5e

Ethics in Information Technology

Chapter 4
Privacy

George W. Reynolds

Learning Objectives

- 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 are the various strategies for consumer profiling, and what are the associated ethical issues?

Learning Objectives

- 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

- **Bill of Rights**: Ten amendments that were ratified to protect the privacy of individuals
- **Fourth Amendment**: States that the right of the people to be secure in their persons, houses, papers, and effects must not be violated
  - Unless a warrant has been issued upon probable cause
- **Right of privacy**: Right to be left alone, the most comprehensive of rights, and most valued by free people

Information Privacy

- Combination of communications privacy and data privacy
  - Communications privacy - Ability to communicate with others without those communications being monitored by other persons or organizations
  - Data privacy - Ability to limit access to one's personal data in order to exercise control over that data and its use

Privacy Laws, Applications, and Court Rulings: Financial Data

- **Fair Credit Reporting Act**: Regulates the operations of credit-reporting bureaus
- **Right to Financial Privacy Act**: Protects the records of financial institution customers from unauthorized scrutiny by the federal government
  - Does not cover disclosures to private businesses or state and local governments

Privacy Laws, Applications, and Court Rulings: Financial Data

- **Gramm-Leach-Bliley Act (GLBA)**: Bank deregulation law that repealed the Glass-Steagall law
  - Financial privacy rule
    - **Opt out**: Customers' refusal to give the institution the right to share personal data with third parties
    - **Opt in**: Customers give financial institutions the right to share their personal data to other financial institutions

Privacy Laws, Applications, and Court Rulings: Financial Data

- Safeguards rule - Requires financial institutions to document a data security plan for clients' personal data protection
- Pretexting rule - Addresses attempts by people to access personal information without proper authority

- **Fair and Accurate Credit Transactions Act**: Allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies

Privacy Laws, Applications, and Court Rulings: Health Information

- **Health Insurance Portability and Accountability Act (HIPAA)**
  - 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**: Contains provisions for electronic health records
  - Bans the sale of health information, promotes the use of audit trails and encryption, and provides rights of access for patients

Privacy Laws, Applications, and Court Rulings: Children's Personal Data

- **Family Educational Rights and Privacy Act (FERPA)**: Assigns certain rights to parents regarding their children's educational records
- **Children's Online Privacy Protection Act (COPPA)**: Aims to give parents control over the collection, use, and disclosure of their children's personal information over the Internet
  - Does not cover the dissemination of information to children

Privacy Laws, Applications, and Court Rulings: Electronic Surveillance

- **Communications Act**: Established the Federal Communications Commission to regulate all:
  - Non-federal-government use of radio and television broadcasting
  - Interstate telecommunications and international communications that originate or terminate in the U.S.

Privacy Laws, Applications, and Court Rulings: Electronic Surveillance

- **Foreign Intelligence Surveillance Act (FISA)**: Describes procedures for the electronic surveillance and collection of **foreign intelligence** information
- **Title III of the Omnibus Crime Control and Safe Streets Act**: Regulates the interception of wire and oral communications
  - Allows law enforcement officials to use wiretapping
  - Known as the **Wiretap Act**

Privacy Laws, Applications, and Court Rulings: Electronic Surveillance

- **Electronic Communications Privacy Act (ECPA)**
  - Protection of communications while in transfer from sender to receiver
  - Protection of communications held in electronic storage
  - Prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant

Privacy Laws, Applications, and Court Rulings: Electronic Surveillance

- **National Security Letter (NSL)**: Compels holders of personal records to turn them over to the government
- **Pen register**: Records electronic impulses to identify the numbers dialed for outgoing calls
- **Trap and trace**: Records the originating number of incoming calls for a particular phone number

Privacy Laws, Applications, and Court Rulings: Electronic Surveillance

- **Communications Assistance for Law Enforcement Act (CALEA)**: Required the telecommunications industry to build tools into its products
  - For use by federal investigators, after obtaining a court order, to intercept communications

Privacy Laws, Applications, and Court Rulings: Electronic Surveillance

- **USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)**: Increased the ability of law enforcement agencies to search personal records
  - **NSL gag provision**: Prohibits NSL recipients from informing anyone that the government has secretly requested an individual's records

Privacy Laws, Applications, and Court Rulings: Electronic Surveillance

- **Foreign Intelligence Surveillance Act (FISA) Amendments Act**: Granted NSA expanded authority to collect international communications as they flow through U.S. telecom network equipment and facilities
- **Fair information practices**: Set of guidelines that govern the collection and use of personal data
  - **Transborder data flow**: Flow of personal data across national boundaries

Privacy Laws, Applications, and Court Rulings: Fair Information Practices

- Organisation for Economic Co-operation and Development (OECD) - International organization that aims to set policies and agreements on topics for which multilateral consensus is required
- **European Union Data Protection Directive**
  - Ensures that data transferred to non-European Union countries is protected
    - **European Data Protection Regulation**: Enforces a single set of rules for data protection across the EU, eliminating the need for costly administrative processes

Privacy Laws, Applications, and Court Rulings: Access to Government Records

- **Freedom of Information Act (FOIA)**: Grants citizens the right to access certain information and records of federal, state, and local governments upon request
  - Request must:
    - Not require wide-ranging, unreasonable, or burdensome searches for records
    - Be made according to procedural regulations published in the Federal Register

Privacy Laws, Applications, and Court Rulings: Access to Government Records

- **Privacy Act**: Sets rules for the collection, maintenance, use, and dissemination of personal data kept in systems of records by federal agencies
  - Prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system

Key Privacy and Anonymity Issues

Data breaches

Electronic discovery

Consumer profiling

Workplace monitoring

Advanced surveillance technology

Data Breaches

- Caused by:
  - Hackers breaking into a database
  - Failure to follow proper security procedures
- Health Information Technology for Economic and Clinical Health Act
  - Mandates that within 60 days after discovery of a data breach, each individual whose health information has been exposed must be notified

Electronic Discovery (e-discovery)

- Collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings
- **Electronically stored information (ESI)**: Any form of digital information stored on any form of electronic storage device
- E-discovery software helps:
  - Analyze large volumes of ESI quickly
  - Simplify and streamline data collection
  - Identify all participants in an investigation to determine who knew what and when

Consumer Profiling

- Information about Web surfers can be obtained through the use of:
  - **Cookies**
  - Tracking software
- Criticism - Personal data may be gathered and sold to other companies without the permission of consumers who provide the data

Workplace Monitoring

- The Fourth Amendment does not limit how a private employer treats its employees
- State privacy statutes tend to favor employers over employees
- Privacy advocates stress on the need for federal legislation to keep employers from infringing upon the privacy rights of employees

Camera Surveillance

- Goal - Deter crime and terrorist activities
- Criticism - May provide leeway for abuse and blackmail
- Domain Awareness system
  - Joint effort of the New York Police Department and Microsoft
  - Goal is to combat terrorist activities and reduce the time required to respond to an incident

Vehicle Event Data Recorder (EDR)

- Records vehicle and occupant data for a few seconds before, during, and after any vehicle crash severe enough to deploy the vehicle's air bags
- Purposes
  - To capture and record data to make changes to improve vehicle performance in the event of a crash
  - For use in a court of law to determine what happened during a vehicle accident

Stalking App

- Cell phone spy software that can be loaded onto a cell phone or smartphone
- Performs location tracking, records calls, views text messages sent or received, and records the URLs of any Web site visited on the phone
- Illegal to install the software on a phone without the permission of the phone owner

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

- 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

- 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