

CSE312/ISE312

Gift of Fire, Fourth edition by Sara Baase

Read: Section 2.5-2.6

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



What We Will Cover

- The Business and Social Sectors
- Government Systems
- Protecting Privacy: Technology, Markets, Rights, and Laws
- Communications

Corresponding page number: 95-119




Protecting Privacy

Technology and Markets:

- Privacy enhancing-technologies (ad blockers, anonymizers, etc.)
- Encryption
 - Private-key
 - Public-key
 - One-way (e.g., message digests)
- Business tools and policies for protecting data


Corresponding page number: 95-100



Encryption Policy

- Government control of encryption prior to 1970s
- Government attempted ban on export of strong encryption software in the 1990s
- Key escrow attempts
- Is software free speech?
- Removal of government restrictions in 2000

Corresponding page number: 98-100



Rights and Law

- Differing view on legal treatment of personal data (e.g., property rights)
- A basic legal framework: Enforcement of agreements and contracts

Can we own facts about ourselves?

Can we apply property rights to information about ourselves?

What information about ourselves do you consider private?

Corresponding page number: 103-106



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

Corresponding page number: 107-110

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

How would the free market view and the consumer protection view differ on errors in Credit Bureau databases?

Corresponding page number: 107-110

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

Corresponding page number: 113-115

CALEA

- The Communications Assistance for Law Enforcement Act
- 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)

Corresponding page number: 115-116

The NSA and Secret Intelligence Gathering

- The National Security Agency (NSA)
 - Robust code-breaking capability
 - Restricted to intercepting communications outside the US
 - Foreign Intelligence Surveillance Act (FISA) established oversight rules for the NSA
- Performs deep packet inspection
- Established an enormous DB of communications

Do you think there should be more oversight of NSA activities?

Do you think that security provided by the NSA justifies some loss of privacy?

Corresponding page number: 116-119