Chapter 4
Privacy

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 authorize electronic surveillance by the government, and what are the associated ethical issues?

• What are the two fundamental forms of data encryption, and how does each work?

Objectives (continued)

• What is identity theft, and what techniques do identity thieves use?

• What are the various strategies for consumer profiling and the associated ethical issues?

• What must organizations do to treat consumer data responsibly?

Objectives (continued)

• Why and how are employers increasingly using workplace monitoring?

• What is spamming, and what ethical issues are associated with its use?

• 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
• 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

The Right of Privacy

• Definition
  – “The right to be left alone—the most comprehensive of rights, and the right most valued by a free people”
  – “The right of individuals to control the collection and use of information about themselves”
• Legal aspects
  – Protection from unreasonable intrusion upon one’s isolation
  – Protection from appropriation of one’s name or likeness

The Right of Privacy (continued)

• Legal aspects
  – Protection from unreasonable publicity given to one’s private life
  – Protection from publicity that unreasonably places one in a false light before the public

Recent History of Privacy Protection

• Legislative acts passed over the past 40 years
  – Most address invasion of privacy by the government
    • Not corporations
  – No single, overarching national data privacy policy
  – Communications Act of 1934
  – Freedom of Information Act (FOIA)
  – Fair Credit Reporting Act of 1970
  – Privacy Act of 1974
  – Children’s Online Protection Act (COPA)
  – Gramm-Leach-Bliley Act
Recent History of Privacy Protection (continued)

- Other initiatives
  - BBB Online and TRUSTe
    - Independent, nonprofit initiatives
    - Favor an industry-regulated approach to data privacy

Recent History of Privacy Protection (continued)

- 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

Summary of the 1980 OECD Privacy Guidelines

<table>
<thead>
<tr>
<th>Principle</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Limitation</td>
<td>Limit the collection of personal data. All such data must be obtained lawfully and fairly with the subject's consent and knowledge.</td>
</tr>
<tr>
<td>Data Quality</td>
<td>Personal data should be accurate, complete, current, and relevant to the purpose for which it is used.</td>
</tr>
<tr>
<td>Purpose Specification</td>
<td>The purpose for which personal data is collected should be specified and should not be changed.</td>
</tr>
<tr>
<td>Use Limitation</td>
<td>Personal data should not be used beyond the specified purpose without a person's consent or by authority of law.</td>
</tr>
<tr>
<td>Security safeguards</td>
<td>Personal data should be protected against unauthorized access, modification, or disclosure.</td>
</tr>
<tr>
<td>Openness Principle</td>
<td>Data policies should exist and a &quot;data controller&quot; should be identified.</td>
</tr>
<tr>
<td>Individual Participation</td>
<td>People should have the right to review their data, to challenge its correctness, and to have incorrect data changed.</td>
</tr>
<tr>
<td>Accountability</td>
<td>A &quot;data controller&quot; should be responsible for ensuring that the above principles are met.</td>
</tr>
</tbody>
</table>


Legal Overview: The Privacy Act

- Secure Flight airline safety program
  - Compares the names and information of 1.4 million daily U.S. airline passengers with data on known or suspected terrorists
  - Violation of Privacy Act
Key Privacy and Anonymity Issues

- Government electronic surveillance
- Data encryption
- Identity theft
- Customer profiling
- Need to treat customer data responsibly
- Workplace monitoring
- Spamming
- Advanced surveillance techniques

Governmental Electronic Surveillance

- Federal Wiretap Act
  - Outlines processes to obtain court authorization for surveillance of all kinds of electronic communications
  - Judge must issue a court order based on probable cause
    - Almost never deny government requests
  - “Roving tap” authority
    - Does not name specific telephone lines or e-mail accounts
    - All accounts are tied to a specific person

Number of Title III Wiretaps Granted

Governmental Electronic Surveillance (continued)

- Electronic Communications Privacy Act of 1986 (ECPA)
  - Sets standards for access to stored e-mail and other electronic communications and records
  - Extends Title III’s prohibitions against the unauthorized interception, disclosure, or use of a person’s oral or electronic communications
  - Prosecutor does not have to justify requests
  - Judges are required to approve every request
Governmental Electronic Surveillance (continued)

• Electronic Communications Privacy Act of 1986 (ECPA)
  – Highly controversial
    • Especially collection of computer data sent over the Internet
  – Failed to address emerging technologies

• Foreign Intelligence Surveillance Act of 1978 (FISA)
  – Allows wiretapping of aliens and citizens in the United States
  – Based on finding of probable cause that a target is
    • Member of a foreign terrorist group
    • Agent of a foreign power
• Executive Order 12333
  – Legal authority for electronic surveillance outside the United States

Governmental Electronic Surveillance (continued)

• Communications Assistance for Law Enforcement Act (CALEA)
  – Requires the telecommunications industry to build tools into its products so that federal investigators can eavesdrop on conversations
    • After getting court approval
  – Contains a provision covering radio-based data communication
  – Includes voice over Internet (VoIP) technology

• USA Patriot Act of 2001
  – Gives sweeping new powers to
    • Domestic law enforcement
    • International intelligence agencies
  – Contains several “sunset” provisions
Data Encryption

• **Cryptography**
  – Science of encoding messages
  – Only sender and intended receiver can understand the messages
  – Key tool for ensuring confidentiality, integrity, authenticity of electronic messages and online business transactions

