

PERSONAL PRIVACY ISSUES



Source: C. Slane, 2002. Used with permission.

Introduction

Why Privacy Is Such a Hot Topic Today

Privacy Exposures and Risks

Protecting Children's On-line Privacy

Employer Spying

Changes to Personal Privacy Following September 11, 2001

Summary

INTRODUCTION

Personal privacy is a subject of great, unending debate. On one hand, businesses argue that they have a responsibility to protect their private assets and a fundamental right to promote their products; similarly, governments argue that they have a responsibility to protect public assets and promote the general welfare of citizens. On the other hand, many people feel that it is unacceptable for businesses and governments to accomplish their objectives at the expense of personal freedoms. The constant challenge is to find the proper balance between freedom, safety, and the public good.

Robert Ellis Smith provides a good working definition of privacy in his book of the same name:

Privacy is the right to control your own living space, as in the right to be free from unreasonable searches and seizures. Privacy is the right to control your own identity, as in the right to be known by a name of your own choice and not a number, the right to choose your own hair and dress styles, the right to personality. Privacy is the right to control information about yourself, as in the right to prevent disclosure of private facts or the right to know which information is kept on you and how it is used.¹

Clearly, a key element of privacy is the ability of each individual to control his or her own information, identity, and property. Although society could not function if each person demanded complete personal privacy, we all want to feel we have control over the amount and types of personal information others know about us. Individuals need privacy in which to think, create, and grow. Similarly, organizations need to maintain a degree of privacy to protect trade secrets, research results, and other proprietary information necessary to develop a competitive edge in the business world.

But there is no such thing as complete personal freedom. We are all subject to laws and rules. Each day when driving to work we must drive in the proper lanes, in the proper direction, and within the posted speed limits—or we must face the consequences. Likewise, complete personal privacy is generally not possible or even desirable for most people. For example, we like it when the host at our favorite restaurant remembers our name or culinary preferences. Yet even as children we learn to respect other people's privacy by knocking on closed doors before entering or not opening someone else's mail.

The quest for privacy must not come at the expense of what can be described as “the right to know.” Businesses have a right to know what their employees are doing on the job, governments have a right to know that public assets are being used for their intended purposes, and marketers have a right to identify customers who may be interested in buying their products. The goal is not to isolate oneself from society in order to maintain complete personal privacy, it is to live within society while still maintaining control over who sees your personal information. But there are new threats to personal privacy every day, as well as new tools to protect that privacy. The purpose of this chapter is to identify some of today's threats to personal privacy and to present some suggestions that individuals and businesses can use to protect their privacy and assets.

WHY PRIVACY IS SUCH A HOT TOPIC TODAY

The privacy debate is the subject of countless books and articles, Web pages, newsletters, and reports. Personal privacy has become a major concern because of the ease with which information is now obtained, stored, and shared through computers, specifically through the Internet. Web sites, for example, collect information that individuals freely provide, such as names, addresses, credit card numbers, phone numbers, and Social Security numbers. However, technologies are also available that allow information to be collected about the Web sites a person visits, or their buying patterns and preferences.

In addition to increased reliance on computers and the Internet, new developments in medical research and care, telecommunications, transportation systems, and financial transfers have also increased the level of information generated about each individual. New technologies in biometrics (e.g., face recognition) developed by the defense industry are spreading into law enforcement, civilian agencies, and private companies.²

Americans received a lesson into the extent that our buying patterns are monitored when, during the Monica Lewinsky/President Clinton investigation, Kenneth Starr subpoenaed a Washington bookstore to provide receipts for all of the books Lewinsky had purchased for the past three years. We all learned a lesson about the limits of privacy when prosecutors obtained from Lewinsky's personal computer drafts of letters she wrote but never sent.

One of the major threats to personal privacy is that people do not know the type, scope, and volume of information that is being collected about them. In the past, Americans took privacy for granted and voluntarily gave some of it up to make their lives easier. One good example of this is the switch from paying by cash to credit or debit card. People showed they were eager to provide their name and account number to strangers in exchange for the convenience of carrying less cash and the ability to buy goods and services on demand. Similarly, we readily provide vast amounts of personal information about our earnings, bank account balances, and personal history to banks and finance companies in exchange for the credit needed to purchase cars and homes. The increasing use of on-line credit card purchases shows that many people remain willing to exchange personal information for greater convenience in satisfying their needs and desires.

A major reason personal privacy is at risk more today than ever before is that paper records have been mostly replaced by computerized records. The vast amounts of information stored on computers can be easily shared throughout the world at the click of a button. Technological advances have also changed the way people work, play, communicate, interact, buy goods and services, and conduct their everyday lives. We in America live closer to our neighbors than ever before in both a literal and figurative sense. The migration to cities has reduced the physical space between us and the computer age has closed the gap even further. The types of data routinely collected on individuals by various means include:

- Your credit history
- Your health history
- Your educational history
- Your employment history
- How much you earn
- What you eat
- What you do in your spare time
- What magazines and books you read
- What calls you make
- What you buy (credit card and check)
- What Web sites you use
- Your sexual preference

When we visit Web sites, we leave electronic footprints that can be retrieved at any point in the future to disclose our preferences, desires, and thoughts. But it is not only our current activities that are being watched. The Web sites we visit or e-mail messages we write today add to our growing historical profile—a profile of personal information that is becoming increasingly more public each day. Employers and law enforcement officials have the ability to retrieve even deleted electronic mail messages. Thus, computers and related technology provide threats to personal privacy through the monitoring or observation of our current activities and through the retrieval of historical records.

Although this chapter will focus extensively on the unauthorized acquisition or misuse of personal information through computers, this is only one type of threat to personal privacy, albeit a major one. Other concerns include:

- Surveillance
- Eavesdropping
- Wiretapping
- Office searches
- Alcohol and drug testing
- Ethnic and racial profiling
- Biometrics
- Unsolicited e-mails (spam), phone calls (telemarketers), or mail

For discussion purposes, it is possible to divide all threats to personal privacy into the following separate but related concepts:³

- *Information privacy, or data protection*, is related to the collection and handling of personal data such as credit information or medical records.
- *Bodily privacy* relates to protections against invasive procedures such as genetic tests, drug tests, and cavity searches.
- *Privacy of communications* is related to the security and privacy of mail, telephones, e-mail, and other forms of communication.
- *Territorial privacy* is related to intrusions into personal domains or environments through searches, video surveillance, and ID checks.

The following sections of this chapter will explore specific threats within these categories in greater detail.

PRIVACY EXPOSURES AND RISKS

Biometrics

Biometrics is the collecting, processing, and storing of a person's physical characteristics for the purpose of identification and authentication. The most popular forms of biometric ID are retina scans, hand geometry, thumb scans, fingerprints, voice recognition, and digitized (electronically stored) photographs.⁴ In an effort to increase security following the World Trade Center and Pentagon attacks on September 11, 2001, there has been an increased interest in using biometric technology to check identities at many public places such as airports and shopping malls. The goal is to be able to immediately check a person's identity by accessing a vast database of digital personal images. One possible scenario would be to require everyone to carry cards containing their fingerprint information as a means of identification (see National ID Cards). A more ominous scenario involves video surveillance cameras in virtually every public building and on every street corner so that every person can be monitored.

One of the most controversial forms of biometrics—DNA identification—is benefiting from new scanning technology that can automatically match DNA samples against a large database in minutes. Police forces in several countries, including the United States, have created national DNA databases. Samples are being routinely taken from larger and larger groups of

people, including people arrested for minor offenses. In addition, there have been proposals to begin collecting DNA samples from all newborn babies.

The privacy concerns with biometrics include how to maintain the security of the image database, whether the personal images will be linked to other personal information stored on-line, and whether it is desirable to have video cameras in all public places. There are also unknown potential legal ramifications stemming from false positive or false negative identifications.

One example of biometrics in use was the face-recognition technology used at the Super Bowl in Tampa. In January 2001, the city of Tampa used the technology to scan the faces of people in crowds at the Super Bowl, comparing them with images in a database of digital mug shots. Tampa also installed cameras equipped with face-recognition technology in their Ybor City nightlife district. The technology failed to identify any criminals and produced several false matches. However, Tampa police said that the publicity probably deterred criminals and that they intended to resume the experiment with improved software. But critics like Barry Steinhardt, president of the American Civil Liberties Union, want the monitoring to stop because facial-recognition technology is prone to error and abuse of privacy.⁵

Joseph J. Atick, the chairman and chief executive of Visionics, a biometric technology supplier, said he is also concerned about the privacy issues raised by biometrics. He supports greater federal regulation and certification of biometric systems, as well as stringent privacy guidelines that could include a ban on keeping any photographic image that does not match data on a suspect. "No match, no memory, is crucial," he said. "This technology has broad potential to affect our lives and I have a responsibility to ensure it is not misused."⁶

Biometric technology has also been used in Virginia Beach, Virginia. The Virginia Department of Criminal Justice Services gave a \$150,000 grant to the city in July 2001 to help it obtain face-recognition cameras to look for criminal suspects and missing children. Although officials had initially expressed mixed feelings about the technology, the city council voted to install the software at the oceanfront. To fully fund the system, the city will have to pay an additional \$50,000.⁷

Citizens can expect increased use of biometric technology in airports following the terrorist attacks on New York and Washington on September 11, 2001. Privacy advocates, citizen groups, political leaders, and manufacturers of the technology itself are debating whether these technologies should be permitted in certain locations, such as airports, and if so, how they should be regulated to protect the privacy of the public. Airlines are looking into biometrics technologies that would allow passengers to volunteer for traveler IDs that could speed the screening process. Also, officials at Logan Airport in Boston and T.F. Green airport in Providence, Rhode Island, have announced that they will be installing face-recognition technology.⁸

The American Civil Liberties Union (ACLU) has opposed the use of face-recognition software to check the identity of airline passengers due to ineffectiveness and privacy concerns. The ACLU noted that the face-recognition technology called "Ferret" by the Department of Defense was abandoned by some government agencies after finding it did not work as advertised. The Immigration and Naturalization Service, for example, had experimented with using face-recognition technology to identify people in cars at the Mexico–United States border. The ACLU warns that face-recognition software is easily confused by changes in hairstyle or facial hair, by aging, weight gain or loss, and by simple disguises. It notes a Department of Defense study that found very high error rates even under ideal conditions where the subject was staring directly into the camera under bright lights. The study found very high rates of both "false positives" (wrongly matching people with photos of others) and "false negatives" (not catching

people in the database). The ACLU concluded that if installed in airports, face-recognition systems would miss a high proportion of suspects included in the photo database and flag huge numbers of innocent people, thereby lessening vigilance, wasting precious manpower resources, and creating a false sense of security.⁹

Communications Monitoring

It is relatively easy for people to eavesdrop or intercept messages between various types of communications devices such as cordless phones, cellular phones, and pagers. For example, because analog cordless phones use radio signals, eavesdroppers can use radio scanners or another cordless phone to listen in on calls. Thus, people should avoid discussing sensitive information or making credit card purchases using their cordless phone. All such information should be shared using wired telephones on both ends of the conversation. However, the advent of digital cordless phones that use frequencies not picked up by scanners may increase the privacy offered by these devices.

The federal government has broad powers to use wiretaps of telephones, pagers, wireless phones, computers and all other electronic communications and communications devices. The two sources of authority for wiretapping in the United States are:¹⁰

1. *The Federal Wiretap Act of 1968*. Wiretaps subject to this Act require a court order indicating that there is probable cause to believe that a crime has been, is being, or is about to be committed.
2. *The Foreign Intelligence Surveillance Act of 1978*. Wiretapping of aliens and citizens is allowed if there is probable cause to believe that the target is a member of a foreign terrorist group or an agent of a foreign power. For U.S. citizens and permanent resident aliens, there must also be probable cause to believe that the person is engaged in activities that “may” involve a criminal violation. Suspicion of illegal activity is not required in the case of aliens who are not permanent residents.

Both Acts allow the government to carry out wiretaps without a court order in emergency situations involving risk of death or serious bodily injury and in national security cases. More information on this type of privacy invasion can be obtained from the Cellular Telecommunications Industry Association, 1250 Connecticut Avenue, N.W., Ste. 200, Washington, D.C. 20036, (202) 785-0081.

Unwanted or Threatening Phone Calls

While unwanted calls are a routine problem for nearly everyone, threatening calls can be a major threat to privacy and security. Phone companies will generally assist customers in tracking and stopping threatening calls. Therefore, as a general rule, recipients of these calls should contact their local telephone service provider before contacting the police. However, the phone company may have trouble identifying the caller if that person uses pay phones or multiple phone numbers.

Telemarketers are a major source of unwanted calls. Everyone has probably had the experience of answering the phone and no one is on the line. This is probably a telemarketing service that uses automatic dialing machines. The machines dial many phone numbers simultaneously,

wait for a person to answer, and then transfer the call to an operator. If all of the operators are busy, the recipient of the call hears silence.

The National Fraud Information Center offers these tips to consumers who wish to avoid being harassed or defrauded by telemarketers:¹¹

- Do business with known and trusted companies. Ask the caller to send information about the product or service offered. Honest companies will be glad to do this.
- Understand all aspects of the transaction before accepting an offer. Know the company, its address and phone number, the product or service, its price, the delivery date, the return and cancellation policy, and the terms of any guarantee. Obtain this information in writing.
- Check out the company's complaint record at a consumer protection agency or the Better Business Bureau.
- Only share financial or other personal information such as bank account numbers, credit card numbers, or Social Security numbers with trusted companies that have a legitimate need to know.
- Do not succumb to high-pressure tactics.
- Request to be removed from the call lists of harassing salespeople. Keep a list next to the phone with the company names and dates. If you are called again on behalf of those companies, report it to your state attorney general and the Federal Trade Commission.
- To avoid unwanted phone calls from many national marketers, send your name, address, and telephone number to:

DMA Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735-9014

OR

Preference Service Manager
Direct Marketing Association
1120 Avenue of the Americas
New York, NY 10036-6700
Send via fax to: (212) 790-1427

DMA member companies that participate in this industry-sponsored program will put you on their "do not call" lists. If you are repeatedly called by fraudulent telemarketers, you may want to consider changing your phone number. For more information, visit www.the-dma.org.

- Don't be shy about hanging up. Your phone is just like the door to your home or apartment. You don't have to open it or invite people in, and you can ask guests to leave at any time. Fraudulent telemarketers are very good at lying to, bullying, or sweet-talking their intended victims. The longer you stay on the line, the deeper they sink their hooks. Don't let a criminal in your home through your telephone line!
- If you need advice about a telephone solicitation or you want to report a possible scam, call the NFIC hotline at 1-800-876-7060.

Here are some things people can do to reduce the number of unwanted or threatening phone calls they receive:

- Change your phone number and request that it be unlisted and unpublished if you are receiving threatening calls.

- Get an answering machine so you can screen your calls.
- Use the Caller ID features available from some companies to help identify the name of the person making the call and phone number from which the call was placed. Although there are ways for callers to override this function, recipients of calls can elect to pick up only calls from numbers they recognize.

Surveillance

The two primary means of surveillance are video surveillance and satellite surveillance. These methods are commonly used to monitor a variety of public and private spaces. Video surveillance, or Closed Circuit Television (CCTV), uses small cameras to view people at areas such as office buildings, shopping malls, parking lots, roads, and sports stadiums. Private homeowners also use video surveillance to protect their property from intruders. The visual quality of video surveillance pictures has improved dramatically in recent years and some systems now include such technical features as infrared capabilities for night viewing. Video systems linked to computer databases have the ability to immediately identify individuals in a crowd. There is a concern that video surveillance technology could be used to subject specific groups of people (e.g., minority youths) to more intense scrutiny than others.

Satellite surveillance can be used to view small details anywhere on the face of the earth. The technology can be used to enhance capabilities during war efforts or to view the aftermath of a natural disaster. The risk to privacy is that the technology will be used as a surveillance tool to monitor individual's homes.

