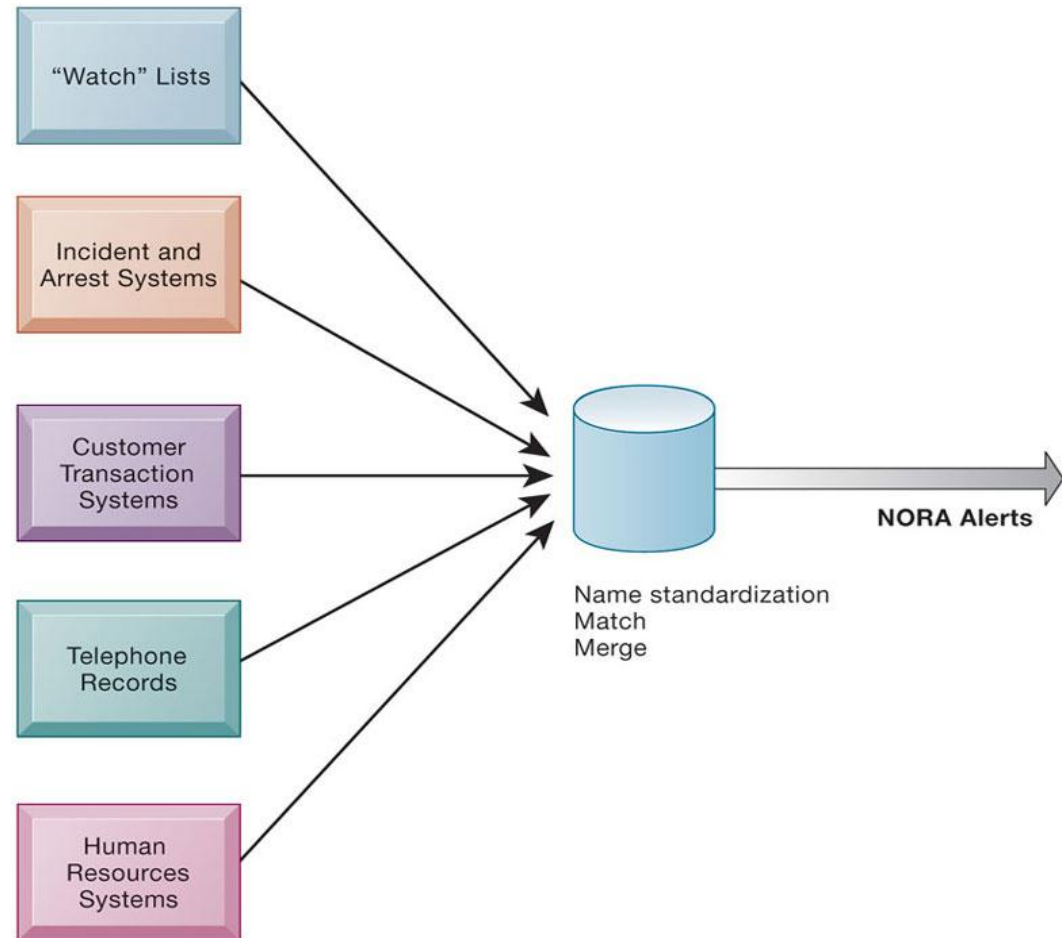
- Profiling
 - Combining data from multiple sources to create dossiers of detailed information on individuals
- Nonobvious relationship awareness (**NORA**)
 - Combining data from multiple sources to find obscure hidden connections that might help identify criminals or terrorists

Files; a pile of documents

* **Online profiling** is one of the most controversial computer-related ethical, social, and political issues today. Although it is used fairly extensively on the Internet, it is also used by insurance firms, health insurance firms, casinos, and of course national authorities around the globe for finding potential terrorists, as well as domestic opponents.

Figure 4.2 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 and issue an alert to the hiring manager.



- NORA is used by both the government and the private sector for its profiling capabilities. One example might be an airline identifying potential terrorists attempting to board a plane. Another might be government identifying potential terrorists by monitoring phone calls.

Principles to Guide Ethical Decisions

Information systems do not exist in a vacuum and that these concepts are instrumental in understanding the impact of systems and measuring their success. Why liability and due process are such important ethical concepts? (A rough answer would be that they provide recourse to individuals negatively effected by mismanagement of information systems, providing incentive to “play by the rules”.)

- **Basic concepts for ethical analysis**

- **Responsibility:** a key element of ethical action
 - Accepting the potential costs, duties, and obligations for decisions
- **Accountability:** a feature of systems and social institutions; systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action
 - Mechanisms are in place to determine who took responsible action, and who is responsible
- **Liability:** extends the concept of responsibility further to the area of laws, a feature of political systems in which a body of laws is in place that permits individuals (and firms) to recover the damages done to them by other actors, systems, or organizations
- **Due process:** a related feature of law-governed societies and is a process in which
 - Laws are well-known and understood, with an ability to appeal to higher authorities to ensure that the laws are applied correctly

Ethical Analysis

- Five-step process for ethical analysis
 1. Identify and describe the facts clearly.
 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.

