On the one hand, information about people is gathered, stored, analyzed, and reported because organizations can use it to make better decisions. Some of these decisions, including whether or not to hire a job candidate, approve a loan, or offer a scholarship.

In addition, in this competitive global market it is importance to know consumers’ purchasing habits and financial condition. Companies use this information to target marketing efforts to consumers who are most likely to buy their products and services. Organizations also need basic information about customers to serve them better. It is hard to imagine an organization having productive relationships with its customers without having data about them. Thus, organizations want systems that collect and store key data from every interaction they have with a customer.

A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales. Reasonable limits must be set on government and business access to personal information; new information and communication technologies must be designed to protect rather than diminish privacy; and appropriate corporate policies must be developed to set baseline standards for people’s privacy.

“the right to be left alone—the most comprehensive of rights, and the right most valued by a free people.”

Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one’s personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).

# Privacy Laws, Applications, and Court Rulings

The discussion will be broken into the following topics: financial data, health information, children’s personal data, electronic surveillance, export of personal data, and access to government records.

## Financial Data

Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, checking and savings accounts, loans, payroll direct deposit, and brokerage accounts. To access many of these financial products and services, individuals must use a personal logon name, password, account number, or PIN. Individuals should be concerned about how this personal data is protected by businesses and other organizations and whether or not it is shared with other people or companies.

* Financial Privacy Rule—This rule established mandatory guidelines for the collection and disclosure of personal financial information by financial organizations.
* Safeguards Rule—This rule requires each financial institution to document a data security plan describing its preparation and plans for the ongoing protection of clients’ personal data.
* Pretexting Rule—This rule addresses attempts by people to access personal information without proper authority by such means as impersonating an account holder or phishing.

## Health Information

The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread. Individuals are rightly concerned about the erosion of privacy of data concerning their health.

## Children’s Personal Data

Internet use by children continues to climb; a recent report out of the United Kingdom found that teenagers spend an average of 31 hours per week online. As a concerned society, many of us feel that there is a need to protect children from being exposed to inappropriate material and online predators; becoming the target of harassment; divulging personal data; and becoming involved in gambling or other inappropriate behavior.

## Export of Personal Data

Various organizations have developed guidelines to ensure that the flow of personal data across national boundaries (transborder data flow) does not result in the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.

## Access to Government Records

The government has a great capacity to store data about each and every one of us and about the proceedings of its various organizations. The Freedom of Information Act enables the public to gain access to certain government records, and the Privacy Act prohibits the government from concealing the existence of any personal data record-keeping systems.

# Identity Theft

Identity theft occurs when someone steals key pieces of personal information to impersonate a person. This information may include such data as name, address, date of birth, Social Security number, passport number, driver’s license number, and mother’s maiden name. Using this information, an identity thief may apply for new credit or financial accounts, rent an apartment, set up utility or phone service, and register for college courses—all in someone else’s name.

Four approaches are frequently used by identity thieves to capture the personal data of their victims: (1) create a data breach to steal hundreds, thousands, or even millions of personal records; (2) purchase personal data from criminals; (3) use phishing to entice users to willingly give up personal data; and (4) install spyware capable of capturing the keystrokes of victims.

## Data Breaches

An alarming number of identity theft incidents involve breaches of large databases to gain personal identity information. The breach may be caused by hackers breaking into the database or, more often than one would suspect, by carelessness or failure to follow proper security procedures.

## Purchase of Personal Data

There is a black market in personal data.

## Phishing

Phishing is an attempt to steal personal identity data by tricking users into entering information on a counterfeit Web site.

## Spyware

Spyware is keystroke-logging software downloaded to users’ computers without the knowledge or consent of the user. It is often marketed as a spouse monitor, child monitor, or surveillance tool. Spyware creates a record of the keystrokes entered on the computer, enabling the capture of account usernames, passwords, credit card numbers, and other sensitive information.

## Identity Theft Monitoring Services

There are numerous identity theft monitoring services, which offer a wide range of coverage.

# Consumer Profiling

Companies openly collect personal information about Internet users when they register at Web sites, complete surveys, fill out forms, or enter contests online. Many companies also obtain information about Web surfers through the use of cookies, text files that a Web site can download to visitors’ hard drives so that it can identify visitors on subsequent visits. Companies also use tracking software to allow their Web sites to analyze browsing habits and deduce personal interests and preferences. The use of cookies and tracking software is controversial because companies can collect information about consumers without their explicit permission. Outside of the Web environment, marketing firms employ similarly controversial means to collect information about people and their buying habits.

## Aggregating Consumer Data

Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data. They want to know as much as they can about consumers—who they are, what they like, how they behave, and what motivates them to buy. The marketing firms provide this data to companies so that they can tailor their products and services to individual consumer preferences. Advertisers use the data to more effectively target and attract customers to their messages.

## Collecting Data from Web Site Visits

Marketers use cookies to recognize return visitors to their sites and to store useful information about them. The goal is to provide customized service for each consumer. When someone visits a Web site, the site asks that person’s computer if it can store a cookie on the hard drive. If the computer agrees, it is assigned a unique identifier, and a cookie with this identification number is placed on its hard drive.

## Personalization Software

In addition to using cookies to track consumer data, online marketers use personalization software to optimize the number, frequency, and mixture of their ad placements, and to evaluate how visitors react to new ads. The goal is to turn first-time visitors to a site into paying customers and to facilitate greater cross-selling activities.

## Consumer Data Privacy

Consumer data privacy has grown into a major marketing issue. Companies that can’t protect or don’t respect customer information often lose business and some become defendants in class action lawsuits stemming from privacy violations.

# Workplace Monitoring

Many organizations have developed a policy on the use of IT in the workplace in order to protect against employee abuses that reduce worker productivity or expose the employer to harassment lawsuits.

# Chapter 2

A profession is a calling that requires specialized knowledge and often long and intensive academic preparation.

IT workers are not recognized as professionals because they are not licensed by the state or federal government. This distinction is important, for example, in malpractice lawsuits, as many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional.