Ethics in Information Technology, Fourth Edition

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
  - Approve of a loan, hire a job candidate etc
- global marketplace and intensified competition have increased the importance of knowing consumers' purchasing habits and financial condition.
- Companies use this information to target marketing efforts to consumers who are most likely to buy their products and services
- Organizations also need basic information about customers to serve them better

Privacy Protection and the Law

- 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 (business and gov)
- Combination of approaches required
  - New laws – technical solutions – privacy policies

Privacy Protection and the Law

- Historical perspective on the right to privacy
  - Questions on constitution – strong government would intrude the privacy of citizens
  - Fourth Amendment reasonable expectation of privacy
  - No expectation of privacy – no privacy right
- Privacy protection from private industry
  - Few laws provide this protection

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
- No established advisory agency that recommends acceptable privacy practices to businesses

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

- Financial data
  - Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, checking and savings accounts, loans, payroll direct deposit
  - To access many of these financial products and services, individuals must use a personal logon name, password, account number, or PIN
  - Loss of this data – loss of privacy and financial loss
  - Users concerned how this data is protected

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 – opt-in and opt-out
      - Safeguards Rule – document data security/protection plan for customer data
      - Pretexting Rule – access personal information without proper authority

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

- Financial data (cont'd.)
  - Gramm-Leach-Bliley Act (1999)
    - Financial Privacy Rule – opt-in and opt-out
    - OPT-OUT
      - » Under this provision, must provide privacy notice
      - » Must also explain customer's right to opt-out to refuse to give right to collect and share personal data
      - » Inform when privacy policy is changed
      - » At the time of relationship and each year afterwards
    - OPT- IN
      - » Customers take no action, automatically opt-in and give right to share personal data

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

- Health information
  - The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread
  - They fear intrusions into their health data by employers, schools, insurance firms, law enforcement agencies, and even marketing firms looking to promote their products and services

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
  - This section covers laws that address government surveillance, including various forms of electronic surveillance.
  - New laws have been added and old laws amended in recent years in reaction to worldwide terrorist activities and the development of new communication technologies.

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
  - Various organizations have developed guidelines to ensure that the flow of personal data across national boundaries (transborder data flow) does not result in the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data

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.)

- Access to government records
  - The government has a great capacity to store data about each and every one of us and about the proceedings of its various organizations
  - **The Freedom of Information Act** enables the public to gain access to certain government records, and the Privacy Act prohibits the government from concealing the existence of any personal data record-keeping systems

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

Local Scenario

- In the existing legal framework of Pakistan, the right to privacy falls under Article 14 (1) of the Constitution, which states that the “dignity of man, and subject to law, the privacy of home, shall be inviolable”
- Only one section of the Electronic Transaction Ordinance, 2002, Article 43 (2) (e) recommends that the federal government may make regulations to provide for “privacy and protection of data of subscribers” but these are yet to be made.
- The Prevention of Electronic Crimes Act, 2016, provides for telecom and internet service providers to retain data for at least 90 days, but does not include any provisions that protect citizen’s data or privacy.
- privacy commission still does not exist, though the IT ministry is on record saying that a draft data protection law is under way

International Scenario

- The British government recently introduced a new draft data protection bill which will replace the 1998 law
  - the bill proposes tougher penalties on companies for data breaches, as well as a requirement by businesses to inform the UK information commissioner's office about any breach within 72 hours

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
- thief may apply for new credit or financial accounts, rent an apartment, set up utility or phone service, and register for college courses

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
  - Credit monitoring service
  - Recognize obvious phishing attempts
  - Improved system and practices

Identity Theft (cont'd.)

- 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.)

- Recommendations for safeguarding your identity data
  - Completely and irrevocably destroy digital identity data on used equipment
  - Shred everything
  - Require retailers to request a photo ID when accepting your credit card
  - Beware shoulder surfing
  - Minimize personal data shown on checks
  - Minimize time that mail is in your mailbox
  - Do not use debit cards to pay for online purchases
  - Use hard-to-guess passwords and PINs

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
  - Organizations are reluctant for data breaches
  - Victims need to informed – why?

Identity Theft (cont'd.)

- Data breach
  - There is no federal law requiring that organizations reveal a data breach. The state of California passed a data security breach notification law in 2002. **It was enacted when the state's payroll database was breached and victims were not notified for six weeks. The law requires that "the disclosure shall be in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement**

Identity Theft (cont'd.)

