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?
- 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)
  - European Community Directive 95/46/EC of 1998
  - 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 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

- 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

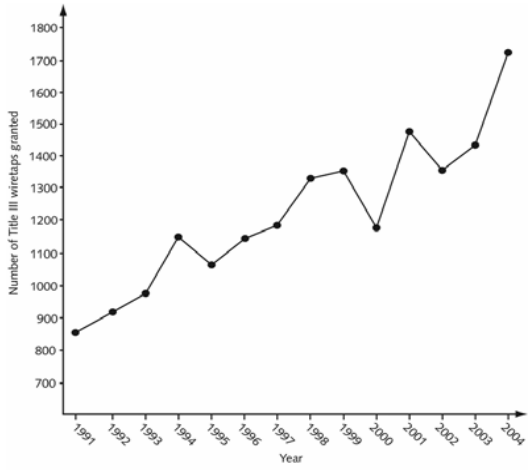
Key Privacy and Anonymity Issues

- 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



Source: Administrative Office of the U.S. Courts, www.uscourts.gov/wiretap.html for 1997-2004 wiretap reports.

FIGURE 4-1 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

Governmental Electronic Surveillance (continued)

- 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

Governmental Electronic Surveillance (continued)

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

Key Provisions of the USA Patriot Act Subject to Sunset

TABLE 4-2 Key provisions of the USA Patriot Act subject to sunset

Section	Issue addressed	Summary
201	Wiretapping in terrorism cases	Added several crimes for which federal courts may authorize wiretapping of people's communications
202	Wiretapping in computer fraud and abuse felony cases	Added computer fraud and abuse to the list of crimes the FBI may obtain a court order to investigate under Title III
203 b	Sharing wiretap information	Allows the FBI to disclose evidence obtained under Title III to other federal officials, including "law enforcement, intelligence, protective, immigration, national defense, [and] national security" officials
203 d	Sharing foreign intelligence information	Provides for disclosure of threat information obtained during criminal investigations to "appropriate" federal, state, local, or foreign government officials for the purpose of responding to the threat
204	FISA pen register/trap-and-trace exceptions	Exempts foreign intelligence surveillance from statutory prohibitions against the use of pen register or trap-and-trace devices, which capture "addressing" information about the sender and recipient of a communication. It also exempts the U.S. government from general prohibitions against intercepting electronic communications and allows stored voice-mail communication to be obtained by the government through a search warrant rather than more stringent wiretap orders.
206	FISA roving wiretaps	Expands FISA to permit "roving wiretap" authority, which allows the FBI to intercept any communications to or by an intelligence target without specifying the telephone line, computer, or other facility to be monitored
207	Duration of FISA surveillance of non-U.S. agents of a foreign power	Extends the duration of FISA wiretap orders relating to an agent of a foreign power from 90 days to 120 days, and allows an extension in 1-year intervals instead of 90-day increments

Key Provisions of the USA Patriot Act Subject to Sunset (continued)

TABLE 4-2 Key provisions of the USA Patriot Act subject to sunset (continued)

Section	Issue addressed	Summary
209	Seizure of voice-mail messages pursuant to warrants	Enables the government to obtain voice-mail messages under Title III using just a search warrant rather than a wiretap order, which is more difficult to obtain. Messages stored on an answering machine tape, however, remain outside the scope of this section.
212	Emergency disclosure of electronic surveillance	Permits providers of communication services (such as telephone companies and Internet service providers) to disclose consumer records to the FBI if they believe immediate danger of serious physical injury is involved. Communication providers cannot be sued for such disclosure.
214	FISA pen register/trap-and-trace authority	Allows the government to obtain a pen register/trap-and-trace device "for any investigation to gather foreign intelligence information." It prohibits the use of FISA pen register/trap-and-trace surveillance against a U.S. citizen when the investigation is conducted "solely on the basis of activities protected by the First Amendment."
215	FISA access to tangible items	Permits the FBI to compel production of any record or item without showing probable cause. People served with a search warrant issued under FISA rules may not disclose, under penalty of law, the existence of the warrant or the fact that records were provided to the government. It prohibits investigation of a U.S. citizen when it is conducted solely on the basis of activities protected by the First Amendment.
217	Interception of computer trespasser communications	Creates a new exception to Title III that permits the government to intercept the "communications of a computer trespasser" if the owner or operator of a "protected computer" authorizes it. It defines a protected computer as any computer "used in interstate or foreign commerce or communication" (because of the Internet, this effectively includes almost every computer).
220	Nationwide service of search warrants for electronic evidence	Expands the geographic scope where the FBI can obtain search warrants or court orders for electronic communications and customer records
223	Civil liability and discipline for privacy violations	Provides that people can sue the government for unauthorized disclosure of information obtained through surveillance
225	Provider immunity for FISA wiretap assistance	Provides immunity from lawsuits for people who disclose information to the government pursuant to a FISA wiretap order, physical search order, or an emergency wiretap or search

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

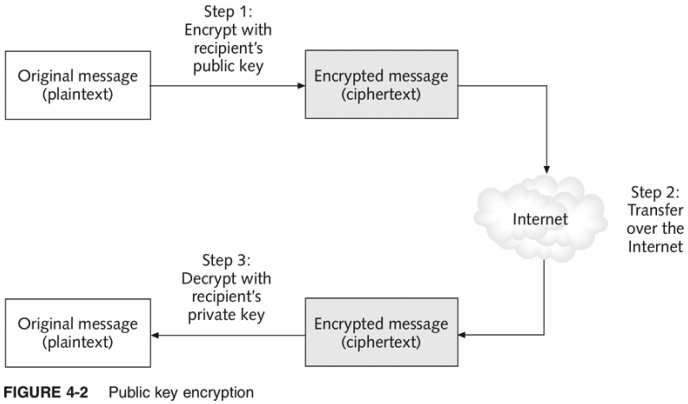


FIGURE 4-2 Public key encryption

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

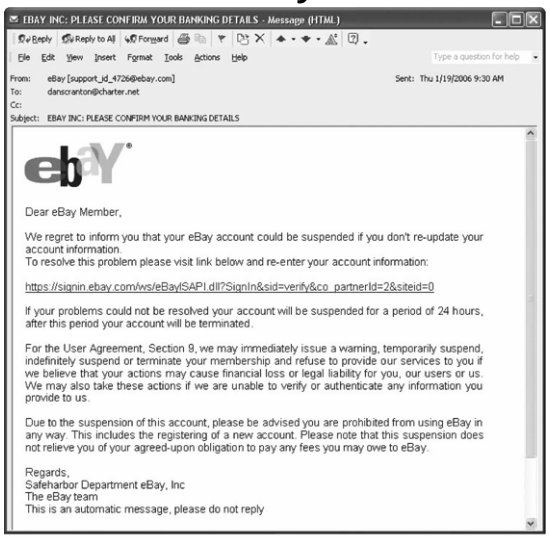
Identity Theft (continued)

- 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


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

Reply | Reply to All | Forward

File Edit View Insert Format Tools Actions 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

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

Consumer Profiling (continued)

- 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

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
- 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)