Retail stores use surveillance not only to watch for shoplifters, but also to analyze patterns of customer movement throughout the store. The purpose is to determine the effectiveness of marketing and customer service. For example, Brickstream Corporation has developed a system that uses ceiling cameras to record and analyze customer movements throughout the store. Any store using the system might be able to determine how long customers will wait in a non-moving checkout line or how many customers stop to look at a particular advertising display. Brickstream executives state that the system reports numeric data and does not personally identify particular shoppers.¹² However, the idea of even more video surveillance in retail shops worries some privacy experts.

ID Chips

Tiny computer chips have been developed that can be implanted into living beings to track their movement. The chips, which have already been implanted into many house pets to track their movement, transmit personal information that can be read by a handheld reader. One day the technology may be used to keep track of people. For example, corrections authorities are interested in using the chips to identify prisoners and parolees, primarily because it is a tamper-proof form of identification. Workers in high-security jobs, like nuclear power plants or airports, might also use the chips. Elderly or disabled people who cannot communicate their name or other personal information might also be candidates for the device. However, the device must still be tested and approved by the Food and Drug Administration. Meanwhile, privacy experts are concerned that the chips could be implanted against someone's wishes. Also, there is a con-

cern that information contained on the chip would be difficult to update if necessary. Meanwhile, the use of chip technology is growing as automobile manufacturers use chips in keys to deter auto theft and libraries use chips to track books.¹³

Unsolicited Mail

Many companies use direct mail advertising campaigns to market the goods or services they are selling. The volume and frequency of the mailings has become a nuisance to many people. The mailing lists companies use contain the names of people who have done business with the company or with companies in the same industry, or people who have expressed an interest in the type of product or service the company sells. A growing number of consumers are electing to “opt out” by asking companies to remove their name from mailing lists and to not sell their name and other personal information to other marketers.

Opt-out agreements may either be permanent or for a limited period. The Web site Consumer-PrivacyGuide.org lists several ways consumers can communicate their preference to opt out of direct mail lists:¹⁴

- Contact your bank, grocery store, utilities, and phone company directly and ask that they do not distribute your personal information.
- Write or call the magazines that you subscribe to and ask them not to release your mailing information when they make their subscription list available.
- Direct marketers are required under the rules of the Direct Marketing Association to provide an opportunity to opt out. Even if the site does not offer the option to opt out when placing orders on-line or on the phone, ask that your information not be shared.
- Contact Operation Opt-Out (www.opt-out.cdt.org), which provides you with links to companies that provide you with an opportunity to opt out on-line. Operation Opt Out also enables you to generate and mail letters to companies that do not allow you to opt out on-line.

The Direct Marketing Association’s (DMA) Mail and E-mail Preference Services allow consumers to opt out of direct mail marketing and e-mail marketing solicitations from many national companies. Because your name will not be on their lists, it also means that these companies can’t rent or sell your name to other companies. To remove your name from many national direct mail lists, write:

Direct Marketing Association
P.O. Box 9008
Farmingdale, NY 11735-9014

OR

Preference Service Manager
Direct Marketing Association
1120 Avenue of the Americas
New York, NY 10036-6700
Send via fax to: (212) 790-1427

Consumers can also remove their e-mail addresses from many national direct e-mail lists by visiting www.e-mps.org. Consumers can opt out of receiving pre-screened credit card offers by

calling 1-888-5-OPTOUT (1-888-567-8688). The three major credit bureaus use the same toll-free number to let consumers choose not to receive pre-screened credit offers.

The National Consumers League offers these tips to consumers who want to remove their name from marketing lists:¹⁵

- Don't provide information that isn't necessary for the transaction. Don't just fill in the blanks without thinking about whether you want to limit the information you supply.
- Be anonymous. Consider using on-line tools and fictitious names in situations where your real identity isn't needed and there is no other option to avoid getting on marketing lists.
- Think twice before entering contests. Entry forms are often used to build marketing lists.
- Know the privacy policy. If you don't see anything about what personal information companies collect and how they use it, ask.
- Understand your privacy choices. If there is no privacy policy or it doesn't allow you to avoid unwanted marketing, take your business elsewhere.
- Know when your personal information is being collected. Be aware of Automatic Number Identification and other ways that your information may be collected and tell the company if you don't want to be put on a marketing list. Ask your phone company how to block your number if you don't want it to show.
- Understand that unlisted and unpublished phone numbers don't guarantee privacy. Marketers may get your number if you've given it to others or they may simply dial you randomly.
- Know your telemarketing rights. Federal law allows you to tell marketers not to call you again. Check with your state attorney general's office to find out if you also have "Do Not Call" rights under state law.
- Know your financial privacy rights. Federal law requires financial institutions to tell you what information they collect and how they use it, and allows you to request that your personal information not be shared with unrelated companies. Check with your state attorney general's office to find out if you also have financial privacy rights under state law.
- Know your medical privacy rights. Federal regulations limit how your health information can be used and shared with others for marketing purposes. Check with your state attorney general's office to find out if you also have medical privacy rights under state law.
- Your state may protect you against spam, or unsolicited e-mails. Check with your state attorney general's office.

Other valuable resources include Junkbusters, Mailshell, and Spamex. Junkbusters (www.junkbusters.com) provides information on reducing the volume of junk e-mail and telemarketing calls. Mailshell (www.mailshell.com) uses filtering technology to prevent junk e-mail from reaching a user's computer. Spamex (www.spamex.com) provides users with disposable e-mail addresses that allow them to identify and stop unwanted e-mail.

