THOMSON
COURSE TECHNOLOGY

Ethics in Information Technology, Second Edition

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?

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 to the U.S. Constitution - reasonable expectation of privacy

The Right of Privacy

- Definition
  - “The right to be left alone”
  - “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

Privacy Protection

- 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 4-1 Summary of the 1980 OECD privacy guidelines

Principle	Guideline
Collection limitation	Limit the collection of personal data. All such data must be obtained lawfully and fairly with the subject's consent and knowledge.
Data quality	Personal data should be accurate, complete, current, and relevant to the purpose for which it is used.
Purpose specification	The purpose for which personal data is collected should be specified and should not be changed.
Use limitation	Personal data should not be used beyond the specified purpose without a person's consent or by authority of law.
Security safeguards	Personal data should be protected against unauthorized access, modification, or disclosure.
Openness principle	Data policies should exist and a "data controller" should be identified.
Individual participation	People should have the right to review their data, to challenge its correctness, and to have incorrect data changed.
Accountability	A "data controller" should be responsible for ensuring that the above principles are met.

Source: *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, pages 14–18, ©2002.

Legal Overview: The Privacy Act

- Prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system.
- 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

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

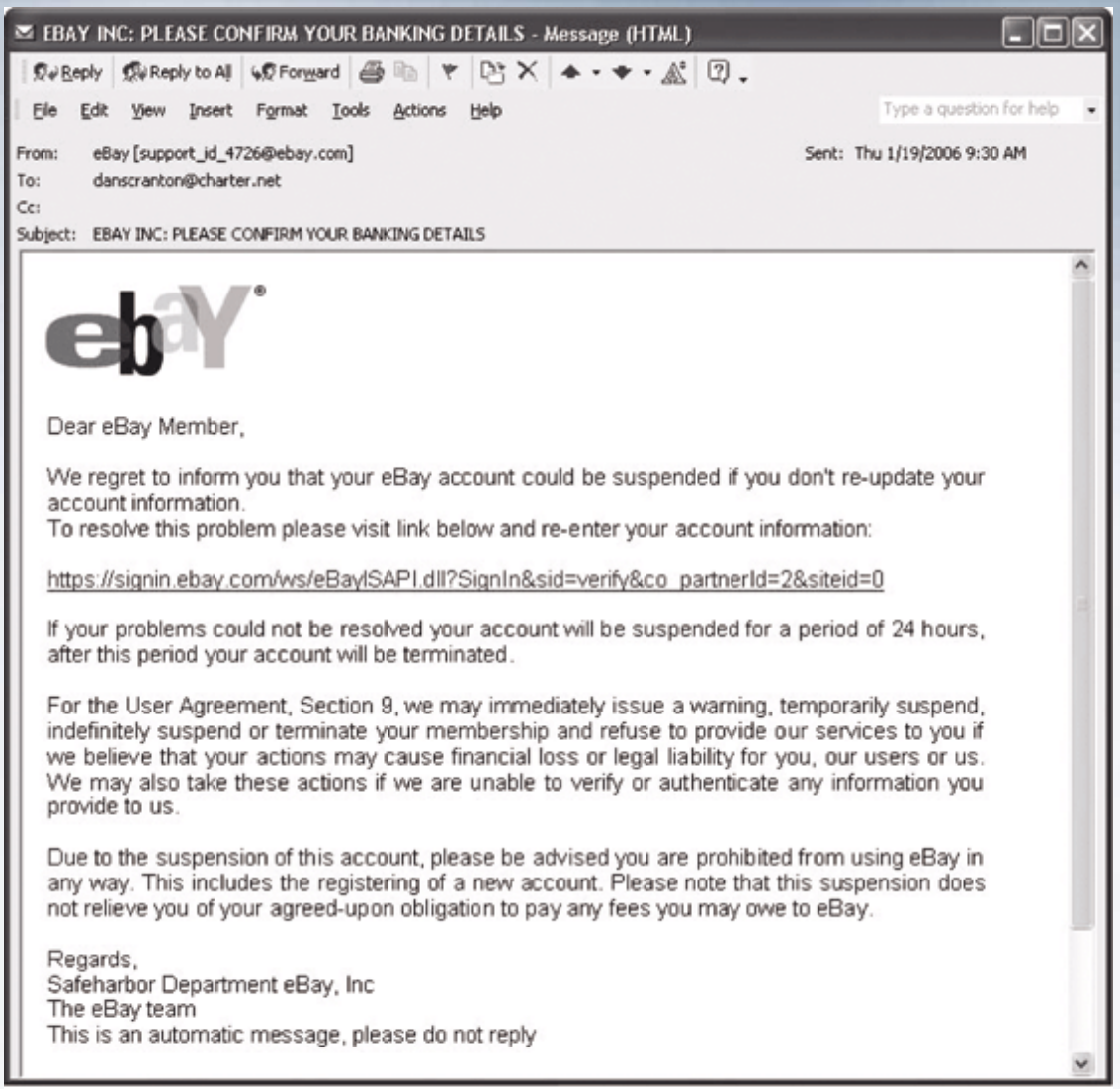
Identity Theft

- 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

E-mail Used by Phishers



EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS - Message (HTML)

Reply | Reply to All | Forward

File Edit View Insert Format Tools Actions Help

Type a question for help

From: eBay [support_id_4726@ebay.com]
Sent: Thu 1/19/2006 9:30 AM
To: danscranton@charter.net
Cc:
Subject: EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

FIGURE 4-3 E-mail used by phishers

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

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

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 4-3 Manager's checklist for treating consumer data responsibly

Questions	Yes	No
Do you 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?	____	____

Workplace Monitoring

- Employers monitor workers
  - Ensures that corporate IT usage policy is followed
- The law does not limit how a private employer treats its employees
  - Public-sector employees have far greater privacy rights than in the private industry
- Privacy advocates demand legislation
  - To keep 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)

- When is it OK to spam?
  - 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
  - "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