



A Gift of Fire

Fourth edition

Sara Baase

Chapter 2: Privacy

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



What We Will Cover

- Privacy Risks and Principles
- The Fourth Amendment, Expectation of Privacy, and Surveillance Technologies
- The Business and Social Sectors
- Government Systems
- Protecting Privacy: Technology, Markets, Rights, and Laws
- Communications



Privacy Risks and Principles

Key Aspects of Privacy:

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



Privacy Risks and Principles

Privacy threats come in several categories:

- Intentional, institutional uses of personal information
- Unauthorized use or release by “insiders”
- Theft of information
- Inadvertent leakage of information
- Our own actions



Privacy Risks and Principles

New Technology, New Risks:

- Government and private databases
- Sophisticated tools for surveillance and data analysis
- Vulnerability of data



Privacy Risks and Principles

New Technology, New Risks – Examples:

Search query data

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



Privacy Risks and Principles

New Technology, New Risks – Examples:
Smartphones

- Location apps
- Data sometimes stored and sent without user's knowledge



Privacy Risks and Principles

New Technology, New Risks – Summary of Risks:

- Anything we do in cyberspace is recorded.
- Huge amounts of data are stored.
- People are not aware of collection of data.
- Software is complex.
- Leaks happen.



Privacy Risks and Principles

New Technology, New Risks – Summary of Risks (cont.):

- A collection of small items can provide a detailed picture.
- Re-identification has become much easier due to the quantity of information and power of data search and analysis tools.
- If information is on a public Web site, it is available to everyone.



Privacy Risks and Principles

New Technology, New Risks – Summary of Risks (cont.):

- 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 cannot directly protect information about ourselves. We depend upon businesses and organizations to protect it.



Privacy Risks and Principles

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.
- *Invisible information gathering* - collection of personal information about a user without the user's knowledge.



Privacy Risks and Principles

Terminology:

- *Cookies* – Files a Web site stores on a visitor's computer.
- *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.



Privacy Risks and Principles

Terminology:

- *Computer matching* – Combining and comparing information from different databases (using social security number, for example) to match records.
- *Computer profiling* – Analyzing data to determine characteristics of people most likely to engage in a certain behavior.



Privacy Risks and Principles

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

- *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).



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?*
- *What are some common elements of privacy policies you have read?*



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.



The Fourth Amendment

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



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; 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

- Make possible “noninvasive but deeply revealing” searches
 - particle sniffers, imaging systems, location trackers
- 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

- *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

- *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

- *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.’”



Search and Seizure of Computers and Phones

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



Video Surveillance and Face Recognition

- Security cameras
 - Increased security
 - Decreased privacy



Video Surveillance and Face Recognition

Discussion questions:

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



Marketing and Personalization

- Data mining
- Targeted ads



Marketing and Personalization

- Informed consent
- “Do Not Track” button in browsers



Marketing and Personalization

- Paying for consumer information



Social Networks

- What *we* do
 - Post opinions, gossip, pictures, “away from home” status
- What *they* do
 - New services with unexpected privacy settings



Our Social and Personal Activity

Discussion Questions

- *Is there information that you have posted to the Web that you later removed? Why did you remove it? Were there consequences to posting the information?*
- *Have you seen information that others have posted about themselves that you would not reveal about yourself?*



Life In the Clouds

- Security of online data
- Convenience



Location Tracking

- Global Positioning Systems (GPS) – computer or communication services that know exactly where a person is at a particular time
- Cell phones and other devices are used for location tracking
- Pros and cons



Location Tracking

- Tools for parents
 - GPS tracking via cell phones or RFID



A Right to Be Forgotten

- The right to have material removed.
 - negative right (a liberty)
 - positive right (a claim right)



Government Systems

Databases:

- Government Accountability Office (GAO) - monitors government's privacy policies
- Burden of proof and "fishing expeditions"
- Data mining and computer matching to fight terrorism



Government Systems

Public Records: Access vs. Privacy:

- Public Records – records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.)
- Identity theft can arise when public records are accessed
- How should we control access to sensitive public records?



Government Systems

Discussion Questions:

- *What data does the government have about you?*
- *Who has access to the data?*
- *How is your data protected?*



National ID Systems

- Social Security Numbers
 - Too widely used
 - Easy to falsify
- Various new proposals would require citizenship, employment, health, tax, financial, or other data, as well as biometric information. In many proposals, the cards would also access a variety of databases for additional information.



National ID Systems

- A new national ID system - Pros
 - would require the card
 - harder to forge
 - have to carry only one card
- A new national ID system - Cons
 - Threat to freedom and privacy
 - Increased potential for abuse



Protecting Privacy

Technology and Markets:

- Privacy enhancing-technologies for consumers
- Encryption
 - Public-key cryptography
- Business tools and policies for protecting data



Encryption Policy

- Government ban on export of strong encryption software in the 1990s (removed in 2000)



Rights and Law

- Warren and Brandeis: The inviolate personality
- Judith Jarvis Thomson: Is there a right to privacy?



Rights and Law

- Transactions
- Ownership of personal data
- A basic legal framework: Enforcement of agreements and contracts
- Regulation



Rights and Law:

Contrasting viewpoints

- Free Market View
 - Freedom of consumers to make voluntary agreements
 - Diversity of individual tastes and values
 - Response of the market to consumer preferences
 - Usefulness of contracts
 - Flaws of regulatory solutions



Rights and Law:

Contrasting viewpoints (cont.)

- Consumer Protection View
 - Uses of personal information
 - Costly and disruptive results of errors in databases
 - Ease with which personal information leaks out
 - Consumers need protection from their own lack of knowledge, judgment, or interest



Rights and Law:

Contrasting viewpoints

Discussion Questions

- *How would the free market view and the consumer protection view differ on errors in Credit Bureau databases?*
- *Who is the consumer in this situation?*



Privacy Regulations in the European Union

- EU's rules are more strict than U.S. regulations
- EU Data Privacy Directive
 - Prohibits transfer of personal information to countries outside the EU that do not have an adequate system of privacy protection.
 - “Safe Harbor” plan
 - Abuses still occur
 - Puts requirements on businesses outside the EU



Communications

Wiretapping and Email Protection:

- Telephone
 - 1934 Communications Act prohibited interception of messages
 - 1968 Omnibus Crime Control and Safe Streets Act allowed wiretapping and electronic surveillance by law-enforcement (with court order)
- Email and other new communications
 - Electronic Communications Privacy Act of 1986 (ECPA) extended the 1968 wiretapping laws to include electronic communications, restricts government access to email



Communications

- The Communications Assistance for Law Enforcement Act (CALEA)
 - Passed in 1994
 - Requires telecommunications equipment be designed to ensure that the government can intercept telephone calls (with a court order or other authorization).
 - Rules and requirements written by Federal Communications Commission (FCC)



The NSA and Secret Intelligence Gathering

- The National Security Agency (NSA)
 - Foreign Intelligence Surveillance Act (FISA) established oversight rules for the NSA
- Secret access to communications records