Credit Card Fraud

Many purchases and financial transactions are made with credit cards instead of cash. In exchange for the convenience and security of not carrying large sums of cash, consumers must realize that cards and card numbers can be easily stolen. Card issuers are placing photos of the card holders on the card to reduce the potential misuse of the card. However, credit and debit

card fraud is still quite common. The American Association of Retired Persons (AARP) provides a list of tips for protecting against the theft or misuse of credit cards:¹⁶

- Don't carry more cards than you plan to use.
- Immediately report lost or stolen cards to the credit card company. If you report the theft early, you won't have to pay the thief's credit card bills. In addition, the credit card company can stop the thief by canceling your credit card number.
- Don't write your PIN (personal identification number) on your credit card. This will prevent the thief from using your PIN to "borrow" large amounts of cash with your card.
- Keep your credit card number to yourself. Thieves don't need your credit card to charge merchandise to your account. They only need your credit card number. Criminals use stolen credit card numbers to make purchases over the phone or through the mail. Sophisticated lawbreakers can even make a new credit card with your name and number on it.

Here are some ways to protect your credit card number:

- When checking out at store registers, shield your credit card from the people around you. Someone might be looking over your shoulder to copy your number.
- Keep track of your credit card receipts. These receipts can reveal your credit card number to anyone who finds them.
- Don't give your credit card number to a telemarketer unless you are sure he or she represents a reputable company or you placed the call. Con artists could pretend to sell you something just to get your credit card number.
- Check your monthly billing statement to see if it includes purchases or transactions you did not make. Report these to the credit card company right away.
- Make sure your transactions are accurate. Be on guard for dishonest merchants who might change your credit card slip after you sign it.
- Always total your charge slip before signing the credit card receipt. Don't leave blank spaces where additional amounts could be added.
- Never sign a blank charge slip.
- Always check your receipts against your billing statement. If you think a charge amount was changed, call your credit card company immediately.

Debit Card Fraud

Debit cards work like a personal check. The card is run through a scanner and the amount of purchase is automatically deducted from the purchaser's checking or savings account. The limit on spending equals the amount in the account.

The AARP offers several tips for safely using a debit card:¹⁷

- Guard the card against loss or misuse because a thief can clear out a bank account before the owner even knows the card is missing.
- If your card is lost or stolen, or if you think it is being used fraudulently, call your bank immediately. Follow up the phone call with a letter. If you fail to notify your bank within 60 days after you receive your bank statement, your liability is unlimited so you could lose all the money in your account. Check your bank statements carefully and promptly for unauthorized charges. There are major debit card issuers that provide more protection and some state laws cap your total loss at \$50.00.

- For all debit card transactions, hold on to your receipts. A thief can get your name and debit card number from a receipt and order goods by mail or over the telephone. The items could be paid for out of your bank account before you know about it.
- Memorize your PIN and don't keep it with your card. Don't choose one that a smart thief could figure out, like your phone number, address, or birthday. Never give your PIN to anyone.

National Identity (ID) Cards

Many countries use cards as a means of identification. In the United States, national ID cards have been generally opposed. However, advocates believe the use of national ID cards can enhance national security and help identify illegal aliens.

Technology is available that would allow legal U.S. residents to carry a card containing a computer chip that could hold a considerable amount of personal information, such as fingerprint images. Many countries use national ID cards and the information on them includes holder's name, identifying number, photograph, date and place of birth, gender, parent's name, place and date the card was issued, expiration date, holder's signature, height, color of eyes, marital status, and profession. Much of the information is contained in bar codes that are machine readable.¹⁸

In January 2002, state motor vehicle officials asked Congress for up to \$100 million to create a national ID system that would include high-tech driver's licenses and a network of tightly linked databases of driver information. In the wake of September 11, driver's license association officials suggested adopting cards containing biometric information such as fingerprints embedded on computer chips to improve security. In their view, the driver's licenses had already become the de facto national identification card. The proposal calls for standardized licensing procedures and improved methods to authenticate drivers to help prevent terrorists and con artists from obtaining and using false driver's licenses as identification. Civil libertarians argue that such a system would allow for unchecked government scrutiny.¹⁹

The military is already using this technology with more than 120,000 active duty military personnel, selected reservists, and Defense Department civilians using the cards as of December 2001. The military plans to issue more than 4 million high-tech identity cards in the next two years.²⁰ The cards the military uses have two photos, two bar codes, a magnetic strip, and an identity chip. The cards have the potential to hold an individual's complete medical history. However, because the cards are "smart cards" (discussed later), they can be used to monitor where a person is physically located at any time.

The attacks on September 11, 2001, escalated a debate about whether national ID cards could help in the war against terrorism by linking the cards to a worldwide database. Governments and law enforcement officials could theoretically access the database records to immediately verify the identity of any person in the world. Critics argue that the "smart card" location tracking technology would erode people's sense of privacy and encourage harassment by law enforcement officials.

