Chapter 2 Summary: Privacy:

I. Definition:

Digital technology and the Internet have made new threats possible and old threats more potent. Computer technologies-Daterbases (Haraty), digital cameras, the Web, among others- have profoundly changed what people can know about us and how they can use the information.

**ASPECTS OF PRIVACY:**

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

We cannot expect complete privacy.

Personal information: Includes any information relating to, or traceable to, an individual person.

**PRIVACY THREATS:**

* Intentional, institutional uses of personal information (primarily for law enforcement and tax collection in the government sector by both businesses and organizations).
* Unauthorized use or release by “insiders”, the people who maintain the information.
* Theft of information.
* Inadvertent leakage of information through negligence or carelessness.
* Our own actions (sometimes intentional trade-offs and sometimes when we are unaware of the risks).

Anonymity: It can protect both privacy and freedom of speech but makes crime easier.

II. New Technology, New Risks:

* GPS and other devices enable others to determine a person’s location and track a person’s movements.
* Government agencies have very sophisticated tools for eavesdropping, watching us, and collecting and analyzing data about us. They can use the tools to reduce crime and increase security and to infringe privacy.

Search engines:

* Collect many terabytes of data.
* Use information to better guess the context of your search.
* Companies analyze the data.

Risks:

* Re-identification which means identifying a person from a set of anonymous data.
* Anything we do online is recorded.
* With the huge amount of storage available, companies, organizations, and governments save huge amounts data that no one would have imagined saving in the recent past.
* People often are not aware that information about them and their activities is being collected and saved.
* Leaks happen. The existence of the data presents a risk.
* Search queries can give a fairly detailed picture of a person’s life.
* Re-identification has become much easier.
* The government sometimes requests or demands sensitive personal data held by businesses and organizations.
* It is extremely likely that data collected for one purpose will be used for other purposes.
* We cannot directly protect information about ourselves. We must depend on the businesses and organizations that hold it to protect it from thieves, accidental leaks, and government prying.

III- Terminology and principles for data collection and use:

**Invisible information gathering:** Describes collection of personal information about someone without the person’s knowledge.

**Cookies:** Are files a Web site stores on each visitor’s computer.

**Terms of service:** In many cases, customer contracts or policy statements inform customers, members, and subscribers about a business or Web site policy on collecting and using data, but many people simply do not read them.

**Secondary use:** Use of personal information for a purpose other than one for which it was supplied.

**Data mining:** Searching and analyzing masses of data to find data patterns and develop new information or knowledge.

**Computer matching:** Combining and comparing information from different databases, often using an identifier such as a person’s SSN to match records.

**Computer profiling:** Analyzing data in computer files to determine characteristics of people most likely to engage in certain behavior.

**Principles for data collection and use:** The first principle for ethical treatment of personal information is informed consent. People vary in how much they value their privacy. The most desirable policy is to give people some control over secondary uses. Such choices are *opt in* and *opt out*. To request that one’s information not be used in a particular way.

**PRIVACY PRINCIPLES FOR PERSONAL INFORMATION:**

* Inform people when personally identifiable information about them is collected, what is collected, and how it will be used.
* Collect only the data needed.
* Offer a way for people to opt out from mailing lists, advertising, and transfer of their data to other parties, and other secondary uses.
* Provide stronger protection for sensitive data, for example, an opt-in policy for disclosure of medical data.
* Keep data only as long as needed.
* Maintain accuracy of data. Where appropriate and reasonable, provide a way for people to access and correct data stored about them.
* Protect security of data (from theft and from accidental leaks).
* Develop policies for responding to law enforcement requests for data.

IV- Big Brother:

The government, the use of myriad personal-data systems to investigate or monitor people is sometimes called *dataveillance*, short for “data-surveillance”. Governments collect data from a variety of sources.

**Databases:** Government databases help government agencies perform their functions, determine eligibility for government jobs and benefits programs, detect fraud in government programs, collect taxes, and catch people who are breaking laws.

**V- The fourth amendment, expectation of privacy, and surveillance technologies:**

*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.*

**Weakening the fourth amendment:**

The Fourth Amendment sets limits on the government’s rights to legally search our homes and businesses and seize documents. It requires that the government have “probable cause” for the search and seizure. That is, there must be good evidence to support the specific search. Two key problems arise from computer technology. First, much of our personal information is no longer safe in our homes or the individual offices of our doctors and financial advisors. Second, new technologies allow the government to search our homes without entering them and to search our persons from a distance without our knowledge. We first consider personal information.

**Video surveillance:** We are used to security cameras in banks and convenience stores. They help in investigations of crimes. Prisons use video surveillance systems for security. Gambling casinos use them to watch for known cheaters. Video surveillance systems monitor traffic and catch drivers who run red lights.

Cameras alone raise some privacy issues. When combined with face-recognition systems, they raise even more privacy issues. We describe applications of cameras and face recognition and some relevant privacy and civil liberties issues.

**Paying for consumer information:** Consumer information is very valuable to marketers. When businesses first began using it heavily, some privacy advocates argued that they should pay consumers for its use.

**Data firms and consumer profiles:**

There is a vast world of data collection over which we have little or no direct control. Many companies that maintain huge consumer databases buy (or merge with) other companies, combining data to build more detailed databases and dossiers.

**Located tracking:** GPS, cell phone, and other technologies and devices enable the development of a large variety of new location-based applications, that is, computer and communications services that depend on knowing exactly where a person (or object) is at a particular time.

**Stolen and lost data:** One of the risks associated with databases of personal information is that criminals steal and use the information. Criminals steal personal data by hacking into computer systems, by stealing computers and disks, by buying or requesting records under false pretenses, and by bribing employees of companies that store the data. Investigators and data brokers get a lot of information by a process called *pretexting* that is by pretending to be someone with a legitimate reason for obtaining the data. (Social engineering).

**Law and ethical responsibility:** Those who collect and store personal data have a responsibility to protect them from misuse. Those responsible for personal data must continually update security policies to cover new technologies and new potential threats.

**What we do ourselves:**

Some people do not know or understand enough how the Web works in order to make good decisions about what to put there. People often want a lot of information about others but do not want others to have access to the same kinds of information about themselves. The Web is public. Most people are decent and harmless, but a lot are evil and dangerous.

**Public records: Access versus privacy:**

Governments maintain “public records”, records that are available to the public. Lawyers, private investigators, journalists, real estate brokers, neighbors, and others use the records.

**Encryption:** Encryption generally includes a coding scheme, or cryptographic algorithm, and specific sequences of characters, called *keys*, used by the algorithm. It is possible to crack using mathematical tools and powerful computer.  
**Rights and law:** The Fourth Amendment protects the negative right (a liberty) against intrusion and interference by government.

**The free-market view:** A free-market view emphasizes freedom of contract: People should be free to enter agreements (or not enter agreements) to disclose personal information in exchange for a fee, services, or other benefits according to their own judgment. The free-market viewpoint sees privacy as a “good”, in the sense that it is both desirable and something we can obtain varying amounts of by buying or trading in the economy.

**The consumer-production view:** This viewpoint is to protect consumers against abuses and carelessness by businesses and against their own lack knowledge, judgment, or interest.

**Communications:** To collect evidence, intelligence agencies intercept communications to collect information about the activities and plans of hostile governments and terrorists. The government needs a court order to legally intercept or record the content of a telephone call for a criminal investigation.

**Designing communications systems for interception:**

New communications technologies developed made access to the content of telephone calls more difficult for law enforcement agencies than it was before.