Privacy

Chris Reedy
from material by Bill Hurd
CS 225 Summer 2006
Privacy

- What do we mean when we say “Respect my privacy”
Types of privacy

- Leave me alone – intrusion
- You don’t need to know that – knowledge about ones personal information
- Stop watching me – freedom from surveillance
Is privacy “a good”

- Is more privacy always better?
- Does the US constitution say specifically we have a “right to privacy”
Do we have a natural right to privacy?

- US Declaration of Independence: right to life, liberty and the pursuit of happiness
- US Bill of Rights
- Evolved from property rights?
  - Contents of your house
- Brandeis – “right to be let alone”
- Stanley Benn – derived from the fact that each person is worthy of respect
  - Allows me to fully become a person
  - Allows intimacy
Balance privacy

- Safeguard us from unjustified intrusions by authorities
- Collect information to make rational decisions in social, governmental and commercial life
- Conduct limited surveillance to protect public order and safety
What is personal information?
Why are we at more risk now?

- What ways can people collect data about you?
- How is it done?
- Where is it stored?
Why are we at more risk now

- Databases – demographic information
- Recording of transactions both web and conventionally
- Email and document forwarding
- Browser cookies
- Spyware
- Radio Frequency Id tags (RFIDs)
- Public information collection and data mining (ChoicePoint)

- Technology makes collection, searching, analysis, storage and distribution easy and cheap
Information gathering is easy

- Caller id
- Shoppers cards like Haggen
- ISP usage tracking
- Web site cookies
- Satellite
- Surveillance cameras
- Are you informed about all these collections?
Secondary use

- Use of information for purposes other than the reason it was supplied
- Usenet Newsgroups
- Could an insurance company find out you were on a particular health newsgroup and use that information to deny you insurance?
Secondary Use

- Data mining
- Purchasing patterns, gasoline
- Records of car purchases
- Match credit card numbers to people
- Estimate car mileage, vehicle replacement

Sell that information to a company selling car loans
Cell phones and 911

- Originally no 911 support
- By federal law cell phones now support 911 with location tracking
  - Within 100 yards always
  - Precisely using GPS
- Similar technology in long haul trucks and rental cars
- What are you gaining/losing by carrying a cell phone?
The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
Thermal imaging

- Class discussion
Company email

- Class discussion
Checking myspace.com

- See the following Slashdot article:
  http://slashdot.org/article.pl?sid=06/06/11/0548259

- Class discussion
You run a small, private software company and you sell your product on the internet
What sort of information do you need to gather to complete a sale of your product?
How much should you collect?

How much does your marketing department want to collect?
Code of Fair Information Practices

1. There must be no personal-data record-keeping system whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Guidelines

- Collect only what is needed
- Inform people what is collected and how it is to be used
- Offer ways to opt out of data transfer
- Protect personal information
  - Keep a log of who accesses and modifies data
- Keep only as long as needed
- Maintain accuracy
- Provide a way to correct inaccurate data