Ethics in Information Technology, Fourth Edition

Chapter 4
Privacy

Objectives

- As you read this chapter, consider the following questions:
  - What is the right of privacy, and what is the basis for protecting personal privacy under the law?
  - What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?
  - What is identity theft, and what techniques do identity thieves use?

Privacy Protection and the Law

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

Information Privacy

- Definition of privacy
  - "The right to be left alone—the most comprehensive of rights, and the right most valued by a free people"
- Information privacy is a combination of:
  - Communications privacy
    - Ability to communicate with others without being monitored by other persons or organizations
  - Data privacy
    - Ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use

Privacy Laws, Applications, and Court Rulings

- Legislative acts passed over the past 40 years
  - Most address invasion of privacy by the government
  - No protection of data privacy abuses by corporations
  - No single, overarching national data privacy policy

Privacy Laws, Applications, and Court Rulings (cont'd.)

- Financial data
  - Fair Credit Reporting Act (1970)
    - Regulates operations of credit-reporting bureaus
  - Fair and Accurate Credit Transactions Act (2003)
    - Allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies
  - Right to Financial Privacy Act (1978)
    - Protects the financial records of financial institution customers from unauthorized scrutiny by the federal government

Privacy Laws, Applications, and Court Rulings

- Electronic surveillance (cont'd.)
  - Foreign Intelligence Surveillance Act (FISA) of 1978
    - Describes procedures for electronic surveillance and collection of foreign intelligence information in communications between foreign powers and agents of foreign powers

Privacy Laws, Applications, and Court Rulings (cont'd.)

- Electronic surveillance (cont'd.)
  - Electronic Communications Privacy Act of 1986 (ECPA)
    - Protects communications in transfer from sender to receiver
    - Protects communications held in electronic storage
    - Prohibits recording dialing, routing, addressing, and signaling information without a search warrant

Key Privacy and Anonymity Issues

- Identity theft
- Electronic discovery
- Consumer profiling
- Treating customer data responsibly
- Workplace monitoring
- Advanced surveillance technology

Identity Theft

- Theft of key pieces of personal information to impersonate a person, including:
  - Name
  - Address
  - Date of birth
  - Social Security number
  - Passport number
  - Driver's license number
  - Mother's maiden name

Identity Theft (cont'd.)

- Fastest-growing form of fraud in the United States
- Consumers and organizations are becoming more vigilant and proactive in fighting identity theft
- Four approaches used by identity thieves
  - Create a data breach
  - Purchase personal data
  - Use phishing to entice users to give up data
  - Install spyware to capture keystrokes of victims

Identity Theft (cont'd.)

- Phishing
  - Stealing personal identity data by tricking users into entering information on a counterfeit Web site
- Spyware
  - Keystroke-logging software
  - Enables the capture of:
    - Account usernames
    - Passwords
    - Credit card numbers
    - Other sensitive information
  - Operates even if infected computer is not online

Electronic Discovery

- Collection, preparation, review, and production of electronically stored information for use in criminal and civil actions
- Quite likely that information of a private or personal nature will be disclosed during e-discovery
- Federal Rules of Procedure define e-discovery processes
- E-discovery is complicated and requires extensive time to collect, prepare, and review data

Electronic Discovery (cont'd.)

- Raises many ethical issues
  - Should an organization attempt to destroy or conceal incriminating evidence?
  - To what degree must an organization be proactive and thorough in providing evidence?
  - Should an organization attempt to "bury" incriminating evidence in a mountain of trivial, routine data?

Consumer Profiling

- Companies openly collect personal information about Internet users
- Cookies
  - Text files that a Web site can download to visitors' hard drives so that it can identify visitors later
- Tracking software analyzes browsing habits
- Similar controversial methods are used outside the Web environment

Consumer Profiling (cont'd.)

- Aggregating consumer data
  - Databases contain a huge amount of consumer behavioral data
  - Affiliated Web sites are served by a single advertising network

Consumer Profiling (cont'd.)

- Four ways to limit or stop the deposit of cookies on hard drives
  - Set the browser to limit or stop cookies
  - Manually delete them from the hard drive
  - Download and install a cookie-management program
  - Use anonymous browsing programs that don't accept cookies

Treating Consumer Data Responsibly (cont'd.)