Although a national ID card has not been implemented in the United States, the technology used to create the cards has found similar uses. As stated earlier, the American Association of Motor Vehicle Administrators is devising a plan to create a national identification system to connect all state driver databases to driver's licenses embedded with computer chips, bar codes, and biometric

identifiers. Also, the Air Transport Association wants travelers to carry a travel card that would include a biometric identifier that could be linked to criminal, intelligence, and financial databases.²¹

One advantage of a national ID system would be that a person's identification could be immediately identified, which would make for more convenience and shorter lines at places like airport terminals. However, the risk is that the information on the cards and vast storehouses of personalized data on each individual that the cards are linked to could be misused. A Privacy International survey of ID cards found that police throughout the world arbitrarily detained individuals who failed to produce their card. The survey also found that minorities and juveniles were often targets of abuse or discrimination based on data the cards contained.²²

Although serious questions remain unanswered about how the cards and related databases would be used, updated, and controlled, perhaps an even more serious concern is the potential damage to a person's life if their card is lost or stolen. The results could range from something as simple as denial of service to a complete loss of identity.²³

The last time Congress addressed similar questions was in 1996 when it voted not to amend the Illegal Immigration Act of 1996. The Act would have required states to list Social Security numbers on all driver's licenses. However, the debate on a national identifier continues, especially after the attacks that occurred on September 11, 2001. For example, Senator Lamar Smith (R—Texas) said he would like to explore requiring Social Security cards and certain immigration documents to have biometric identifiers, such as fingerprints.²⁴

ID Theft

As of the end of December 2000, the Federal Trade Commission (FTC) had processed over 40,000 entries from consumers and victims of identity theft. Of the entries collected during 2000, 69 percent were victims' complaints, reporting incidents in which one or more types of identity theft occurred. Thirty-one percent were requests for information from consumers that are concerned about becoming victims of identity theft. In 2001, the FTC processed 117,210 reports (a 34 percent increase in reported cases): 86,168 (74 percent) from victims of identity theft, and 31,042 (26 percent) from other consumers concerned about identity theft, making identity theft/fraud today's fastest growing white-collar crime.

Identity theft was the leading consumer fraud complaint reported in 2001. The Federal Trade Commission's identity theft hot line receives about 1,700 calls each week. About 42 percent of the 204,000 total complaints received by the FTC in 2001 involved identity theft. Identity theft occurs when a person's identity information (e.g., credit card number or Social Security number) is used by another person to steal the victim's money or to commit some other type of fraud. There may be as many as 750,000 identity thefts each year.²⁵ The AARP reports that losses to consumers and institutions due to identity theft totaled \$745 million in 1997, according to the U.S. Secret Service.²⁶

In November 2002, federal investigators uncovered a massive identity theft and identity fraud scheme that is thought to have spanned nearly three years and involved more than 30,000 victims. Early in the investigation it was estimated that losses to individuals, identity theft victims, could reach as high as \$2.7 million. Three individuals were arrested and charged with wire fraud and related wire fraud charges, as well as stealing financial information on thousands of Americans (and possibly foreign nationals).

The mole in this identity fraud/theft scam was a company insider. The insider had worked as a help-desk professional with Teledata Communications Inc., a New York–based company that provides financial institutions and other companies with individualized customer credit reports. The credit reports, which Teledata sells to client companies, are compiled using data provided by the leading credit rating organizations (i.e., Equifax, TransUnion, and Experian). Ultimately, when all the dust settles, this could turn out to be one of the largest cases of identity fraud/theft ever uncovered.

The Federal Trade Commission has identified the following ways thieves can steal a person's identity:²⁷

- Open a new credit card account using another person's name, date of birth, and Social Security number; use the credit card up to its limit; and not pay the bill.
- Change the mailing address on another person's credit card account and use the card in that person's name.
- Establish cellular phone service in another person's name.
- Open a bank account in another person's name and write bad checks on the bogus account.
- File for bankruptcy under another person's name to avoid paying debts incurred in the course of stealing their identity.
- Counterfeit checks or debit cards containing another person's bank account number.
- Take out auto loans in another person's name to buy cars for themselves.

Thieves obtain personal identifying information by finding or stealing consumers' credit card receipts, purse, or wallet. Sometimes the thieves take this information directly from the victim's mailbox or garbage cans. Other thieves simply forge or create fake information and documents such as Social Security cards or driver's licenses. Also, many people still put their Social Security number on their checks, which makes the information easy for others to obtain. Increasingly, high-tech thieves are hacking into corporate databases in attempts to obtain large volumes of credit card numbers and other identifying information. Although credit card companies usually have limits on the amount of money a customer can lose through identity theft, it often takes victims a considerable amount of time and effort to regain control of their lives.²⁸

The Social Security number has to some extent become a national identifier. Although Social Security numbers were originally issued for the Social Security Administration to use for employment and tax purposes, some other federal agencies currently mandated to use the number include the Civil Service Commission, Internal Revenue Service, Department of Defense, food stamp program, Department of Justice, Department of Energy, Department of Treasury, Department of State, Department of Interior, Department of Labor, and the Department of Veterans Affairs. All federal agencies use the number as an identifier for record-keeping purposes. State agencies also use the number for welfare, health, and revenue purposes. Third parties, such as banks and universities, regularly request the number to verify the purchaser of products or services.²⁹ Because the number is so widely used as a unique identifying number, the privacy of the number is no longer guaranteed. Also, Social Security cards are easy to forge because they contain no photo or other unique information. Criminals can almost literally adopt the identity of another person by obtaining his/her Social Security number.

