

CSE312/ISE312

Gift of Fire, Fourth edition by Sara Baase

Read: Section 2.1-2.2

Slides prepared by Cyndi Chie and Sarah Frye. Fourth edition revisions by Sharon Gray.



What We Will Cover Today

- Privacy Risks and Principles
- The Fourth Amendment, Expectation of Privacy, and Surveillance Technologies

Corresponding page number: 47

Definitions

- Personal information – any information relating to, or traceable to, and individual person
- Directory information – name, address, telephone number, date and place of birth, honors and awards, and dates of attendance
- 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

Corresponding page number:

Key Aspects of Privacy

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

Identify how technology has affected these aspects of privacy.

Using examples, can you give a negative and positive aspects of lessening of privacy in each category?

Corresponding page number: 48

Privacy Threats

- Intentional, institutional uses of personal information
 - Government
 - Private industry
- Unauthorized use or release by “insiders”
- Theft of information
- Inadvertent leakage (carelessness)
- Our own actions

Give some concrete examples of each of these threats

Corresponding page number: 49

New Technology, New Risks

- Government and private databases
 - Voting preferences
 - Purchase preferences
- Sophisticated tools for surveillance and data analysis
 - Shopping analysis
 - Purchase analysis
 - Web browsing
- Vulnerability of data
 - Protection of data
 - Acquisition of companies

What new technologies make these risks possible?

Corresponding page number: 50-51

Example: Search Query Data

- Search engines collect many terabytes of data daily
- Data is analyzed to target advertising and develop new services
- Examples
 - Subpoena to Google
 - AOL data leak
 - Student e-mail accounts

Do you think that further restrictions should be placed on Google's use of search data?


Corresponding page number: 51-52

FERPA

- Family Education Rights and Privacy Act (1974)
 - en.wikipedia.org/wiki/FERPA
 - www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- Rights of parents, which transfer to children upon entering college or reaching 18 years old
 - Right to inspect and review educational records
 - Right to request schools amend incorrect records
 - Grant permission to release records (with exceptions)
- Schools may disclose directory information

How do you look up posted grade information?

Do your parents have the right to request your grades?




Example: Smart Phones

- Location based services supposedly send location data to enhance functions in app
- Phone ID and/or location send in many apps
- Various apps copy user's contact info to remote servers
- Data sometimes stored and sent without user's knowledge

Are you aware of the loss of data?
Do you feel you have control over
the distribution of data from your
smart phone?


Corresponding page number: 53-54



Summary of Risks ...

- Anything we do in cyberspace is recorded
- Huge amounts of data are stored
- People are not aware of collection of data
- Businesses and individuals are often not aware of what their software observes
- Large amounts of seemingly innocuous data can provide a detailed profile of an individual
- Re-identification is feasible

Corresponding page number: 55



... Summary of Risks

- If information is on a public Web site, it is available to everyone (e.g., public access data)
- Information on the Internet seems to last forever.
- Data collected for one purpose will find other uses
- Government can request sensitive personal data held by businesses or organizations
- We depend upon businesses and organizations to protect information about ourselves

Corresponding page number: 55-56



Terminology

- *Personal information* – any information relating to an individual person.
- *Informed consent* – users being aware of what information is collected and how it is used (first principle of ethical treatment of personal info)
- *Invisible information gathering* - collection of personal information about a user without the user's knowledge.

Do you have informed consent in most transactions concerning your personal data?

Corresponding page number: 56-58

Other Examples

- Free browser cursor that tracked usage
- Automobile event data recorder
- Spyware
- Third party ad servers
- User recognition techniques
 - Device fingerprinting
 - Cookie planting (e.g., on-line contests)

Cookies are files a Web site stores on a visitor's computer


Corresponding page number: 56-58

Terminology

Big Data

- *Secondary use* – Use of personal information for a purpose other than the purpose for which it was provided
- *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
- *Computer profiling* – Analyzing data to determine characteristics of people most likely to engage in a certain behavior

Corresponding page number: 58




Informed Consent

Two common forms for providing informed consent are:

- *opt out* – Person must request (usually by checking a box) that an organization *not* use information
- *opt in* – The collector of the information may use information only if person explicitly permits use (usually by checking a box)

Corresponding page number: 59



Privacy Risks and Principles

Discussion Questions

- *Have you seen opt-in and opt-out choices? Where? How were they worded?*
- *Were any of them deceptive?*
- *Has anyone actually read a privacy policy?*

Corresponding page number: 59

Privacy Risks and Principles

Fair information principles

1. Inform people when you collect information
2. Collect only the data needed
3. Offer a way for people to opt out
4. Keep data only as long as needed
5. Maintain accuracy of data
6. Protect security of data
7. Develop policies for responding to law enforcement requests for data

Why would companies not do some of these?

Corresponding page number: 60

The Fourth Amendment Section 2.2

The right of the people to be secure in their person, 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.

—4th Amendment, U.S. Constitution

Corresponding page number: 61



The Fourth Amendment

- Sets limits on government's rights to search our homes and businesses and seize documents and other personal effects
- Requires government provide probable cause
- Two key problems arise from new technologies:
 - Much of our personal information is no longer safe in our homes;
 - New technologies allow the government to
 - search our homes without entering them and
 - search our persons from a distance without our knowledge.

What are some examples of new technology the search and seize?

Corresponding page number: 61-62



Class Question

- What restrictions should we place on their use?
- When should we permit government agencies to use them without a search warrant?


Corresponding page number: 63



Supreme Court Decisions

- *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.

Corresponding page number: 63



Supreme Court Decisions

- *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

Corresponding page number: 64

Supreme Court Decisions

- *Kyllo 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.’”

If drones become in general public use, should their use not be an invasion of privacy?

Corresponding page number: 64

Class Question

- Police need a search warrant to attach a tracking device to a car
- Would cell phone tracking or video surveillance tracking also need a search warrant?

Is there an expectation of privacy in our travels (on foot or in a car)?

Corresponding page number: 65

Search and Seizure of Computers and Phones

- Courts take a view that if an officer has a warrant to investigate a crime and sees evidence in “plain view” of another crime, that evidence may be seized and used to prosecute
- Police may search an arrested person and examine personal property within his or her reach

How should we interpret “plain view” or “reach” for search of computer or smartphone files?

Corresponding page number: 66-68

Video Surveillance and Face Recognition

What are the limits?

- *Location only?*
- *Tracking targets?*
- *Tracking everyone?*
- *Should organizers at events which are possible terrorist targets use such systems?*
- *Should we allow them to screen for people with unpaid parking tickets?*

Corresponding page number: 70