- 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.)

- Spyware
  - In 2007, the FBI planted spyware on the computer of a 15-year-old student in an attempt to identify him as the person responsible for sending numerous bomb threats to his high school. The FBI first obtained a warrant to allow the agency to install a program called the Computer and Internet Protocol Address Verifier on the student's computer. The software recorded the IP addresses, dates, and times of each communication sent from the student's computer. The student was sentenced to 90 days in juvenile detention and fined $8,852.

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

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 – preferences or online behavior
    - Collaborative filtering - similar buying habits
    - Demographic filtering – demographic information
    - Contextual commerce-product promotions

Consumer Profiling (cont'd.)

- Personalization software
  - Rules-based – preferences or online behavior
    - If you use website to book airline tickets to popular vacation spot, rules based software might ensure that you are shown adds for rental cars
  - Collaborative filtering - similar buying habits
    - If you bought a book by an author, company might recommend another book by another author. Significant percentage of other customers also bought the other book

Consumer Profiling (cont'd.)

- Personalization software
  - Demographic filtering – demographic information
    - Microsoft has captured age, sex, and location information for years through its various Web sites, including MSN and Hotmail. It has accumulated a vast database on tens of millions of people, each assigned a global user ID. Microsoft has also developed a technology based on this database that enables marketers to target one ad to men and another to women.

Consumer Profiling (cont'd.)

- Personalization software
  - Contextual Commerce – consumer recommendations based on similar buying habits
    - For example, as you read a story about white-water rafting, you may be offered a deal on rafting gear or a promotion for a white-water rafting vacation in West Virginia

Consumer Profiling (cont'd.)

- Consumer data privacy
  - Consumer data privacy major market issue
  - Companies who don't protect data
    - Lose business
    - Become defendants
- For example, privacy groups spoke out vigorously to protest the proposed merger of Web ad server DoubleClick and database marketing company Abacus Direct. The groups were concerned that the information stored in cookies would be combined with data from mailing lists, thus revealing the Web users' identities. This would enable a network advertiser to identify and track the habits of unsuspecting consumers. Public outrage and the threat of lawsuits forced DoubleClick to back off this plan.

Consumer Profiling (cont'd.)

- Opponents of consumer profiling
  - Whois using data
  - How it is being used

or who is using it. For example, when Toysmart.com went bankrupt in 2000, it planned to sell customer information from its Web site to the highest bidder, to earn cash to pay its employees and creditors. This data included names, addresses, and ages of customers and their children. TRUSTe had licensed Toysmart.com to put the TRUSTe privacy seal on its Web site, provided that Toysmart.com never divulged customer information to a third party. Because Toysmart.com was planning to violate that agreement, TRUSTe submitted a legal brief asking the bankruptcy court to withhold its approval for the proposed sale. TRUSTe officials also registered a complaint with the FTC, which launched an investigation and then filed suit to stop Toysmart.com from selling its customer list and related information, in violation of the privacy policy that appeared on the company's Web site. Finally, Walt Disney Company, which owned 60 percent of Toysmart.com, bought the list and "retired it"—both to protect customers' privacy and to put an end to the controversy.

Treating Consumer Data Responsibly

- Strong measures are required to avoid customer relationship problems
- Companies should adopt:
  - Fair Information Practices
  - Information carefully protected and shared
  - Consumers can review their own data
  - Company informs customer to use data for research – opt out
  - Companies establish corporate data policy

Treating Consumer Data Responsibly

- Chief privacy officer (CPO)
  - Executive to oversee data privacy policies and initiatives
  - Comply with governments laws and regulations
  - Must be authorized to stop/modify market initiative
  - Duties include
    - Training employees about privacy
    - Company privacy policy for risks
    - Figuring out gaps

Treating Consumer Data Responsibly

- Chief privacy officer (CPO)
  - Rationale-early involvement in such issues–less cost
  - For example, U.S. Bancorp, a bank with more than $250 billion in assets as of early 2009, appointed a CPO, but only after spending $3 million to settle a lawsuit that accused the bank of selling confidential customer financial information to telemarketers.

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
  - Reasons for monitoring
    - Less productivity
    - Comply with legal liabilities of computer users

Workplace Monitoring

- 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
  - Laws related to these continue to evolve

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 - accuracy
- 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