PRIVACY

Privacy in Cyberspace

- **Privacy**
  - Individual's ability to restrict or eliminate the collection, use, and sale of confidential personal information

  - Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others''

- **Anonymity**
  - Means to communicate without disclosing one's identity
  - More difficult with the use of computers and the Internet

Different views of privacy

- Privacy as limited access to self
  - the extent to which we are known to others and the extent to which others have physical access to us

- Privacy as control over information
  - not simply *limiting* what others know about you, but *controlling* it
  - this assumes individual autonomy, that you can control information in a meaningful way (not blind click through, for example)

Privacy surveys find concerns (USA)

- Increasingly people say they are concerned about online privacy (80-90%)

- Improved privacy protection is factor most likely to persuade non-Net users to go online

- 27% of US Net users have abandoned online shopping carts due to privacy concerns

- 64% of US Net users decided not to use a web site or make an online purchase due to privacy concerns

- 34% of US Net users who do not buy online would buy online if they didn't have privacy concerns

Privacy and Computer Technology

Key Aspects of Privacy:

- Freedom from intrusion (being left alone)

- Control of information about oneself

- Freedom from surveillance (being tracked, followed, watched)
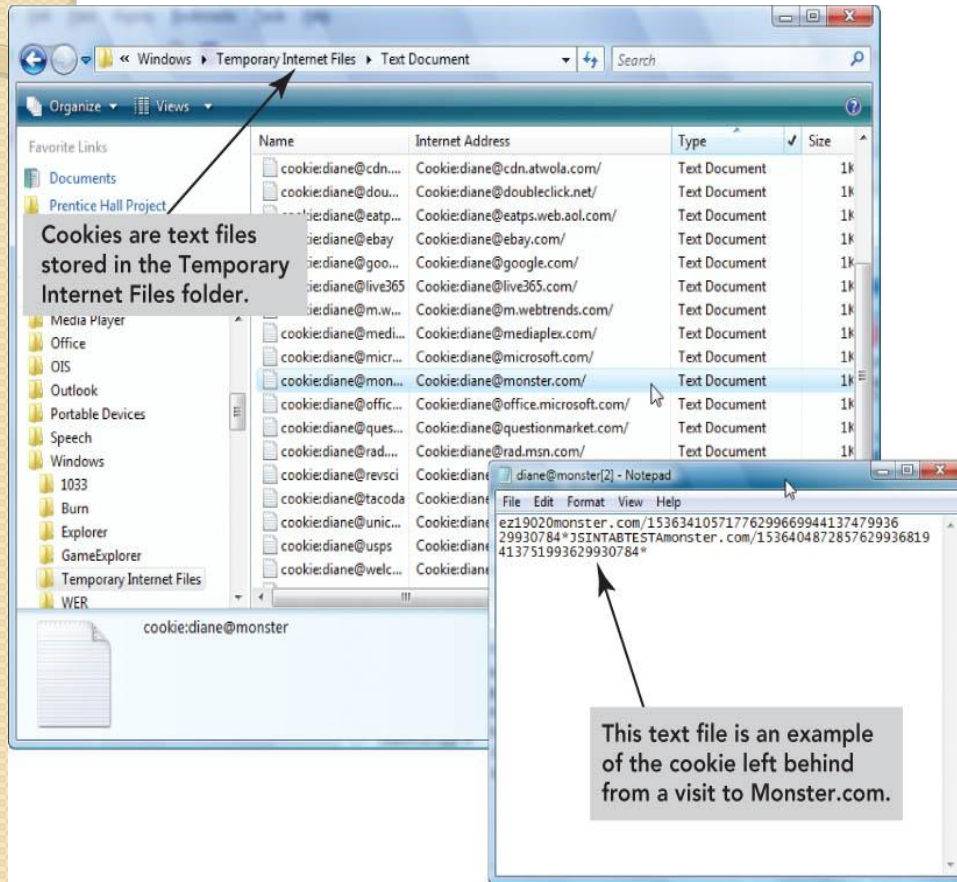
Privacy and Technology

New Technology, New Risks:

- Government and private databases

- Sophisticated tools for surveillance and data analysis

- Vulnerability of data

Some Terminologies

- Invisible information gathering - collection of personal information about someone without the person's knowledge

- Secondary use - use of personal information for a purpose other than the one it was provided for

- Computer matching - combining and comparing information from different databases (using social security number, for example, to match records)

- Computer profiling - analyzing data in computer files to determine characteristics of people most likely to engage in certain behavior

The Problem: Collection of Information Without Consent

Cookies are text files stored in the Temporary Internet Files folder.

cookie:diane@monster

diane@monster[2] - Notepad

ez19020monster.com/15363410571776299669944137479936
29930784*JSINTABTESTAmonster.com/15364048728576299368194
13751993629930784*

This text file is an example of the cookie left behind from a visit to Monster.com.

- **Technologies that jeopardize anonymity**
  - Cookies
  - Radio frequency identification

The Problem: Collection of Information Without Consent

- **Cookies**
  - Small files written to your hard disk by Web sites visited
  - Examples include:
    - Track your browsing habits
    - Gather personal information without your consent

The Problem: Collection of Information Without Consent

- **Radio frequency identification (RFID)**
  - Uses radio waves to track a chip
  - Used for inventory control in stores
  - Recognizes microchips in pets
  - May compromise anonymity and privacy if information stored on RFID tags attached to U.S. passports

In Ghana

- **Ghana**
  - ◦ 24 august 2010

  - ◦ Government initiated stakeholder consultation for the passage of Data Protection Bill (DPB) and Electronic Communications Regulations Bill (ECRB) to serve as legal instruments for the safeguarding of personal data and privacy.

  - ◦ The Bill provides for the protection of privacy through the regulation of information processing relating to individuals including the method by which data is obtained, held, used or disclosed.

Big Brother is watching

- Government Accountability Office (GAO) - monitors government's privacy policies

- Computer matching to fight terrorism

Video Surveillance:

- Security cameras
  - Increased security
  - Decreased privacy

Discussion Questions

- What data does the government have about you?

-

- Who has access to the data?

- How is your data protected?

Diverse Privacy Topics

Stolen and Lost Data:

- Hackers
- Physical theft (laptops, thumb-drives, etc.)
- Requesting information under false pretenses
- Bribery of employees who have access

Diverse Privacy Topics

What We Do Ourselves:

- Personal information in online profiles
- Pictures of ourselves and our families
- File sharing and storing
- Is privacy old-fashioned?
  - Young people put less value on privacy than previous generations
  - May not understand the risks

Diverse Privacy Topics

Public Records: Access vs. Privacy:

- Public Records - records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.)

- Identity theft can arise when public records are accessed

- How should we control access to sensitive public records?

Discussion

- Is there information that you have posted to the Web that you later removed?

- Why did you remove it?

- Were there consequences to posting the information?

- Have you seen information that others have posted about themselves that you would not reveal about yourself?

Protecting Privacy

Technology and Markets:

- Privacy enhancing-technologies for consumers

- Encryption
  - Public-key cryptography

- Business tools and policies for protecting data

Protecting Privacy

- **Protecting privacy online/home**
  - Tell children not give out personal information.

  - Complete forms only if you see a privacy statement.

  - Create logins and passwords for each person using the computer.

  - Do not save account numbers or passwords.

  - Close a secured account site when not using a computer.

Protecting Privacy

◦ Use **strong passwords**

- Do use: difficult to guess passwords; at least 14 characters or more long; uppercase letters, lowercase letters, numbers, and special characters

- Don't use: a recognizable word or phrase; name of anything or anyone close to you, including names of family members or pets; recognizable strings of numbers, such as social security numbers or birth dates

Protecting Privacy

- Do not leave cell phones in public places.

- Turn off services not in use, especially Bluetooth.

- Verify that devices have secure configurations.

Protecting Privacy

- **Employee monitoring**
  - ◦ Majority of large U.S. employers observe employee phone calls, e-mails, Web browsing habits, and computer files

- **Protecting privacy at work**
  - ◦ Refrain from making personal calls on a work phone
  - ◦ Avoid using company e-mail for personal purposes
  - ◦ Assume you are monitored