A great deal of basic personal information is becoming public information. For example, a Web site called anybirthday.com claims to contain the birthdates of 135 million people. The site can also provide gender and zip code information. Searches are free of charge. Like so many Internet companies, anybirthday.com makes money by selling advertising space on its Web site. Anyone who wishes not to be listed on the database can "opt out."³⁰

Although the Federal Trade Commission acknowledges that identity theft cannot be prevented, it provides the following suggestions for minimizing the risk of becoming a victim:³¹

- Before revealing any personally identifiable information, find out how it will be used and whether it will be shared with others. Ask if you can choose to not submit the confidential information requested.
- Pay attention to billing cycles and contact creditors if bills don't arrive on time. Identity thieves often change the billing address on a victim's credit card in an attempt to avoid detection.
- Guard your mail from theft by depositing outgoing mail in post office collection boxes and by promptly removing mail from mailboxes after it has been delivered. Put a vacation hold on mail deliveries when on vacation and away from home.
- Passwords protect credit cards, bank accounts, and phone accounts. Avoid using passwords that are easily guessed such as mother's maiden name, birth date, last four digits of phone number or Social Security number, or any series of consecutive numbers.
- Carry only the identification and credit cards that are actually needed.
- Do not give out personal information on the phone, through the mail, or over the Internet unless you have initiated the contact or know whom you are dealing with. Identity thieves often misrepresent themselves over the phone to obtain personal information.
- Shred charge receipts, credit card applications, insurance forms, physician statements, bank checks, and other financial statements that are being discarded. Cut up all expired credit cards and driver's licenses before discarding.
- Store confidential personal information in a safe place.
- Find out who controls personal information at work and ensure that the records are kept in a secure location.
- Give your Social Security number only when absolutely necessary. Ask to use other types of identifiers when possible.
- Don't carry your Social Security card or birth certificate. Keep them in a safe place.
- Review your credit report every year and make sure it is accurate and includes only authorized activities. A credit report contains information on where a person works and lives, credit accounts opened, debt information, arrest data, and any bankruptcy proceedings. The major credit bureaus have Web sites that generally allow consumers to order a copy of their credit report on-line or off, or to learn how to identify and report credit card misuse, how to remove their name from pre-approved credit card offer mailing lists, and how to opt out of other junk mail lists. The major credit bureaus are as follows:
 - Equifax (www.equifax.com). To order a credit report, call 800-685-1111, or write to P.O. Box 740241, Atlanta, GA 30374-0241. To report fraud, call 800-525-6285/ TDD 800-255-0056, or write to P.O. Box 740241, Atlanta, GA 30374-0241.
 - Experian (www.experian.com). To order a report, call 888-EXPERIAN (397-3742), or write to P.O. Box 2104, Allen, TX 75013. To report fraud, call 888-EXPERIAN (397-3742)/ TDD 800-972-0322, or write to P.O. Box 9532, Allen, TX 75013.
 - TransUnion (www.transunion.com). To order a report, call 800-916-8800, or write to P.O. Box 1000, Chester, PA 19022. To report fraud, call 800-680-7289/ TDD 877-553-7803, or write to Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634-6790.

The FTC recommends the following steps to be followed by people who feel their identity has been stolen:³²

1. Contact the fraud departments of each of the three major credit bureaus (listed previously), review your credit report, and request that a “fraud alert” be placed in your file.
2. Contact creditors to determine whether any accounts have been tampered with or opened fraudulently. Immediately close accounts that have been tampered with and open new ones with new, non-identifiable Personal Identification Numbers (PINs) and passwords.
3. File a report with local police or the police in the community where the identity theft took place.

The United States Department of Justice provides additional information on actions that should be taken by victims of identity theft. The list is based in part on information from the California Public Interest Research Group (CalPIRG) and the Privacy Rights Clearinghouse. The following actions should be taken immediately after identity theft is suspected in order to minimize the financial damage the crime can cause:³³

- Contact the Federal Trade Commission (FTC) to report the situation at either www.ftc.gov, 1-877-ID THEFT (877-438-4338) or TDD at 202-326-2502, or at Consumer Response Center, FTC, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.
- Contact the local office of the Postal Inspection Service if you suspect that an identity thief submitted a change-of-address form with the Post Office to redirect your mail or used the mail to commit frauds involving your identity.
- Contact the Social Security Administration if you suspect that your Social Security number was fraudulently used (call 800-269-0271 to report the fraud).
- Contact the Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).
- Call the fraud units of the three major credit bureaus (listed previously).
- Contact all creditors with whom your name or identifying data have been fraudulently used. For example, you may need to contact your long-distance telephone company if your long-distance calling card has been stolen or if you find fraudulent charges on your bill.
- Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name without your knowledge. You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).
- Contact the major check verification companies if you have had checks stolen or bank accounts set up by an identity thief. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses. Some check verification companies include:
 - CheckRite—(800) 766-2748
 - ChexSystems—(800) 428-9623 (closed checking accounts)
 - CrossCheck—(800) 552-1900
 - Equifax—(800) 437-5120
 - National Processing Co. (NPC)—(800) 526-5380
 - SCAN—(800) 262-7771
 - TeleCheck—(800) 710-9898

The FTC’s Web site (www.ftc.gov/privacy/cred-ltr.htm) also contains a sample opt-out letter (see Exhibit 8.1). Consumers can use the form to contact the three national credit reporting

agencies (Equifax, Experian, and TransUnion) to request that their personal credit report information not be shared with third parties. Fraud-related information and assistance are also available through the Internet Fraud Watch (www.fraud.org) and the Call for Action Hotline (www.callforaction.org). Victims should also report any stolen securities to the Securities and Exchange Commission.

Census Information

Some people are concerned that personal information provided to the United States Census Bureau will become public information. However, the Privacy Act of 1974 and Title 13 of the United States Code protect privacy and confidentiality by restricting the use or disclosure of census information received from individuals and businesses. Furthermore, census data is generally published in aggregate or summary form. Only sworn employees of the Census Bureau may have access to individual census information.³⁴

Interactive Television

Technology is quickly obliterating the line between computers and television. New technologies allow interactive devices that act like computers to receive television signals. Also, many personal computers are equipped with television tuner cards. These new systems promise shows on demand and interactive communication with other viewers. However, as more people receive television through communications networks, television viewers will begin to face the same privacy concerns now facing computer users. Viewers can anticipate that their viewing habits will be tracked and their viewing profile will be made available to marketing companies. Advertisers are also interested in using interactive television to track which commercials each customer watches. The next possible step is for cable companies to target specific commercials to specific households or television sets during normal programming.

