Privacy

- What is privacy?
- Is it a distinct right from other rights?
- How do we give trust and give privacy?
- Conflict: The right to privacy and the right to freedom of expression.
- What laws do we have to protect privacy?
- Is big brother watching us?
  - Electronic Trails
  - Covert electronic surveillance
  - USA PATRIOT act
- When is data mining going too far?
Privacy: what is it?

- It is a notion of access.
  - Physical proximity to a person.
  - Information about a person.
- How do we decide what should be private and what should be public?
  - Where do we draw the line?
  - Can too much privacy be harmful?
- Privacy: a social agreement.
  - Individuals have control over who gains physical or personal information access.
Harms and benefits of privacy

**Harm:**
- Plan illegal or immoral activities.
- Can put strain on an individual.
  - Too much privacy doesn’t allow a person to share personal burdens.
- Can hide dysfunctional families.
  - Families get a natural right to privacy.
  - Family problems are not shared with the community.

**Benefits:**
- Allows for individual maturity.
  - Social cues of individual responsibility.
  - Allow for individual development.
  - A recognition of true freedom.
- Allows the removal of our public persona: a means to remove stress.
- Allows for development of intellectual activities: shut others out of our thoughts.
- Controlling access allows for a development of diverse relationships.
Natural right

- Evolves out of property rights.
  - Your physical home is deemed private, access can only be granted by owner.
  - THIRD AMENDMENT of the USA CONSTITUTION: No soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.
- Privacy rights violations is often a violation of a right of some other cluster.
  - So there is no need to define privacy precisely.
  - Initial law recognizes privacy as “the right to be let alone” from the French law.
- A natural right is difficult to define.
- Privacy is a *prudent right* as it benefits society more than it harms.
Privacy and trust

We have more privacy today than we had in the past vs the agrarian society of the past.

Rise of the modern:
- Home separate us from our community.
- Motor cars allow us to travel alone (no bus/public transport).
- Televisions keep us out of public movie theaters.
- Computers: access information at home rather than a public library.

We live among strangers.

How do we trust:
- Get bank loans.
- Trust a taxi driver to get us home.
- Trust our teachers to care for our children.

We have to rely on a person reputation.
- Collecting information about a person.
- Drivers license.
- Credit cards.
Disclosing Information

- **Public information**
  - Self reported information.
  - Telephone directory listings.
  - Disclosure of address.
  - Disclosure of names.

- **Personal Information**
  - Information not public information or part of the public record.
  - Becomes part of public information through voluntary, involuntary, or statutory disclosure.
Rewards or loyalty programs

Body Scanners: custom made clothes, clothing recommendations.

Digital Video Recorders: usage is recorded and sold to other companies.

Automobile “black boxes”.

Enhanced 911 Services: tracking locations of cell phone users to within 100 meters.

RFID: better than bar-codes, doesn’t turn off though.

Cookies: websites can use it to track user activity.

Spyware: monitors web surfing, log keystrokes, take snapshots of your computer screen.
U.S. Legislation

- Regulate the collection and distribution of information.
- Fair Credit Reporting act: laws promoting accuracy and privacy of information.
- Fair and accurate credit transaction act: provide consumers with a free copy of credit report every 12 months.
- Family education rights and privacy act: the rights to correct information and release of education information.
- Video privacy act: can’t disclose rental records without written consent, destroy records after a year.
- Many more ....
USA PATRIOT act

Four principle categories (affecting privacy):

- Greater authority to monitor communications.
- Greater power to regulate banks, prevent laundering foreign money.
- Make it more difficult for terrorists to enter the US.
- Defines new crimes and penalties for terrorist activities.

Don’t have to show probable cause for trap-and-trace devices.

- Allow court order to extend to other counties/states.
- Can search a person’s premises without first serving a search warrant.

Success:

- Allow better information sharing and gathering by law enforcement officers.
- Increased removal of other terrorist and breaking up of terror cells.
Data Mining

- Database searching for patterns or relationships.
- Collaborative filtering: identify relationships between items.
  - Make recommendations.
  - Companies regular sell this information.
- IRS Audits:
  - Compare tax forms to reported data from employers - detect incomplete tax forms
  - Use the system to figure out who to audit.
- Who owns the information?
  - Does seller or person purchasing an item control that information?
- Rules governing secondary use of information.
  - Opt-in Verses Opt-out
    - Opt-in: Consumer gives explicit permission - preferred by privacy advocates.
    - Opt-out: Consumer explicitly forbid the use - direct marketing associations prefer this.
A means to protecting your privacy: obscuring its content.

Symmetric Encryption:
- A single key is needed to encrypt and decrypt.
  - How do we safely exchange the key?

Asymmetric encryption: public-key encryption.
- Each individual has a public and private key.
- The public key is shared to be used for encryption.
- Only the private key can decrypt the message.
- Exchange public keys to share data safely.
Public-key encryption

- Mathematical relationships between the public and private key.
  - Private key can be derived from public key.
- Strength of encryption is based on length of key.
  - Stronger (longer) keys take longer to break.
  - Stronger (longer) keys take longer to create as well.
- Time sensitivity of the information decides key strength.
- US initially banned export of strong encryption technology.
  - Initially to prevent international criminals getting strong encryption.
  - NSA didn’t want US strong encryption technology in the hands of international countries.
  - US companies suffered as they couldn’t export programs: lost out to international companies who could create strong encryption.
  - Law was repelled in 2000: violation of the right to protect privacy.
Digital Cash

- Anonymous electronic money system.
- Cash stored on smart cards.
- Banks rely on public key encryption.
- Keys can still be broken.
- Banks sign money with their private key.
- Use the banks public key to verify the information.
- Customers encrypt their money with the their private keys.
- Banks verify information with your public key.