# Privacy

In general, privacy is the right to be left alone and to be free of unreasonable personal intrusions. Information privacy is the right to determine when, and to what extent, information about you can be gathered and/or communicated to others.

Privacy rights apply to individuals, groups, and institutions. The right to privacy is recognized today in all U.S. states and by the federal government, either by statute or in common law.

Privacy can be interpreted quite broadly. However, court decisions in many countries have followed two rules fairly closely:

1. The right of privacy is not absolute. Privacy must be balanced against the needs of society.

2. The public's right to know supersedes the individual's right of privacy

These two rules illustrate why determining and enforcing privacy regulations can be difficult.

As we discussed earlier, rapid advances in information technologies have made it much easier to collect, store, and integrate vast amounts of data on individuals in large databases. On an average day, data about you are generated in many ways: surveillance cameras located on toll roads, on other roadways, in busy intersections, in public places, and at work; credit card transactions; telephone calls (landline and cellular); banking transactions; queries to search engines; and government records (including police records). These data can be integrated to produce a digital dossier, which is an electronic profile of you and your habits. The process of forming a digital dossier is called profiling.

Data aggregators, such as LexisNexis (www.lexisnexis.com), ChoicePoint (www.choicepoint .com), and Acxiom (www.acxiom.com), are prominent examples of profilers. These companies collect public data such as real estate records and published telephone numbers, in addition to nonpublic information such as Social Security numbers; fi nancial data; and police, criminal, and motor vehicle records. They then integrate these data to form digital dossiers on most adults in the United States. They ultimately sell these dossiers to law enforcement agencies and companies that conduct background checks on potential employees. They also sell them to companies that want to know their customers better, a process called customer intimacy.

## Electronic Surveillance

According to the American Civil Liberties Union (ACLU), tracking people's activities with the aid of information technology has become a major privacy-related problem. The ACLU notes that this monitoring, or electronic surveillance, is rapidly increasing, particularly with the emergence of new technologies. Electronic surveillance is conducted by employers, the government, and other institutions.

Emerging technologies such as low-cost digital cameras, motion sensors, and biometric readers are helping to increase the monitoring of human activity. In addition, the costs of storing and using digital data are rapidly decreasing. The result is an explosion of sensor data collection and storage.

In fact, your smartphone has become a sensor. The average price of a smartphone has increased 17 percent since 2000. However, the phone's processing capability has increased by 13,000 percent during that time, according to technology market research fi rm ABI Research (www.abiresearch.com)

smartphones can now record video, take pictures, send and receive e-mail, search for information, access the Internet, and locate you on a map, among many other things. Your phone also stores large amounts of information about you that can be collected and analyzed. A special problem arises with smartphones that are equipped with global positioning system (GPS) sensors. These sensors routinely geotag photos and videos, embedding images with the longitude and latitude of the location shown in

the image. Thus, you could be inadvertently supplying criminals with useful intelligence by posting personal images on social networks or photo-sharing Web sites. These actions would show the criminals exactly where you live.

Another example of how new devices can contribute to electronic surveillance is facial recognition technology. Just a few years ago, this software worked only in very controlled settings such as passport checkpoints. However, this technology can now match faces even in regular snapshots and online images. For example, Intel and Microsoft have introduced in-store digital billboards that can recognize your face. These billboards can keep track of the products you are interested in based on your purchases or browsing behavior. One marketing analyst has predicted that your experience in every store will soon be customized.

Google and Facebook are using facial-recognition software—Google Picasa and Facebook Photo Albums—in their popular online photo-editing and sharing services. Both companies encourage users to assign names to people in photos, a practice referred to as photo tagging. Facial-recognition software then indexes facial features. Once an individual in a photo is tagged, the software searches for similar facial features in untagged photos. This process allows the user to quickly group photos in which the tagged person appears. Signifi cantly, the individual is not aware of this process.

Once you are tagged in a photo, that photo can be used to search for matches across the entire Internet or in private databases, including databases fed by surveillance cameras. How could this type of surveillance affect you? As one example, a car dealer can take a picture of you when you step onto the car lot. He or she could then quickly profi le you (fi nd out information about where you live, your employment, etc.)

The scenarios we just considered deal primarily with your personal life. However, electronic surveillance has become a reality in the workplace as well. In general, employees have very limited legal protection against surveillance by employers. The law supports the right of employers to read their employees' e-mail and other electronic documents and to monitor their employees' Internet use. Today, more than three-fourths of organizations routinely monitor their employees' Internet usage. In addition, two-thirds use software to block connections to inappropriate Web sites, a practice called URL fi ltering. Further, organizations are installing monitoring and fi ltering software to enhance security by blocking malicious software and to increase productivity by discouraging employees from wasting time

## Personal Information in Databases

• Do you know where the records are? • Are the records accurate? • Can you change inaccurate data? • How long will it take to make a change? • Under what circumstances will personal data be released? • How are the data used? • To whom are the data given or sold? • How secure are the data against access by unauthorized people?

Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

Every day we see more and more electronic bulletin boards, newsgroups, electronic discussions such as chat rooms, and social networking sites