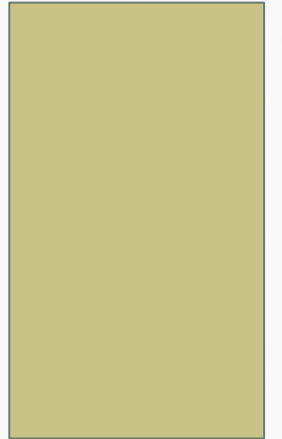
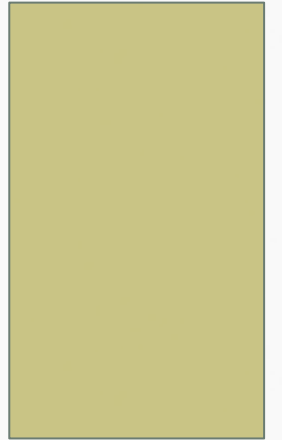


WEEK 4



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”

# THE RIGHT OF PRIVACY

- 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
  - 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)

# 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

# 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

# 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 State

# 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

# DATA ENCRYPTION

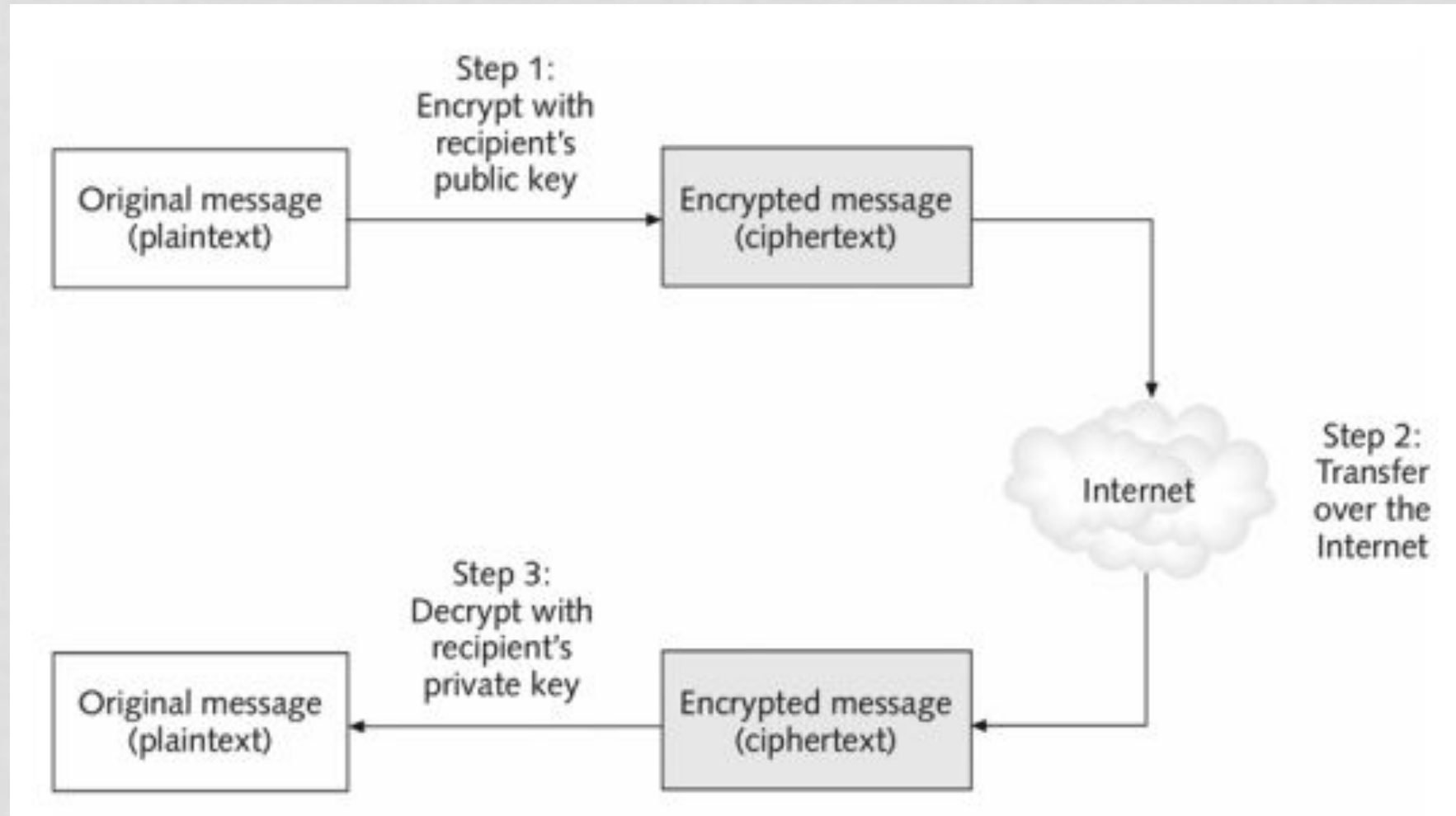
- Cryptography
  - Science of encoding messages
  - Only sender and intended receiver can understand the messages
  - Key tool for ensuring confidentiality, integrity, authenticity of electronic messages and online business transactions
- Encryption
  - Process of converting electronic messages into 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



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 stole

## IDENTITY THEFT (CONTINUED)

- 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

# 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
- Chief privacy officer (CPO)
  - Executive to oversee data privacy policies and initiatives

# 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 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)

- 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

## ESSAY ASSIGNMENT (DUE SUNDAY, 30TH JUNE)

- 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, 30TH JUNE)

- (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



**THANK YOU!**