Privacy Act (1974)

The **Privacy Act** establishes a code of fair information practices that sets rules for the collection, maintenance, use, and dissemination of personal data that is kept in systems of records by federal agencies. It also prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system. Under this law, any agency that maintains such a system must publicly describe both the kinds of information in it and the manner in which the information will be used. The law also outlines 12 requirements that each record-keeping agency must meet, including issues that address openness, individual access, individual participation, collection limitation, use limitation, disclosure limitation, information management, and accountability. The purpose of the act is to provide safeguards for people against invasion of personal privacy by federal agencies. The CIA and law enforcement agencies are excluded from this act; in addition, it does not cover the actions of private industry.[48]

In a case involving the Privacy Act, a woman and her young daughter, both U.S. citizens, reentered the country from Canada border. A customs database incorrectly branded the mother as "armed and dangerous." She was then handcuffed, questioned for several hours, and finally released without explanation. The woman sued under the Privacy Act and sought damages from the Department of Homeland Security for the agency's failure to ensure the accuracy of its computer records. A federal appeals court held that the Privacy Act provides monetary damages for harms stemming from inaccurate government records.[49]

KEY PRIVACY AND ANONYMITY ISSUES

The rest of this chapter discusses a number of current and important privacy issues, including data breaches, electronic discovery, consumer profiling, workplace monitoring, and advanced surveillance technology.

Data Breaches

An alarming number of identity theft incidents can be traced back to data breaches involving large databases of personal information. Data breaches are sometimes caused by hackers breaking into a database, but more often than one might suspect, they are caused by carelessness or failure to follow proper security procedures. For example, a laptop computer containing the unencrypted names, birth dates, and Social Security numbers of 26.5 million U.S. veterans was stolen from the home of a Veterans Affairs (VA) analyst. The analyst violated existing VA policy by removing the data from his workplace.[50]

Table 4-3 identifies the eight largest U.S. data breaches.

The number of data breach incidents is alarming (over 1,450 in 2012 alone),[51] as is the lack of initiative by some companies in informing the people whose data was stolen. Organizations are reluctant to announce data breaches due to the ensuing bad publicity and potential for lawsuits by angry customers. However, victims whose personal data was compromised during a data breach need to be informed so that they can take protective measures.

As mentioned earlier in this chapter, the Health Information Technology for Economic and Clinical Health Act included strong privacy provisions for electronic health records.

TABLE 4-3 Largest reported U.S. data breaches

Date incident was reported	Number of records involved	Organization(s) involved
March 17, 2012	150 million	Shanghai Roadway D&B Marketing Services, Ltd.
January 20, 2009	130 million	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
January 17, 2007	94 million	The TJX Companies
June 1, 1984	90 million	TRW, Sears Roebuck
April 26, 2011	77 million	Sony Corporation
June 19, 2005	40 million	CardSystems, Visa, MasterCard, American Express
December 26, 2011	40 million	Tianya
July 28, 2011	35 million	SK Communications, Nate, Cyworld

Source Line: Open Security Foundation's DataLossDB, http://datalossdb.org.

One such mandate is that within 60 days after discovery of a data breach, each individual whose health information has been exposed must be notified, and if a breach involves 500 or more people, notice must be provided to prominent media outlets.[52] According to the Health Information Trust Alliance, from 2009 to mid-2012, there were 495 medical data breaches involving 21 million patient records. The average time to notify individuals following a breach was 68 days, with over half of the organizations failing to notify affected individuals within the 60-day deadline.[53]

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring organizations to disclose security breaches involving personal information.[54] Some states have extremely stringent laws regarding the reporting of a data breach of patient health records. For example, under California law, a data breach involving protected health information must be reported to government agencies and affected individuals within five days of discovery. The Lucile Packard Children's Hospital at Stanford University was fined $250,000 by the California Department of Public Health when it took 19 days to report the theft of a computer with protected health information on 532 patients.[55]

The cost to an organization that suffers a data breach can be quite high—by some estimates nearly $200 for each record lost. Nearly half the cost is typically a result of lost business opportunity associated with the customers whose patronage has been lost due to the incident. Other costs include public-relations-related costs to manage the firm's reputation, and increased customer-support costs for information hotlines and credit monitoring services for victims.

Zappos, an online shoe and clothing retailer and a subsidiary of Amazon, was subject to a major data breach wherein a cybercriminal gained access to customer names, email addresses, billing and shipping addresses, phone numbers, the last four digits of their credit card numbers, and the customers' encrypted passwords for the Zappos Web site. The database that stores credit card and payment data for the company was not breached. Zappos immediately emailed its 24 million customers to notify them of the data breach

and to strongly suggest that they reset their password on Zappos.com and any other Web site where they used a similar password.[56] Despite what many observers considered to be a timely response to the incident, Amazon and Zappos were hit with nine federal class action lawsuits within three months of the incident. Plaintiffs said they feared an increased risk of identity theft and other financial-related crimes.[57] It is likely that Zappos faces millions of dollars in legal fees and perhaps tens of millions of dollars in additional costs to settle the claims.

Electronic Discovery

Discovery is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents. The purpose of discovery is to ensure that all parties will go to trial with as much knowledge as possible. Under the rules of discovery, neither party is able to keep secrets from the other. Should a discovery request be objected to, the requesting party may file a motion to compel discovery with the court.

Electronic discovery (e-discovery) is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings. **Electronically stored information (ESI)** includes any form of digital information, including emails, drawings, graphs, Web pages, photographs, word-processing files, sound recordings, and databases stored on any form of electronic storage device, including hard drives, CDs, and flash drives. Through the e-discovery process, it is quite likely that various forms of ESI of a private or personal nature (e.g., personal emails) will be disclosed.

The Federal Rules of Procedure define certain processes that must be followed by a party involved in a case in federal court. Under these rules, once a case is filed, the involved parties are required to meet and discuss various e-discovery issues, such as how to preserve discoverable data, how the data will be produced, in what format data will be provided, and whether production of certain electronically stored information will lead to waiver of attorney-client privilege. A key issue is the scope of e-discovery (e.g., how many years of ESI will be requested, what topics and/or individuals need to be included in the e-discovery process, etc.).

Often organizations will send a litigation hold notice to its employees (or to the opposing party) to save relevant data and to suspend data that might be due to be destroyed based on normal data retention rules. Apple and Samsung were embroiled in a long-running dispute involving alleged patent infringement. During the litigation, the court cited Samsung for failing to circulate a comprehensive litigation hold instruction among its employees when it first anticipated litigation. According to the court, this failure resulted in the loss of emails from several key Samsung employees. Samsung then raised the same issue—Apple had neglected to implement a timely and comprehensive litigation hold to prevent broad destruction of pertinent email. A key learning from this case is that an organization should focus on its own ESI preservation and production efforts before it raises issues with its opponent's efforts.[58]

It can require extensive time to collect, prepare, and review the tremendous volume of ESI kept by an organization. E-discovery is further complicated because there are often multiple versions of information (such as various drafts) stored in many locations (such as the hard drives of the creator and anyone who reviewed the document, multiple company

file servers, and backup tapes). As a result, e-discovery can become so expensive and time consuming that some cases are settled just to avoid the costs.[59]

Traditional software development firms as well as legal organizations have recognized the growing need for improved processes to speed up and reduce the costs associated with e-discovery. As a result, dozens of companies offer e-discovery software that provides the ability to do the following:

- Analyze large volumes of ESI quickly to perform early case assessments
- Simplify and streamline data collection from across all relevant data sources in multiple data formats
- Cull large amounts of ESI to reduce the number of documents that must be processed and reviewed
- Identify all participants in an investigation to determine who knew what and when

E-discovery raises many ethical issues: Should an organization ever attempt to destroy or conceal incriminating evidence that could otherwise be revealed during discovery? To what degree must an organization be proactive and thorough in providing evidence sought through the discovery process? Should an organization attempt to bury incriminating evidence in a mountain of trivial, routine ESI?

Consumer Profiling

Companies openly collect personal information about 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 can be downloaded to the hard drives of users who visit a Web site, so that the Web site is able to 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.

After cookies have been stored on your computer, they make it possible for a Web site to tailor the ads and promotions presented to you. The marketer knows what ads have been viewed most recently and makes sure that they aren't shown again, unless the advertiser has decided to market using repetition. Some types of cookies can also track what other sites a user has visited, allowing marketers to use that data to make educated guesses about the kinds of ads that would be most interesting to the user.

In early 2012, members of the Obama administration, digital advertisers, browser software manufacturers, and privacy advocates agreed in principle to create a "Do Not Track" button for Web browsers. The idea was to make it easy for Internet users to communicate their desire to not be tracked as they surfed the Web. Users of the Firefox, Explorer, or Safari Web browsers can select a "Do Not Track" option so that the browser sends a message to each site visited that you do not wish to have cookies deposited on your computer. However, it is up to each individual Web site to decide if they will comply with your request to not be tracked; they are not required to honor your request.[60]

Outside of the Web environment, marketing firms employ similarly controversial means to collect information about people and their buying habits. Each time a consumer uses a credit card, redeems frequent flyer points, fills out a warranty card, answers a phone survey,

buys groceries using a store loyalty card, orders from a mail-order catalog, or registers a car with the DMV, the data is added to a storehouse of personal information about that consumer, which may be sold or shared with third parties. In many of these cases, consumers never explicitly consent to submitting their information to a marketing organization.

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 possible 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. Ideally, this means that buyers should be able to shop more efficiently and find products that are well suited for them. Sellers should be better able to tailor their products and services to meet their customers' desires and to increase sales. However, concerns about how this data is used prevent many potential online shoppers from making purchases.

Online marketers cannot capture personal information, such as names, addresses, and Social Security numbers, unless people provide them. Without this information, companies can't contact individual Web surfers who visit their sites. Data gathered about a user's Web browsing through the use of cookies is anonymous, as long as the network advertiser doesn't link the data with personal information. However, if a Web site visitor volunteers personal information, a Web site operator can use it to find additional personal information that the visitor may not want to disclose. For example, a name and address can be used to find a corresponding phone number, which can then lead to obtaining even more personal data. All this information becomes extremely valuable to the Web site operator, who is trying to build a relationship with Web site visitors and turn them into customers. The operator can use this data to initiate contact or sell it to other organizations with which they have marketing agreements.

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.

Opponents of consumer profiling are also concerned that personal data is being gathered and sold to other companies without the permission of consumers who provide the data. After the data has been collected, consumers have no way of knowing how it is used or who is using it.

Workplace Monitoring

Plenty of data exists to support the conclusion that many workers waste large portions of their work time doing non-work-related activity. One recent study revealed that between 60 to 80 percent of workers' time online has nothing to do with work.[61] Another source estimates that, on average, workers spend about four or five hours per week on personal matters. In a recent survey by an IT staffing firm, 54 percent of companies reported they were banning the use of social networking sites such as Facebook, Twitter, MySpace, and LinkedIn to help reduce waste at work.[62] As discussed in Chapter 2, many organizations have developed policies on the use of IT in the workplace in order to protect against employee abuses that reduce worker productivity or that expose the employer to harassment lawsuits. For example, an employee may sue his or her employer for creating

an environment conducive to sexual harassment if other employees are viewing pornography online while at work and the organization takes no measures to stop such viewing. (Email containing crude jokes and cartoons or messages that discriminate against others based on sex, race, or national origin can also spawn lawsuits.) The institution and communication of an IT usage policy establishes boundaries of acceptable behavior and enables management to take action against violators.

The potential for decreased productivity and increased legal liabilities has led many employers to monitor workers to ensure that corporate IT usage policies are being followed. Many U.S. firms find it necessary to record and review employee communications and activities on the job, including phone calls, email, and Web surfing. Some are even videotaping employees on the job. In addition, some companies employ random drug testing and psychological testing. With few exceptions, these increasingly common (and many would say intrusive) practices are perfectly legal.

The Fourth Amendment to the Constitution protects citizens from unreasonable government searches and is often invoked to protect the privacy of government employees. Public-sector workers can appeal directly to the "reasonable expectation of privacy" standard established by the 1967 Supreme Court ruling in *Katz v. United States*.

However, the Fourth Amendment cannot be used to limit how a private employer treats its employees. As a result, public-sector employees have far greater privacy rights than those in private industry. Although private-sector employees can seek legal protection against an invasive employer under various state statutes, the degree of protection varies widely by state. Furthermore, state privacy statutes tend to favor employers over employees. For example, to successfully sue an organization for violation of their privacy rights, employees must prove that they were in a work environment in which they had a reasonable expectation of privacy. As a result, courts typically rule against employees who file privacy claims for being monitored while using company equipment. A private organization can defeat a privacy claim simply by proving that an employee had been given explicit notice that email, Internet use, and files on company computers were not private and that their use might be monitored.

Society is struggling to define the extent to which employers should be able to monitor the work-related activities of employees. On the one hand, employers want to be able to guarantee a work environment that is conducive to all workers, ensure a high level of worker productivity, and limit the costs of defending against privacy-violation lawsuits filed by disgruntled employees. On the other hand, privacy advocates want federal legislation that keeps employers from infringing on the privacy rights of employees. Such legislation would require prior notification to all employees of the existence and location of all electronic monitoring devices. Privacy advocates also want restrictions on the types of information collected and the extent to which an employer may use electronic monitoring. As a result, many privacy bills are being introduced and debated at the state and federal levels. As the laws governing employee privacy and monitoring continue to evolve, business managers must stay informed in order to avoid enforcing outdated usage policies. Organizations with global operations face an even greater challenge because the legislative bodies of other countries also debate these issues.

The U.S. Food and Drug Administration admitted in 2012 that it monitored the private email accounts of nine of its scientists and doctors who had expressed concerns about the FDA process for approving medical devices. Through the use of keystroke monitoring

software, the FDA process captured some 80,000 pages of email including users' email passwords and bank account information. The FDA sends a mixed signal to employees by telling them that their email may be monitored, while at the same time telling them that the use of their government-issued computers for limited personal use is acceptable. Such a message could be interpreted as setting a reasonable expectation of privacy.[63] The impacted employees filed a lawsuit claiming that FDA officials violated their privacy and constitutional rights by monitoring their private email communications. Some investigators believe that the FDA used the emails to build a case to retaliate against the employees.[64]

Advanced Surveillance Technology

A number of advances in information technology—such as surveillance cameras and satellite-based systems that can pinpoint a person's physical location—provide amazing new data-gathering capabilities. However, these advances can also diminish individual privacy and complicate the issue of how much information should be captured about people's private lives.

Advocates of advanced surveillance technology argue that people have no legitimate expectation of privacy in a public place and thus Fourth Amendment privacy rights do not apply. Critics raise concerns about the use of surveillance to secretly store images of people, creating a new potential for abuse, such as intimidation of political dissenters or blackmail of people caught with the "wrong" person or in the "wrong" place. Critics also raise the possibility that such technology may not identify people accurately.

Camera Surveillance

Surveillance cameras are used in major cities around the world in an effort to deter crime and terrorist activities. Critics believe that such scrutiny is a violation of civil liberties and are concerned about the cost of the equipment and people required to monitor the video feeds. Surveillance camera supporters offer anecdotal data that suggests the cameras are effective in preventing crime and terrorism. They can provide examples in which cameras helped solve crimes by corroborating the testimony of witnesses and helping to trace suspects.

There are 4.2 million closed circuit TV cameras (CCTV) in operation throughout Great Britain—which amounts to 1 CCTV camera for every 14 people. China, by way of comparison, has 2.75 million cameras, or 1 camera for every 472,000 citizens.[65] The number of cameras in London was greatly expanded during the 2012 Olympics, and a system called DYVINE enables all London CCTV cameras to be monitored and controlled from the New Scotland Yard.[66]

Washington, D.C.'s Homeland Security and Emergency Management Agency (HSEMA) receives video feeds from more than 4,500 surveillance cameras embedded in and around its schools and public transportation system hubs. HSEMA is evaluating the addition of thousands of more video feeds from private businesses such as banks, corner stores, and gas stations around the city. According to an HSEMA spokesperson, the cameras are designed to raise "situational awareness" during "developing significant events."[67]

The Chicago Transit Authority (CTA) has installed 17,000 cameras in an attempt to reduce crime on their system. According to the CTA, during the first ten months of 2012,

the cameras aided in the arrest of 135 criminals and helped reduce the overall crime rate on the CTA system by 23 percent.[68]

The Domain Awareness system is a joint effort of the New York Police Department and Microsoft to combat terrorist activities and reduce the time required to respond to an incident. The system links together the city's 3,000 surveillance cameras and 2,600 radiation detectors as well as license plate readers and NYPD computer records, including 911 calls. The $40 million dollar system is sensitive enough to tell if a radiation detector was set off by actual radiation, a weapon, or a harmless medical isotope. It can also find where a suspect's car is located and track where it has been for the past few weeks. If a suspicious package is left somewhere, police will be able to look back in time and see who left it there.[69] At a press conference announcing the system, New York City Mayor Michael Bloomberg dismissed concerns that the system would enable police to achieve "Big Brother" capabilities stating, "What you're seeing is what the private sector has used for a long time. If you walk around with a cell phone, the cell phone company knows where you are… We're not your mom and pop's police department anymore."[70]

Vehicle Event Data Recorders

A **vehicle event data recorder (EDR)** is a device that records vehicle and occupant data for a few seconds before, during, and after any vehicle crash that is severe enough to deploy the vehicle's air bags. Sensors located around the vehicle capture and record information about vehicle speed and acceleration; seat belt usage; air bag deployment; activation of any automatic collision notification system, and driver inputs such as brake, accelerator, and turn signal usage.[71] The EDR cannot capture any data that could identify the driver of the vehicle. Nor can it tell if the driver was operating the vehicle under the influence of drugs or alcohol.

The U.S. government does not require EDRs in passenger vehicles. Vehicle manufacturers voluntarily elect to install EDRs, and the capabilities of EDRs vary from manufacturer to manufacturer. If fact, most vehicle owners don't know whether or not their vehicle has an EDR. Beginning with model year 2011 vehicles, the National Highway Traffic Safety Administration (NHTSA) defined a minimum set of 15 data elements that must be captured for manufacturers who voluntarily install EDRs on their vehicles. This data can be downloaded from the EDR and be used for analysis.

One purpose of the EDR is to capture and record data that can be used by the manufacturer to make future changes to improve vehicle performance in the event of a crash. Another purpose is for use in a court of law to determine what happened during a vehicle accident.

State laws dictate who owns the EDR data, and these provisions vary from state to state. NHTSA must ask permission from the owner of a vehicle before downloading any data for government analysis. Courts can subpoena EDR data for use in court proceedings. There have been numerous cases in which EDR data has been ruled as admissible and reliable in court hearings, and there are cases in which such data has had a significant impact on the findings of the court.[72] For example, in *Howard v. Miami Twp, Fire Div*, 171 Ohio App.3d 184, 2007-Ohio-1508, an accident reconstruction expert was able to use EDR data to determine that the driver was exceeding the speed limit at the time of a fatal accident.[73]

The fact that most cars now come equipped with an EDR and that the data from this device may be used as evidence in a court of law is not broadly known by the public. The future capabilities of EDRs and the extent of use of their data in court proceedings remains to be seen.

Stalking Apps

Technology has made it easy for a person to track the whereabouts of someone else at all times, without ever having to follow the person. Cell phone spy software called a **stalking app** can be loaded onto someone's cell phone or smartphone within minutes, making it possible for the user to perform location tracking, record calls, view every text message or picture sent or received, and record the URLs of any Web site visited on the phone. A built-in microphone can be activated remotely to use as a listening device even when the phone is turned off.[74] All information gathered from such apps can be sent to the user's email account to be accessed live or at a later time. Some of the most popular spy software includes Mobile Spy, ePhoneTracker, FlexiSPY, and Mobile Nanny.[75]

There is no law that prohibits a business from making an app whose primary purpose is to help one person track another, and anyone can purchase this software over the Internet. (Some users have complained that they contracted malware when downloading stalker apps or that the app failed to work as advertised.) However, it is illegal to install the software on a phone without the permission of the phone owner. It is also illegal to listen to someone's phone calls without their knowledge and permission. However, these legal technicalities are not a deterrent for a determined stalker.

The Senate Judiciary Committee has approved a bill that would extend the criminal and civil liabilities for the improper use of stalking apps to include the software companies that sell them. Such companies would have to disclose the existence of the stalking app on the phone and gain the phone owner's permission before capturing location information and sharing it with anyone else. The proposed bill includes an exception to the permission requirement for parents who want to place tracking software on the cell phones of minor children without them being aware that it is there.[76]