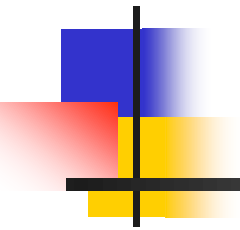
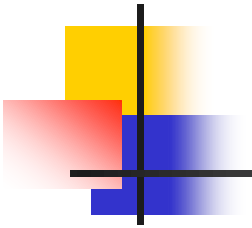


Privacy

Professor Stephen S. Yau

Spring 2014



Privacy

- Ability of individuals or group to prevent their ***personal information*** from being known to people other than those the owners give the information to.
- One of hottest topics in information assurance due to increasing capabilities of IT technology:
  - Collect information on individuals
  - Combine facts from separate sources, and merge them with other information; resulting in various databases of private information

Basic Privacy Principles

- ***Lawfulness*** and ***fairness***
- ***Necessity*** of data collection and processing
- ***Specification*** and ***binding***
  - No "non-sensitive" data
- ***Transparency***
  - Data subject´s right to information correction, erasure or blocking of incorrect/illegally stored data
- Supervision by ***independent*** data protection authority and sanctions
- Adequate organizational and technical ***safeguards***

Computer Forensics vs. Privacy Protection

- Computer forensics focuses on ***finding hidden information***
- Privacy protection concerns with ***individual's right to hide certain personal information***
- What kind of information can be collected under what kind of situations is usually limited and controlled by Constitution or legislation
  - In US, the most important high-level document that defines this limitation is the ***Fourth Amendment to the Constitution***.
  - After 9/11, ***PATRIOT Act*** changed this in favor of the government, giving federal authorities much wider latitude in monitoring Internet usage and expands the way such that data is shared among different agencies.

What Can Be Collected and When? (Cont.)

- The Fourth Amendment ***generally prohibits opening, accessing, or viewing information from closed containers without a warrant.*** If investigators identify the suspect has a right to privacy, they should consider to secure a warrant.
- In US, individuals may ***lose their right to privacy*** when ***transferring data to a third party***, and that their right to privacy does ***not extend to searches conducted by private parties who are not acting on behalf of government***.
  - If someone took his personal computer to a repair shop, and the technician there noticed child pornography on the system, the repair shop is compelled to notify the authorities

What Can Be Collected and When?

- Two types of searches
  - ***Warranted:*** Investigator obtained explicit authorization (warrant) from proper authorities.
  - ***Warrantless:*** Investigator has implicit authorization (warrantless) from probable cause or otherwise to conduct the search

What Can Be Collected and When? (Cont.)

- Warrantless searches happen only when
  - The suspect has ***lost his/her right to privacy***
  - ***Consent is given by the owner***:
    - An employer normally has full authority to search corporate data systems because employee signed certain agreement before using those systems.
    - Scope of the consent and who gave the consent can both be complex legal issues.

Privacy Protection

- Privacy and data protection laws promoted by ***government***
- ***Self-regulation*** for fair information practices by codes of conducts promoted by ***businesses***
- Privacy-enhancing technologies (PETs) adopted by ***individuals***
- Privacy education of ***consumers and IT professionals***

Threats to Privacy

- ***Application level***
  - Threats to collection/transmission of large quantities of personal data
  - Applications, such as research involving population studies, electronic commerce, distance learning
- ***Communication level***
  - Threats to anonymity of sender / forwarder / receiver
  - Threats to anonymity of service provider
  - Threats to privacy of communication, such as via monitoring / logging of transactional data: Extraction of user profiles & its long-term storage
- ***System level***
  - For example, threats due to attacks on system in order to gain access to its data
- ***Audit trails***

Threats to Privacy (cont.)