Ethical Principles (1 of 2)

- **Golden Rule**

c.f. 己所不欲勿施於人

자기가 하기 싫은 일을 남에게도 하게 해서는 안 됨

- Do unto others as you would have them do unto you

- **Immanuel Kant's Categorical Imperative**

Difference
?
-> refer to
below!

- If an action is not right for everyone to take, it is not right for anyone

- **Slippery Slope Rule (Descartes' Rule of Change)**

- If an action cannot be taken repeatedly, it is not right to take at all

Understand the difference! Briefly, the difference is that the categorical imperative spans the entirety of the populace, whereas the rule of change applies to the decisions of one person over time. For example, the categorical imperative applies to an employee who tries to steal money from his employer. He shouldn't do this, because if all employees attempted to do so, the company would fail. The rule of change applied to the same situation might run as follows: although the employee's stealing one dollar from the company would not lead to any true problem, repeatedly stealing one dollar, or stealing a lot of dollars, would be unacceptable and ultimately lead to the destruction of the company.

Ethical Principles (2 of 2)

- Utilitarian Principle
 - Take the action that achieves the higher or greater value
- Risk Aversion Principle
 - Take the action that produces the least harm or 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

How does the “no free lunch” rule relate to copyrights, patents, and trademarks?

Explain that the appearance of unethical behavior is as harmful as actual unethical behavior at times, so adherence to these principles are critical. In an age of “opensource software” how does the principle of “no free lunch” work out? Opensource software is an example of an economic good which is licensed by the creator for distribution often without charge, or even attribution. In this case, there is a “free lunch.” But it occurs because the creators of the software consent to this arrangement.

Professional Codes of Conduct

- Promulgated by associations of professionals
 - American Medical Association (AMA)
 - American Bar Association (ABA)
 - Association for Computing Machinery (ACM)
- Promises by professions to regulate themselves in the general interest of society

* Codes of ethics

- **Governance Codes**

- Establishing guidelines and policies, as well as implementing technical guardrails with respect to conduct-> one tool that organizations are using to help ensure ethical decision making

- Responsible AI in Chapter 11

Real-World Ethical Dilemmas

- One set of interests pitted against another
- Examples
 - Monitoring employees: Right of company to maximize productivity of workers versus workers' desire to use Internet for short personal tasks
 - Facebook monitors users and sells information to advertisers and app developers

Other ethical dilemmas include companies trying to use new systems to reduce the size of their workforce, such as using automated systems to reduce the need for human call center employees. Emphasize that in cases like these, right and wrong are not clearly defined, but instead, contrasting values are at odds with one another (companies value productivity, employees value their work and pay).

4.3 Discuss Information Rights and Privacy Issues

Information Rights: Privacy and Freedom in the Internet Age (1 of 3)

- 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 and association)
 - Fourth Amendment (unreasonable search and seizure)
 - Fifth and 14th Amendment (guarantee of due process)
 - Additional federal statutes (e.g., Privacy Act of 1974)

Information Rights: Privacy and Freedom in the Internet Age (2 of 3)

- Fair information practices (**FIP**):
 - Set of principles governing the collection and use of information (in 1973)
 - 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
- Think what is meant by a “mutuality of interest between record holder and individual.” (Briefly, the individual wants to engage in a transaction, and the record holder needs information about the individual to support the transaction—both are interested parties in the transaction.)

Information Rights: Privacy and Freedom in the Internet Age (3 of 3)

- 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 should be able to review and 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.

These five Fair Information Practices provide the foundation for all privacy legislation in the United States, and much of Europe. You might go to a popular Web site, find its privacy policy, and see how well the site conforms to the principles above. Chances are good that the Web site you choose will have several statements in their policies which permit them to do anything they want with personal information. Also, do a search on “FTC privacy” and go to one of the reports listed. A search on “FTC behavioral targeting” also produces many fine reports on the topic.

EU General Data Protection Regulation (GDPR)

- Requires unambiguous explicit informed consent of customer (in 2018)
- EU member nations cannot transfer personal data to countries without similar privacy protection
 - Applies across all EU countries to any firms operating in EU or processing data on EU citizens or residents
 - Strengthens right to be forgotten * Safe harbor
- Privacy shield agreements: All countries processing EU data must conform to GDPR requirements
- Heavy fines: \$20 million or 4% of global daily revenue

* The EU AI Act

EU protections of privacy are far more stringent/powerful than the United States because they require informed consent before a firm can do anything with personal information besides support the transaction at hand. In Europe, there is no junk postal mail for instance because advertising firms are prohibited from using personal information obtained from third parties, and without the consent of the individual.

Internet Challenges to Privacy (1 of 2)

First-party tracking (individual web sites), third-party tracking

- Cookies
 - Identify browser and track visits to site
 - Super cookies (Flash cookies)
- Web beacons (web bugs; tracking file)
 - Tiny graphics embedded in e-mails and web pages
 - Monitor who is reading email message or visiting site
- Spyware Adware
 - Surreptitiously installed on user's computer
 - May transmit user's keystrokes or display unwanted ads
- Google services and behavioral targeting (aka interest-based advertising)

Internet Challenges to Privacy (2 of 2)

- The United States allows businesses to gather transaction information and use this for other marketing purposes.
- **Opt-out model** vs. **Opt-in model** (of informed consent)
- Online industry promotes self-regulation over privacy legislation.
 - Complex/ambiguous privacy statements
 - Opt-out models selected over opt-in
 - Online “seals” of privacy principles

- Cookie banners: a pop-up window that allows users to accept or reject cookies from the site

✓ **Challenges Posed by AI:**

- The collection of data for use by facial recognition systems (Chap. 11) has been the subject of much concern.

Do you believe that businesses should be pressed to provide more comprehensive privacy protections online? Businesses prefer the looser regulation, but individuals may not. Also most individuals do not take the proper steps to ensure their own privacy in any case. Most people do not know how to protect their privacy online. Does that mean that privacy is unimportant or that people don't care?

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.
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.

Technical Solutions

- Solutions include:
 - Email encryption
 - Anonymity tools
 - Anti-spyware tools
- Overall, technical solutions have failed to protect users from being tracked from one site to another
 - Browser features
 - “Private” browsing
 - “Do not track” options

- There are a few technologies that can protect user privacy during interactions with Web sites.
- For the most part, technical solutions have failed to protect users from being tracked as they move from one site to another.
- There is no online ads industry agreement on how to respond to Do Not Track requests, and currently no legislation requiring Web sites to stop tracking.

4.4 Discuss Intellectual Property Issues

- Intellectual property
 - Tangible and intangible products of the mind created by individuals or corporations
- Protected in **four main ways**:
 - **Copyright**: : statutory grant protecting intellectual property from being copied for the life of the author, plus 70 years; + Corporate-owned works-> 95 years
 - **Patents**: grants creator of invention an exclusive monopoly on ideas behind invention for 20 years
 - **Trademarks**
 - **Trade secrets**: intellectual work or product belonging to business, not in the public domain

Challenges to Intellectual Property Rights

- Digital media different from physical media (e.g., books)
 - Ease of replication
 - Ease of transmission (networks, Internet)
 - Ease of alteration
 - Difficulty in classifying software
 - Ease of theft because of compactness
 - Difficulties in establishing uniqueness
- Digital Millennium Copyright Act (DMCA) 1998

- Makes it illegal to circumvent technology-based protections of copyrighted materials

* **SIIA** (Software and Information Industry Association) by MS, major software and information content firms-> runs an antipiracy hotline for individuals to report piracy activities, offers educational programs to help organizations combat software piracy, ...

Computer-Related Liability Problems

- If software fails, who is responsible?
- If seen as part of a machine that injures or harms, software producer and operator may be liable
- If seen as similar to book, difficult to hold author/publisher responsible
- If seen as a service, would this be similar to telephone systems not being liable for transmitted messages?

*** Challenges Posed by AI**

Spotlight on Organizations Case Study: Section 230 Under Fire

- Case Study Questions
 - What are the ethical, social, and political issues that Internet platforms face with respect to user content?
 - Do you think Section 230 should be repealed or amended? Why or why not?
 - In what ways does the controversy over Section 230 illustrate the difficulties of creating laws governing the use of new digital technologies?

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)
 - The s/w industry has not yet arrived at testing standards that would result in s/w of acceptable but imperfect performance

Quality of Life: Equity, Access, Boundaries (1 of 3)

- **Negative social consequences of systems**
- Big Tech: concentrating economic and political power; EU Digital Market Act (**DMA**; 2024) aims to prevent “gatekeeper” platforms from exploiting their interlocking products and services to lock in their users and squash potential rivals.
- Rapidity of change: reduced response time to competition-> businesses may not have enough time to respond to global competition
- Maintaining boundaries: family, work, and leisure-> 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

Quality of Life: Equity, Access, Boundaries (2 of 3)

- Computer crime and abuse
 - Computer crime: commission of illegal acts through use of computer 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; most originates from bot networks. More tightly regulated in Europe than in the US.
 - CAN-SPAM Act (US, 2003) does not outlaw spamming but does ban deceptive email practices. It prohibits the use of fake return addresses.
- Employment
 - Trickle-down technology
 - Reengineering work resulting in job loss

Quality of Life: Equity, Access, Boundaries (3 of 3)

* **Time-wasting** gap: children of higher-income families are far more likely to use Internet access to pursue educational goals, whereas lower-income children are much more likely to spend time on entertainment and games

- Equity and access
 - The digital divide: Certain ethnic and income groups in the United States less likely to have computers or Internet access
- Physical, Mental, and Cognitive Health Risks
 - **Repetitive stress injury (RSI)**: Largest source is computer keyboards
 - **Carpal tunnel syndrome (CTS)**: the most common kind of computer-related RSI
 - **Computer vision syndrome (CVS)**: Eyestrain and headaches related to screen use
 - **Technostress**: Aggravation, impatience, fatigue

Understand How the Information in This Chapter Can Help Your Career

- **Real-World Scenario**

Cermentos Argos Uses Privacy Analysts to Cement
Competitive Advantage