CSE/ISE 312

Privacy

(Part 1)

What We Will Cover

- Privacy risks and principles
- 4th Amendment, expectations, and surveillance
- Business and social sectors
- Government systems
- Protecting Privacy
- Communications

Privacy Risks and Principles

Three Key Aspects of Privacy:

- Freedom from intrusion - being left alone
- Control of information about oneself
- Freedom from surveillance (from being tracked, followed, watched, eavesdropped on)

Privacy Threats

- Intentional, institutional use
- Insider access
- Theft of information
- Inadvertent leakage
- Personal actions

Definitions

- Personal information – any information relating to, or traceable to, an individual person
- Informed consent – users being aware of what information is collected and how it is stored
- Invisible information gathering - collection of personal information about someone without the person's knowledge
- Cookies - files that a website stores on a visitor's computer

New Technology, New Risks

- Government and private databases
- Sophisticated tools for surveillance and data analysis
- Vulnerability of data
- Rapid decline in the cost of data storage allows for massive databases
- Electronic data storage leads to a proliferation of privacy threats

More Examples

Search query data

- Search engines collect many terabytes of data daily
- Data is analyzed to target ads and develop new services
- Who gets to see this data? Why should we care?

Smartphones

- Location apps
- Data sometimes stored and sent without users' knowledge

Summary of Privacy Issues (1)

- Almost everything we do online is recorded
- Huge amounts of data are stored
- People are often not aware of collection of personal data
- Software is complex, not even sure which collects data
- Leaks happen
- A collection of many small data items can provide a detailed picture of person's life

Summary of Privacy Issues (2)

- **Re-identification** – piecing together someone's identity - has become much easier than before
- Information available on the Internet will be found by people for whom it was not intended
- Electronic data seems to last forever
- Data collected for one purpose will find other uses
- The government sometimes requests personal data
- We cannot directly protect information about ourselves

Terminology

- Secondary use - use of personal information for a purpose other than the one it was provided for
- Data mining - searching and analyzing masses of data to find patterns and develop new information or knowledge
- 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 a certain behavior

Stolen and Lost Data

- Examples:
  - Spyware: software often downloaded from a web site without user knowledge, collecting user data and activity and sends to remote parties
  - Business and government lose customer/citizen information due to weak security
  - Pretexting: pretend to be someone who is legitimate to obtain data.
- One should be aware and consciously make decisions; IT professionals should endeavor to develop security systems

Principles for Data Collection and Use

- Informed consent – informing people how collected information is being used
- Opt-in and opt-out policies – people specify an exception to the default condition (either to not use information or use information by default)
- Data retention

Forms of Informed Consent

Two common forms for providing informed consent are opt in and opt out:

- opt in – The collector of the information may use information only if person explicitly permits use (usually by checking a box)
- opt out – Person must request (usually by checking a box) that an organization *not* use information
- Under an opt in policy, more people are likely to be "out"
- Under an opt out policy, more people are likely to be "in"

Fair Information Principles (FIP)

- Recommendations from privacy experts
  1. Inform people when you collection information, what you collect and how you use it
  2. Collect only the data needed
  3. Offer opt-outs
  4. Keep data only as long as needed
  5. Maintain accuracy of data
  6. Protect security of data
  7. Develop policies for law enforcement requests

The Fourth Amendment

- Part of the US Bill of Rights
- ***"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."***

Key Problems Arise from New Tech.

- The US Constitution sets limits on government's rights to search our homes, businesses, and seize docs and other personal effects. Requires government to provide probable cause.
- Much of our information today is no longer located in our homes; it resides in huge databases outside our control
- New technologies allow the government to search our homes without entering them and search our persons from a distance without our knowledge

New Technologies

- Non-invasive but deeply revealing searches
  - Particle sniffers
  - Imaging systems
  - Location trackers
- Modern surveillance techniques are redefining expectation of privacy
- What restrictions should we place on their use? When should we permit government agencies to use them without a search warrant?

Supreme Court Decisions and Expectation of Privacy (1)

- Supreme court decisions continue to address impact of new tech on 4th Amendment protection
- *Olmstead v. United States* (1928)
  - Supreme Court allowed the use of wiretaps on telephone lines without a court order
  - Interpreted the Fourth Amendment to apply only to physical intrusion and only to the search or seizure of material things, not conversations.

Supreme Court Decisions and Expectation of Privacy (2)

- *Katz v United States* (1967)
  - Supreme Court reversed its position and ruled that the Fourth Amendment *does* apply to conversations
  - Court said that the Fourth Amendment protects people, not places. To intrude in a place where reasonable person has a reasonable expectation of privacy requires a court order

Supreme Court Decisions and Expectation of Privacy (3)

- *Kylo v United States* (2001)
  - Supreme Court ruled that police could not use thermal-imaging devices to search a home from the outside without a search warrant.
  - Court stated that where "government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'"

Search and Seizure of Computers and Phones

- The 4th Amendment requires that search warrants be specific about object to search
- If an officer with a warrant sees evidence of another crime in plain view, the office may seize it
- How should we interpret “plain view” for search of computer or smartphone files?
- Access by law enforcement agents to all data on a computer device can be a serious threat to privacy, liberty, and free speech

Video Surveillance and Face Recognition

Security cameras

- Low accuracy rate may result in detention of many innocent people
- Abuse by the operators
- Is the level of surveillance compatible with privacy and a free society?
- What trade-offs between privacy and security are we willing to make?