• **Encryption**
  – Process of converting electronic messages into a form understood only by the intended recipients

**Data Encryption (continued)**

• **Encryption key**
  – Variable value applied using an algorithm to encrypt or decrypt text

• **Public key encryption system uses two keys**
  – Message receiver’s public key - readily available
  – Message receiver’s private key - kept secret

• **RSA - a public key encryption algorithm**

• **Private key encryption system**
  – Single key to encode and decode messages
Public Key Encryption

Data Encryption (continued)

- Most people agree encryption eventually must be built into
  - Networks
  - File servers
  - Tape backup systems
- Seagate Technology hard drive
  - Automatically encrypts all data
- U.S. Arms Export Control Act controls the export of encryption technology, hardware, and software

Identity Theft

- Theft of key pieces of personal information to gain access to a person’s financial accounts
- Information includes:
  - Name
  - Address
  - Date of birth
  - Social Security number
  - Passport number
  - Driver’s license number
  - Mother’s maiden name

Identity Theft (continued)

- Fastest growing form of fraud in the United States
- Lack of initiative in informing people whose data was stolen
- Phishing
  - Attempt to steal personal identity data
  - By tricking users into entering information on a counterfeit Web site
  - Spear-phishing - a variation in which employees are sent phony e-mails that look like they came from high-level executives within their organization
Identity Theft (continued)

- Spyware
  - Keystroke-logging software
  - Enables the capture of:
    - Account usernames
    - Passwords
    - Credit card numbers
    - Other sensitive information
  - Operates even if an infected computer is not connected to the Internet
- Identity Theft and Assumption Deterrence Act of 1998 was passed to fight fraud

E-mail Used by Phishers

E-mail used by phishers:

Consumer Profiling

- Companies openly collect personal information about Internet users
- Cookies
  - Text files that a Web site puts on a user’s hard drive so that it can remember the information later
- Tracking software
- Similar methods are used outside the Web environment
- Databases contain a huge amount of consumer behavioral data

Consumer Profiling (continued)

- Affiliated Web sites
  - Group of Web sites served by a single advertising network
- Customized service for each consumer
- Types of data collected while surfing the Web
  - GET data
  - POST data
  - Click-stream data
Consumer Profiling (continued)

• Four ways to limit or even 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

• Personalization software is used by marketers to optimize the number, frequency, and mixture of their ad placements
  – Rules-based
  – Collaborative filtering
  – Demographic filtering
  – Contextual commerce

• Platform for Privacy Preferences (P3P)
  – Shields users from sites that don’t provide the level of privacy protection desired

Consumer Profiling (continued)

Treating Consumer Data Responsibly

• Strong measures are required to avoid customer relationship problems
• Code of Fair Information Practices
• 1980 OECD privacy guidelines
• Chief privacy officer (CPO)
  – Executive to oversee data privacy policies and initiatives

Manager’s Checklist for Treating Consumer Data Responsibly

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have a written data privacy policy that is followed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can consumers easily view your data privacy policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are consumers given an opportunity to opt in or out of your data policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you collect only the personal information needed to deliver your product or service?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you ensure that the information is carefully protected and accessible only by those with a need to know?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you provide a process for consumers to review their own data and make corrections?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you identified a person who has full responsibility for implementing your data policy and dealing with consumer data issues?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Workplace Monitoring

• Employers monitor workers
  – Ensures that corporate IT usage policy is followed
• 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 keeps employers from infringing upon privacy rights of employees

Spamming

• Transmission of the same e-mail message to a large number of people
• Extremely inexpensive method of marketing
• Used by many legitimate organizations
• Can contain unwanted and objectionable materials

Spamming (continued)

• Controlling the Assault of Non-Solicited Pornography and Marketing (CANSPAM)
  – Says it is legal to spam but
    • Spammers cannot disguise their identity
    • There must be a label in the message specifying that the e-mail is an ad or solicitation
    • They must include a way for recipients to indicate they do not want future mass mailings

Advanced Surveillance Technology

• Camera surveillance
  – U.S. cities plan to expand surveillance systems
  – “Smart surveillance system”
• Facial recognition software
  – Identifies criminal suspects and other undesirable characters
  – Yields mixed results
• Global Positioning System (GPS) chips
  – Placed in many devices
  – Precisely locate users
Summary

• The legal concept of the right to privacy has four aspects
• A number of laws have been enacted over the past 40 years that affect a person’s privacy
• Laws authorize electronic surveillance by the government
• Data encryption
  – Public key encryption system
  – Private key encryption system
• Identity theft

Summary (continued)

• Consumer behavior data is collected both online and offline
• Code of Fair Information Practices and 1980 OECD privacy guidelines
• Employers record and review employee communications and activities on the job
• Advances in information technology
  – Surveillance cameras
  – Facial recognition software
  – GPS systems

Essay assignment
(Due Sunday, 11th Nov)

• Suppose students living in a dormitory are given a smart card, which contains their ID and records each use of the card. What are possible good purposes of such record keeping? What are the problems with it? Is it right? Is it right if students are informed?
• Give arguments and examples to support your answers.
• (max 600 words)

Assignment
(Due Sunday, 13th Nov)

• (a) Find a website at which you can buy some things with credit cards. Look for privacy policy. Write a brief summary of it. Include URL, business name, product. How many sites you looked at before finding one with a privacy policy.
• (b) Find a recent application of smart cards. Discuss its privacy implications and protections.
• (max 600 words)