CYBER LAW AND POLICY

Lesson 5
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?

Objectives (cont'd.)

- What are the various strategies for consumer profiling, and what are the associated ethical issues?
- What must organizations do to treat consumer data responsibly?
- Why and how are employers increasingly using workplace monitoring?
- What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

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 (cont'd.)

- Financial data (cont'd.)
  - Gramm-Leach-Bliley Act (1999)
    - Bank deregulation that enabled institutions to offer investment, commercial banking, and insurance services
    - Three key rules affecting personal privacy
      - Financial Privacy Rule
      - Safeguards Rule
      - Pretexting Rule

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

- Opt-out policy
  - Assumes that consumers approve of companies collecting and storing their personal information
  - Requires consumers to actively opt out
  - Favored by data collectors
- Opt-in policy
  - Must obtain specific permission from consumers before collecting any data
  - Favored by consumers

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

- Health information
  - Health Insurance Portability and Accountability Act (1996)
    - Improves the portability and continuity of health insurance coverage
    - Reduces fraud, waste, and abuse
    - Simplifies the administration of health insurance
  - American Recovery and Reinvestment Act (2009)
    - Included strong privacy provisions for electronic health records
    - Offers protection for victims of data breaches

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

- State laws related to security breach notification
  - Over 40 states have enacted legislation requiring organizations to disclose security breaches
  - For some states, these laws are quite stringent

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

- Children's personal data
  - Children's Online Privacy Protection Act (1998)
    - Web sites catering to children must offer comprehensive privacy policies, notify parents or guardians about its data-collection practices, and receive parental consent before collecting personal information from children under 13
  - Family Education Rights and Privacy Act (1974)
    - Assigns rights to parents regarding their children's education records
    - Rights transfer to student once student becomes 18

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

- Electronic surveillance
  - Communications Act of 1934
    - Established the Federal Communications Commission
    - Regulates all non-federal-government use of radio and television plus all interstate communications
  - Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act)
    - Regulates interception of telephone and oral communications
    - Has been amended by new laws

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

- 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
      - Pen register records electronic impulses to identify numbers dialed for outgoing calls
      - Trap and trace records originating number of incoming calls

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

- Electronic surveillance (cont'd.)
  - Communications Assistance for Law Enforcement Act (CALEA) 1994
    - Amended both the Wiretap Act and ECPA
    - Required the telecommunications industry to build tools into its products so federal investigators could eavesdrop and intercept electronic communications
    - Covered emerging technologies, such as:
      - Wireless modems
      - Radio-based electronic mail
      - Cellular data networks

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

- Electronic surveillance (cont'd.)
  - USA PATRIOT Act (2001)
    - Increased ability of law enforcement agencies to search telephone, email, medical, financial, and other records
    - Critics argue law removed many checks and balances that ensured law enforcement did not abuse its powers
    - Relaxed requirements for National Security Letters (NSLs)

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

- Export of personal data
  - Organisation for Economic Co-operation and Development Fair Information Practices (1980)
    - Fair Information Practices
      - Set of eight principles
      - Model of ethical treatment of consumer data

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

- Export of personal data (cont'd.)
  - European Union Data Protection Directive
    - Requires companies doing business within the borders of 15 European nations to implement a set of privacy directives on the fair and appropriate use of information
    - Goal to ensure data transferred to non-European countries is protected
    - Based on set of seven principles for data privacy
    - Concern that U.S. government can invoke USA PATRIOT Act to access data

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

- BBBOnLine and TRUSTe
  - Independent initiatives that favor an industry-regulated approach to data privacy
  - BBBOnLine reliability seal or a TRUSTe data privacy seal demonstrates that Web site adheres to high level of data privacy
  - Seals
    - Increase consumer confidence in site
    - Help users make more informed decisions about whether to release personal information

