PRIVACY

Book: A Gift of Fire
Chapter 2
Book: Ethics in Information Technology
Chapter 4

Information Privacy

- Definition of privacy
  - *"The right to be left alone"*

- Information privacy is a combination of:
  - *Communications privacy*
  - *Data privacy*

  Communications privacy
    - Ability to communicate with others without being monitored by other persons or organizations

  Data privacy
    - 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 and Computer Technology

- Computer technology is not necessary for the invasion of privacy.
- Computer technologies—databases, digital cameras, the Web, smartphones, and global positioning system (GPS) devices, among others—have profoundly changed what people can know about us and how they can use that information.
- Understanding the risks and problems is a first step towards protecting privacy.
- ***For computer professionals, understanding the risks and problems is a step towards designing systems with built-in privacy protections and less risk.***

Privacy and Computer Technology

Key Aspects of Privacy:

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

Privacy threats come in several categories

- Intentional, institutional uses of personal information (in the government sector primarily for law enforcement and tax collection, and in the private sector primarily for marketing and decision making)
- 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 when we are unaware of the risks)

Privacy and Computer Technology (cont.)

New Technology, New Risks:

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

Government and private databases

- Today there are thousands (probably millions) of databases, both government and private, containing personal information about us. In the past, there was simply no record of some of this information, such as our specific purchases of groceries and books. Government documents like divorce and bankruptcy records have long been in public records, but accessing such information took a lot of time and effort. When we browsed in a library or store, no one knew what we read or looked at. It was not easy to link together our financial, work, and family records.

Government and private databases

- Now, large companies that operate video, email, social network, and search services can combine information from a member's use of all of them to obtain a detailed picture of the person's interests, opinions, relationships, habits, and activities.
- Even if we do not log in as members, software tracks our activity on the Web. In the past, conversations disappeared when people finished speaking, and only the sender and the recipient normally read personal communications.
- Now, when we communicate by texting, email, social networks, and so on, there is a record of our words that others can copy, forward, distribute widely, and read years later.

Sophisticated tools for surveillance and data analysis

- Miniaturization of processors and sensors put tiny cameras in cellphones that millions of people carry everywhere. Cameras in some 3-D television sets warn children if they are sitting too close. What else might such cameras record, and who might see it?
- The wireless appliances we carry contain GPS and other location devices. They enable others to determine our location and track our movements.
- Patients refill prescriptions and check the results of medical tests on the Web. They correspond with doctors by email.

Sophisticated tools for surveillance and data analysis

- We store our photos and videos, do our taxes, and create and store documents and financial spreadsheets in a cloud of remote servers instead of on our own computer.
- Law enforcement agencies have very sophisticated tools for eavesdropping, surveillance, and collecting and analyzing data about people's activities, tools that can help reduce crime and increase security—or threaten privacy and liberty.

Vulnerability of data

- Combining powerful new tools and applications can have astonishing results. It is possible to snap a photo of someone on the street, match the photo to one on a social network, and use a trove of publicly accessible information to guess, with high probability of accuracy, the person's name, birth date, and most of his or her Social Security number.
- This does not require a supercomputer; it is done with a smartphone app. We see such systems in television shows and movies, but to most people they seem exaggerated or way off in the future. All these gadgets, services, and activities have benefits, of course, but they expose us to new risks. The implications for privacy are profound.

Stolen and Lost Data

- Hackers
- Physical theft (laptops, thumb-drives, etc.)
- Requesting information under false pretenses
- Bribery of employees who have access

Stolen and lost data

- 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.
- Shady information brokers sell data (including cellphone records, credit reports, credit card statements, medical and work records, and location of relatives, as well as information about financial and investment accounts) that they obtain illegally or by questionable means.
- Criminals, lawyers, private investigators, spouses, ex-spouses, and law enforcement agents are among the buyers. A private investigator could have obtained some of this information in the past, but not nearly so easily, cheaply, and quickly.

Stolen and lost data

- Another risk is accidental (sometimes quite careless) loss. Businesses, government agencies, and other institutions lose computers, disks, memory cards, and laptops containing sensitive personal data (such as Social Security numbers and credit card numbers) on thousands or millions of people, exposing people to potential misuse of their information and lingering uncertainty.
- They inadvertently allow sensitive files to be public on the Web. Researchers found medical information, Social Security numbers, and other sensitive personal or confidential information about thousands of people in files on the Web that simply had the wrong access status.

Stolen and lost data

- The websites of some businesses, organizations, and government agencies that make account information available on the Web do not sufficiently authenticate the person accessing the information, allowing imposters access.
- Data thieves often get sensitive information by telephone by pretending to be the person whose records they seek. They provide some personal information about their target to make their request seem legitimate. That is one reason why it is important to be cautious even with data that is not particularly sensitive by itself.

A summary of risks

- Anything we do in cyberspace is recorded, at least briefly, and linked to our computer or phone, and possibly our name.
- With the huge amount of storage space available, companies, organizations, and governments save huge amounts of data that no one would have imagined saving in the recent past.
- People often are not aware of the collection of information about them and their activities.
- Software is extremely complex. Sometimes businesses, organizations, and website managers do not even know what the software they use collects and stores.

A summary of risks

- Leaks happen. The existence of the data presents a risk.
- A collection of many small items of information can give a fairly detailed picture of a person's life.
- Direct association with a person's name is not essential for compromising privacy. Re-identification has become much easier due to the quantity of personal information stored and the power of data search and analysis tools.
- If information is on a public website, people other than those for whom it was intended will find it. It is available to everyone.

A summary of risks

- Once information goes on the Internet or into a database, it seems to last forever. People (and automated software) quickly make and distribute copies. It is almost impossible to remove released information from circulation.
- It is extremely likely that data collected for one purpose (such as making a phone call or responding to a search query) will find other uses (such as business planning, tracking, marketing, or criminal investigations).
- The government sometimes requests or demands sensitive personal data held by businesses and organizations.
- We often cannot directly protect information about ourselves. We depend on the businesses and organizations that manage it to protect it from thieves, accidental collection, leaks, and government prying.

Key Issues of Privacy

Term : Personal information

In the context of privacy issues, it includes any information relating to, or traceable to, an individual person

It also includes information associated with a particular person's user name, online nickname, identification number, email address, or phone number.

Nor does it refer only to text. It extends to any information, including images, from which someone can identify a living individual.

1. Invisible Information Gathering

- Collection of personal information about someone without the person's knowledge
- The important ethical issue is that if someone is not aware of the collection and use, he or she has no opportunity to consent or withhold consent.
- Whether or not a particular example of data collection is invisible information gathering can depend on the level of public awareness.
- Example: Cartoon character cursor, spyware, event data recorders etc

Invisible Information Gathering

When our computers and phones communicate with websites, they must provide information about their configuration (e.g., the Web browser used).

Some companies provide device fingerprinting software for combating fraud and intellectual property theft and for tracking people's online activity.

Both collection of configuration information and building of activity profiles are invisible. Financial firms that use device fingerprinting for security of customer accounts are likely to say so in a privacy policy. We are less likely to know when someone is using it to build marketing profiles.

Invisible information gathering

- ***Cookies*** are files a website stores on a visitor's computer. Within the cookie, the site stores and then uses information about the visitor's activity.
- For example, a retail site might store information about products we looked at and the contents of our virtual "shopping cart." On subsequent visits, the site retrieves information from the cookie. Cookies help companies provide personalized customer service and target advertising to the interests of each visitor. They can also track our activities on many sites and combine the information. Today, more people are aware of cookies and use tools to prevent or delete them.

Personalization software

- Rule based personalization software
- Collaborative filtering
- Demographic filtering
- Contextual commerce

2. Secondary use

- use of personal information for a purpose other than the one it was provided for
- Examples include sale of consumer information to marketers or other businesses.

Data Mining, Matching & Profiling

- ***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 (using social security number, for example, to match records)
- ***Computer profiling*** - analyzing data in computer files to determine characteristics of people most likely to engage in certain behavior

3. Identity Theft

- Theft of key pieces of personal information to impersonate a person, including:
  - *Name*
  - *Address*
  - *Date of birth*
  - *Social Security number*
  - *Passport number*
  - *Driver's license number*
  - *Mother's maiden name*

Identity Theft (cont'd.)

- Four approaches used by identity thieves
  - *Create a data breach (caused by hacking, theft.)*
  - *Purchase personal data*
  - *Use phishing to entice users to give up data*
  - *Install spyware to capture keystrokes of victims*

Principles for Data Collection and Use

Principles for Data Collection and Use:

- Informed consent
- Opt-in and opt-out policies
- Fair Information Principles (or Practices)

Informed consent

- There is an extra ordinary range to amount of privacy different people want. Some blog about their married life and affairs however others do not leave without a record of their purchase. They get angry if anyone collects information about them.
- If any company collects data about individual and let them know the use policies person can decide according to his/her own values.

Opt in- opt out policies

- Under an opt-out policy, one must check or click a box on a contract, membership form, or agreement or contact the organization to request that they not use one's information in a particular way. If the person does not take action, the presumption is that the organization may use the information.
- Under an opt-in policy, the collector of the information may not use it for secondary uses unless the person explicitly checks or clicks a box or signs a form permitting the use.

Fair Information Principles (or Practices)

- Inform people when you collect information about them, what you collect, and how you use it. Some important points are :-
- Collect only the data needed.
- Offer a way for people to opt out from mailing lists, advertising, and other secondary uses. Offer a way for people to opt out from features and services that expose personal information.

Fair Information Principles (or Practices)

- 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). Provide stronger protection for sensitive data.
- Develop policies for responding to law enforcement requests for data.

Fair Information Principles (or Practices)

- It can be difficult to apply the fair information principles to some new technologies and applications
- the increase of cameras in public places
- the enormous amount of personal information people share in social networks, and the power of smartphones.
- For example, when someone puts personal information in a tweet to thousands of people, how do we determine the purpose for which he or she supplied the information? Can any recipient use the information in any way? How widely distributed must information be before it is public in the sense that anyone can see or use it?

Key Privacy and Anonymity Issues

- Identity theft
- Electronic discovery
- Consumer profiling
- Treating customer data responsibly
- Workplace monitoring
- Advanced surveillance technology

Identity Theft

- Theft of key pieces of personal information to impersonate a person, including:
  - *Name*
  - *Address*
  - *Date of birth*
  - *Social Security number*
  - *Passport number*
  - *Driver's license number*
  - *Mother's maiden name*
- Fastest-growing form of fraud in the United States
- Consumers and organizations are becoming more vigilant and proactive in fighting identity theft
- Four approaches used by identity thieves
  - *Create a data breach to steal hundreds, thousands, or even millions of personal records*
  - *Purchase personal data from criminals*
  - *Use phishing to attract users to willingly give up personal data*
  - *Install spyware to capture keystrokes of victims*

Identity Theft (cont'd.)

- Data breaches of large databases
  - *To gain personal identity information*
  - *May be caused by:*
    - Hackers
    - Failure to follow proper security procedures
- Purchase of personal data
  - *Black market for:*
    - Credit card numbers in bulk—$.40 each
    - Logon name and PIN for bank account—$10
    - Identity information—including DOB, address, SSN, and telephone number—$1 to $15
- Phishing
  - *Stealing personal identity data by tricking users into entering information on a counterfeit Web site*
- *Spyware*
  - *Keystroke-logging software*
  - *Enables the capture of:*
    - Account usernames
    - Passwords
    - Credit card numbers
    - Other sensitive information
  - *Operates even if infected computer is not online*

Electronic Discovery

- Collection, preparation, review, and production of electronically stored information for use in criminal and civil actions
- Quite likely that information of a private or personal nature will be disclosed during e-discovery
- Federal Rules of Procedure define e-discovery processes
- E-discovery is complicated and requires extensive time to collect, prepare, and review data
- Raises many ethical issues
  - *Should an organization attempt to destroy or conceal incriminating evidence?*
  - *To what degree must an organization be proactive and thorough in providing evidence?*
  - *Should an organization attempt to "bury" incriminating evidence in a mountain of trivial, routine data?*

Consumer Profiling

- Companies openly collect personal information about Internet users
- Cookies
  - *Text files that a Web site can download to visitors' hard drives so that it can identify visitors later*
- Tracking software analyzes browsing habits
- Aggregating consumer data
  - *Databases contain a huge amount of consumer behavioral data*
- Collecting data from Web site visits
  - *Goal: provide customized service for each consumer*

Consumer Profiling (cont'd.)

- Personalization software
  - *Used by marketers to optimize the number, frequency, and mixture of their ad placements*
- Consumer data privacy
  - *Platform for Privacy Preferences (P3P)*
    - Shields users from sites that don't provide the level of privacy protection desired

Treating Consumer Data Responsibly

- Strong measures are required to avoid customer relationship problems
- Companies should adopt:
  - *Fair Information Practices*
- Chief privacy officer (CPO)
  - *Executive to oversee data privacy policies and initiatives*

Treating Consumer Data Responsibly (cont'd.)

TABLE 4-6 Manager's checklist for treating consumer data responsibly

Question	Yes	No
Does your company have a written data privacy policy that is followed?		
Can consumers easily view your data privacy policy?		
Are consumers given an opportunity to opt in or opt out of your data policy?		
Do you collect only the personal information needed to deliver your product or service?		
Do you ensure that the information is carefully protected and accessible only by those with a need to know?		
Do you provide a process for consumers to review their own data and make corrections?		
Do you inform your customers if you intend to use their information for research or marketing and provide a means for them to opt out?		
Have you identified a person who has full responsibility for implementing your data policy and dealing with consumer data issues?		

Source Line: Course Technology/Cengage Learning.

Workplace Monitoring

- Employers monitor workers
  - *Protect against employee abuses that reduce worker productivity or expose employer to harassment lawsuits*
- Privacy advocates want federal legislation
  - *To keep employers from infringing upon privacy rights of employees*

Advanced Surveillance Technology

- Camera surveillance
  - *Many cities plan to expand surveillance systems*
  - *Advocates argue people have no expectation of privacy in a public place*
  - *Critics concerned about potential for abuse*
- Global positioning system (GPS) chips
  - *Placed in many devices*
  - *Precisely locate users*
  - *Banks, retailers, airlines eager to launch new services based on knowledge of consumer location*

Protecting Privacy

Technology and Markets:

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

Technology and Markets

Privacy enhancing-technologies for consumers

- Many individuals, organizations, and businesses help meet the demand for privacy to some degree:
  - *Individual programmers post free privacy-protecting software on the Web.*
  - *Entrepreneurs build new companies to provide technology-based privacy protections.*
  - *Large businesses respond to consumer demand and improve policies and services.*
  - *Organizations such as the Privacy Rights Clearing house provide excellent information resources.*
  - *Activist organizations such as the Electronic Privacy Information Center inform the public, file lawsuits, and advocate for better privacy protection.*

Encryption

- It is possible to intercept email and data in transit on the Internet and to pick wireless transmissions out of the air. Someone who steals a computer or hacks into one can view files on it.
- Most eavesdropping by private citizens is illegal. Hacking and stealing laptops are crimes. The law provides for punishment of offenders when caught and convicted, but we can also use technology to protect ourselves.

Encryption

- Encryption is a technology, often implemented in software, that transforms data into a form that is meaningless to anyone who might intercept or view it. The data could be email, business plans, credit card numbers, images, medical records, cellphone location history, and so on.
- Software at the recipient's site (or on one's own computer) decodes encrypted data so that the recipient or owner can view the messages or files. Software routinely encrypts credit card numbers when we send them to online merchants. People are often not even aware that they are using encryption. The software handles it automatically.

Encryption

- Many privacy and security professionals view encryption as the most important technical method for ensuring the privacy of messages and data sent through computer networks.
- Encryption also protects stored information from intruders and abuses by employees.
- It is the best protection for data on laptops and other small data storage devices carried outside an office.

Encryption

Encryption generally includes a coding scheme, or cryptographic algorithm, and specific sequences of characters (e.g., digits or letters), called *keys*, used by the algorithm. Using mathematical tools and powerful computers, it is sometimes possible to "break" an encryption scheme—that is, to decode an encrypted message or file without the secret key. Modern encryption technology has a flexibility and variety of applications beyond protecting data. For example, it is used to create ***digital signatures, authentication methods, and digital cash.***

Business tools and policies for protecting data

The businesses, organizations, and government agencies that collect and store personal data have an ethical responsibility (and in many cases a legal one) to protect it from misuse.

Responsible data holders must anticipate risks and prepare for them. They must continually update security policies to cover new technologies and new potential threats.

Business tools and policies for protecting data

A well-designed database for sensitive information includes several features to protect against leaks, intruders, and unauthorized employee access.

Each person with authorized access to the system should have a unique identifier and a password.

A system can restrict users from performing certain operations, such as writing or deleting, on some files. User IDs can be coded so that they give access to only specific parts of a record. For example, a billing clerk in a hospital does not need access to the results of a patient's lab tests.

Business tools and policies for protecting data

- The computer system keeps track of information about each access, including the ID of the person looking at a record and the particular information viewed or modified.
- This is an *audit trail* that can later help trace unauthorized activity.
- The knowledge that a system contains such provisions will discourage many privacy violations.

Business tools and policies for protecting data

Website operators pay thousands, sometimes millions, of dollars to companies that do *privacy audits*. Privacy auditors check for leaks of information, review the company's privacy policy and its compliance with that policy, evaluate warnings and explanations on its website that alert visitors when the site requests sensitive data, and so forth. Hundreds of large businesses have a position called *chief privacy officer*. This person guides company privacy policy. Just as the Automobile Association of America rates hotels, the Better Business Bureau and similar organizations offer a seal of approval, an icon companies that comply with their privacy standards can post on websites.

Business tools and policies for protecting data

Large companies use their economic influence to improve consumer privacy. IBM and Microsoft removed Internet advertising from websites that do not post clear privacy policies. Walt Disney Company and Info seek Corporation did the same and, in addition, stopped accepting advertising on their websites from sites that do not post privacy policies.

The Direct Marketing Association adopted a policy requiring its member companies to inform consumers when they will share personal information with other marketers and to give people an opt-out option.

Business tools and policies for protecting data

Many companies agreed to limit the availability of sensitive consumer information, including unlisted telephone numbers, driving histories, and all information about children. There continue, of course, to be many businesses without strong privacy policies, as well as many that do not follow their own stated policies. The examples described here represent a trend. They suggest actions responsible companies can take. As some problems are addressed, new ones continually arise.

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?