TABLE 4-6 Manager's checklist for treating consumer data responsibly

Question	Yes	No
Does your company have a written data privacy policy that is followed?		
Can consumers easily view your data privacy policy?		
Are consumers given an opportunity to opt in or opt out of your data policy?		
Do you collect only the personal information needed to deliver your product or service?		
Do you ensure that the information is carefully protected and accessible only by those with a need to know?		
Do you provide a process for consumers to review their own data and make corrections?		
Do you inform your customers if you intend to use their information for research or marketing and provide a means for them to opt out?		
Have you identified a person who has full responsibility for implementing your data policy and dealing with consumer data issues?		

Source Line: Course Technology/Cengage Learning.

Treating Consumer Data Responsibly (cont'd.)

2. Company's Obligations. Company shall provide User with access to the Software and user products. Company will be available during normal business hours for support on User inquiries. Users will designate a primary contact to send and receive inquiries.

3. Registration. Company shall send User a registration code within seven (7) business days after reception of valid order form and (if required) advance payment. This code enables User access to the cloud-based services.

4. Basic Information Provided By User For A Paid Subscription. In order to provide services to User, Company may collect from User and store in its cloud or other storage system basic information including, without limitation, User's name, address, telephone number(s), email address(es), and information regarding the User or other products, equipment and/or systems present in User premises (collectively, "Basic Information"). Company shall have the right to use Basic Information for any purpose related to Company's internal business activities, and to share Basic Information with Company's authorized third party dealers who may use such information for any internal purpose related to their respective business activities.

10. Privacy.

10.1 Company collects User information in an effort to improve User's online experience, and to communicate with User about Company's products, services and promotions. Company does not sell or rent User's personal information to third parties. Company does, however, share User's information with third parties that provide services on Company's behalf or with whom Company has partnered to offer a particular product or service.

10.2 If Company privacy policy changes, Company shall post an updated version on Company's website. The policy revision date will be posted at the top of the page. User may exercise User's choices about how Company collects User information from time to time.

10.3 Company may collect information — User voluntarily submits to Company, for example:
(i) Identifying information such as User's name and email address;
(ii) Security information such as User's username, password, and acceptance of policies, licenses and warranties;
(iii) Contact information such as User's company name, mailing address and phone number;
(iv) Billing information such as credit card, expiration date, billing address and account history;
(v) Queries to Customer Service and Technical Support;
(vi) site behavior such as pages visited, downloads, or searches requested;
(vii) Browser information such as browser version, IP address, and the presence of various plug-ins and tools. While Company may possess social security numbers of our employees, consultants and contractors, Company does not collect social security numbers of website users.

10.4 Company collects information from User when User voluntarily submit that information to Company, including, for example: registering on our websites, placing an order, subscribing to services, participating in one of our surveys, contests or promotions, attending a company seminar, training session or trade show booth, requesting literature, or contacting Company for technical or customer support.

Workplace Monitoring

- Employers monitor workers
  - Protect against employee abuses that reduce worker productivity or expose employer to harassment lawsuits
- Fourth Amendment cannot be used to limit how a private employer treats its employees
  - Public-sector employees have far greater privacy rights than in the private industry
- Privacy advocates want federal legislation
  - To keep employers from infringing upon privacy rights of employees

Advanced Surveillance Technology

- Camera surveillance
  - Many cities plan to expand surveillance systems
  - Advocates argue people have no expectation of privacy in a public place
  - Critics concerned about potential for abuse
- Global positioning system (GPS) chips
  - Placed in many devices
  - Precisely locate users
  - Banks, retailers, airlines eager to launch new services based on knowledge of consumer location

Summary (cont'd.)

- Identity theft is fastest-growing form of fraud
- E-discovery can be expensive, can reveal data of a private or personal data, and raises many ethical issues
- Web sites collect personal data about visitors
- Consumer data privacy has become a major marketing issue

Summary (cont'd.)

- Employers monitor employees to maintain employee productivity and limit exposure to harassment lawsuits
- Advances in information technology provide new data-gathering capabilities but also diminish individual privacy
  - Surveillance cameras
  - GPS systems