- ***Identity theft*** – the most serious crime against privacy
- ***Aggregation*** and ***data mining***
- ***Poor system security***
- ***Government*** threats
  - Taxes, homeland security, etc.
  - People's privacy vs. homeland security concerns
- ***Interne***t as privacy threat
  - Unencrypted e-mail/web surfing/attacks
- ***Corporate rights*** and ***private business***
  - Companies may collect certain data
- ***Privacy for sale*** - many traps
  - "Free" is not free, such as frequent-buyer cards reducing your privacy

Privacy Practices in E-Commerce

- The Federal Trade Commission (FTC) specifies five privacy practices that all companies engaged in e-commerce should observe
  1. ***Notice/Awareness***
     - In general, websites should clearly inform users how it collects and handles user information

Privacy Practices in E-Commerce (cont.)

- ***Essential notifications***
  - Identification of the ***entity*** collecting the data
  - Identification of the ***uses*** to which the data will be put
  - Identification of any ***potential recipients*** of the data
  - The ***nature*** of the data collected and the ***means*** by which it is collected
  - Whether the provision of the requested data is ***voluntary or required***, and the ***consequences*** of a refusal to provide the requested information
  - The ***steps*** taken by the data collector to ensure the ***confidentiality, integrity and quality of the data***

Privacy Practices in E-Commerce (cont.)

2. ***Choice/Consent***

- Websites must give consumers ***options*** as to how any personal information collected from them may be used
- Two traditional types of choice/consent
  - ***Opt-in*** requires affirmative steps by the consumers to ***allow*** the collection and/or use of information
  - ***Opt-out*** requires affirmative steps to ***disallow*** the collection and/or use of such information.

Privacy Practices in E-Commerce (cont.)

3. ***Access/Participation***

- User would be able to ***review, corr***ect, and in some cases ***delete*** personal information on a particular website.
- ***Access*** must encompass
  - ***timely*** and ***inexpensive access*** to data
  - simple means for contesting ***inaccurate or incomplete data***
  - mechanism by which the data collector can ***verify*** the information
  - means by which ***corrections and/or consumer objections*** can be added to the data file and sent to all data recipients.

Privacy Practices in E-Commerce (cont.)

4. ***Security/integrity***

- Websites must use both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.

Privacy Practices in E-Commerce (cont.)

5. ***Enforcement/Redress***

- ***Mechanisms to enforce*** all above privacy principles.
- ***Self-Regulation***: Mechanisms to ensure ***compliance*** (enforcement) and appropriate means of ***recourse*** by injured parties (redress).
- ***Private Remedies***: A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices .
- ***Government Enforcement***: Civil or criminal penalties enforced by governments.

A Case Study

- A corporation collects customers' transactions from over 1,500 stores in 10 countries, and allows more than 3,000 suppliers to access and analyze data on their products to identify customer buying patterns, manage local store inventory and identify new merchandising opportunities.
- What concerns on privacy of the collected information?

Possible Privacy Approaches

- ***Randomization:*** Add noise to the data without changing data's aggregate distribution
- ***Distributed privacy preservation:*** Analyze data across various entities without collecting data from entities
- ***Downgrading application effectiveness:*** Modify the data to downgrade the accuracy of the results by data mining, and remove sensitive information from the results

Acts Related to Privacy Protection

- Privacy Act of 1974 ***http://www.justice.gov/opcl/privstat.htm***
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 ***http://www.dol.gov/dol/topic/health-plans/portability.htm***
- E-Government Act of 2002 ***http://www.archives.gov/about/laws/egov-act-section-207.html***
- Online Privacy Protection Act of 2003 ***http://en.wikipedia.org/wiki/Online_Privacy_Protection_Act***
- Children's Online Privacy Protection Act of 1998 (COPPA) ***http://www.ftc.gov/ogc/coppa1.htm***
- Fair Information Practice Principles (FIPs) specified by the Federal Trade Commission (FTC) ***http://www.ftc.gov/reports/privacy3/fairinfo.shtm***

References

- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security*, Course Technology, 2011
- Mark Stamp, *Information Security: Principles and Practice*, Wiley, 2011
- M. Merkow, J. Breithaupt, *Information Security: Principles and Practices*, Prentice Hall, August 2005, 448 pages, ISBN 0131547291
- Charu C. Aggarwal, Philip S. Yu, "Privacy-Preserving Data Mining: A Survey", *Handbook of Database Security*, 2008, pp. 431-460.