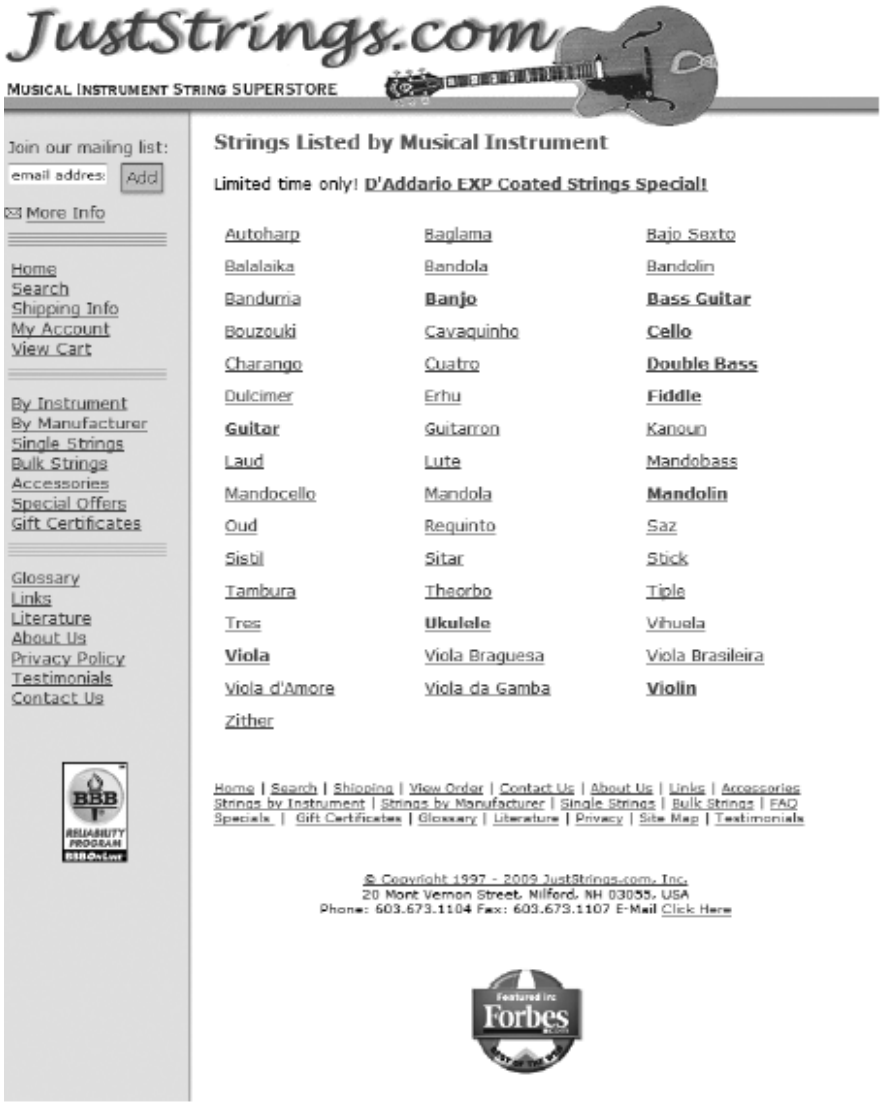

FIGURE 4-1 JustStrings.com displays the BBBOnLine Reliability Program seal

Credit: From www.juststrings.com. Reprinted by permission of JustStrings.com.

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

- Access to government records
  - Freedom of Information Act (1966 amended 1974)
    - Grants citizens the right to access certain information and records of the federal government upon request
    - Exemptions bar disclosure of information that could:
      - Compromise national security
      - Interfere with active law enforcement investigation
      - Invade someone's privacy

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

- Access to government records (cont'd.)
  - The Privacy Act of 1974
    - Prohibits government agencies from concealing the existence of any personal data record-keeping system
    - Outlines 12 requirements that each record-keeping agency must meet
    - CIA and law enforcement agencies are excluded from this act
    - Does not cover actions of private industry

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.)

- Data breaches of large databases
  - To gain personal identity information
  - May be caused by:
    - Hackers
    - Failure to follow proper security procedures
- Purchase of personal data
  - Black market for:
    - Credit card numbers in bulk—$.40 each
    - Logon name and PIN for bank account—$10
    - Identity information—including DOB, address, SSN, and telephone number—$1 to $15

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

Identity Theft (cont'd.)

- Identity Theft and Assumption Deterrence Act of 1998 was passed to fight fraud
- Identity Theft Monitoring Services
  - Monitor the three major credit reporting agencies (TransUnion, Equifax, and Experian)
  - Monitor additional databases (financial institutions, utilities, and DMV)

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
- Collecting data from Web site visits
  - Goal: provide customized service for each consumer
  - Types of data collected
    - GET data
    - POST data
    - Click-stream data

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

Consumer Profiling (cont'd.)

- Personalization software
  - Used by marketers to optimize the number, frequency, and mixture of their ad placements
    - Rules-based
    - Collaborative filtering
    - Demographic filtering
    - Contextual commerce
- Consumer data privacy
  - Platform for Privacy Preferences (P3P)
    - Shields users from sites that don't provide the level of privacy protection desired

Treating Consumer Data Responsibly

- Strong measures are required to avoid customer relationship problems
- Companies should adopt:
  - Fair Information Practices
  - 1980 OECD privacy guidelines
- Federal Trade Commission responsible for protecting privacy of U.S. consumers
- Chief privacy officer (CPO)
  - Executive to oversee data privacy policies and initiatives

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.

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

- Laws, technical solutions, and privacy policies are required to balance needs of business against rights of consumers
- A number of laws have been enacted that affect a person's privacy particularly in the areas of financial and health records, protection following a security breach, children's personal data, electronic surveillance, export of personal data, and access to government records

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
- Code of Fair Information Practices and 1980 OECD privacy guidelines provide an approach to treating consumer data responsibly

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