Medical Privacy

Medical information is regularly shared between third parties such as drug companies, employers, universities, and government health agencies. Patients often do not know their information is being shared. For example, a Washington, D.C., woman sued a surgeon and a national magazine after the magazine ran a photo of her following cosmetic surgery. A risk to privacy in the workplace is that employers will use the increasing amount of medical information at their disposal as a basis for personnel decisions involving hiring and job promotions.³⁵

Consumers Digest provided the following statistics related to medical privacy:³⁶

- According to the AFL/CIO, “employers commonly use information about an individual’s medical condition in [making] decisions about hiring, firing or promotions.”
- Medical information is available from insurers through state workers’ compensation programs and industry databases on insurance claims known as the “Index” system.
- Workers’ compensation claim information is easily bought from employment-screening firms for as little as \$12.

Be sure to send your letter to ALL three credit bureaus.

Options
Equifax, Inc.
P.O. Box 740123
Atlanta, GA 30374-0123

Experian
Consumer Opt-Out
Name Removal Option
701 Experian Parkway
Allen, TX 75013

Trans Union Corporation's
Name Removal Option
P.O. Box 97328
Jackson, MS 39288-7328

Date

To whom it may concern:

I request to have my name removed from your marketing lists. Here is the information you have asked me to include in my request:

FIRST, MIDDLE & LAST NAME

(List all name variations, including Jr., Sr., etc.)

CURRENT MAILING ADDRESS

PREVIOUS MAILING ADDRESS

(Fill in your previous mailing address if you have moved in the last 6 months.)

Note: not required by Equifax and Experian.

SOCIAL SECURITY NUMBER

Note: not required by Experian.

DATE OF BIRTH

Note: not required by Equifax and Experian.

Thank you for your prompt handling of my request.

SIGNATURE

Exhibit 8.1. Credit Bureaus: Sample Opt-Out Letter³⁷

- Employers can pull even more medical information from credit records (health-care billing), bankruptcy records, and even handwriting analysis (some medical and mental states).

Consumers Digest recommends that individuals follow these actions to protect their medical privacy:³⁸

- Ask for a copy of your medical records from your physician, hospital, and other care providers. Correct any misinformation. Ask your doctor how much information is released to third parties, what privacy policies they have in place, and what they do in practice, as opposed to their policies.
- If you are concerned about privacy during a hospital stay, find out who has access to your treatment and records. If your concern is extreme, ask to see “access logs” of computer medical-records systems.
- If possible, restrict the amount of medical information released to employers or insurers. Instead of signing blanket authorizations regarding “any medical provider to release any medical information,” negotiate to restrict the authorization to a specific provider or hospital.
- If you are concerned about your personal information being sold, don’t fill out medical questionnaires accompanying surveys or drug promotions or toll-free information hotlines. Your name may be sold to companies marketing products that apply to your particular maladies.
- It is advisable to obtain a copy of your MIB file to ensure that if any information has been added, it should actually be there and it is accurate and has not been miscoded. MIB (www.mib.com) is an association of U.S. and Canadian life insurance companies. It is a leading provider of information and database management services to the financial services industry. MIB’s core fraud protection services have protected insurers, policyholders, and applicants from those who would attempt to conceal or omit information relevant to the sound and equitable underwriting of life, health, disability, and long-term care insurance.

Member companies send information to MIB when they receive an application for life, health, disability, or long-term care insurance. The applicant receives a written notice that authorizes the insurance company to release the information to MIB.

The type of information in your MIB record may include medical conditions represented by one or more of about 230 codes. Conditions most commonly reported include:

- Height and weight
- Blood pressure
- ECG readings
- Laboratory test results if, and only if, these facts are considered significant to health or longevity

There are also five codes for non-medical information that might affect insurability. Examples of non-medical information significant enough to warrant a report to MIB include:

- An adverse driving record
- Participation in hazardous sports
- Aviation activity

When a consumer applies to an MIB member company for life, health, disability, or long-term care insurance coverage, the company may check for a record at MIB. If there is a record, it is sent in coded form to authorized personnel only at the company making the request. The purpose of the report is to detect and deter applicants from omit-

ting or misrepresenting significant facts. The insurer who receives a record from MIB will compare it with information provided by the applicant. If the information in the MIB record is inconsistent with other information, the insurer may conduct further investigation.

To obtain a copy of your MIB Record (if one exists) follow these steps:

1. Download a Request for Disclosure Form (www.mib.com/html/us_residents.html or www.mib.com/html/canadian_residents.html for Canadian residents).
2. Fill in the Request for Disclosure Form completely.
3. Print the Request for Disclosure Form.
4. Sign and mail the Request for Disclosure Form (along with your check/money order for \$9.00, unless paying by credit card) to:
 - U.S. Residents:
MIB, Inc.
P.O. Box 105
Essex Station
Boston, MA 02112
(617) 426-3660
 - Canadian Residents:
MIB, Inc.
330 University Avenue
Toronto, Ontario M5G 1R7
(416) 597-0590
- Ask your employer if it is self-insured and obtain a copy of all policies relating to medical information. Are medical records stored in personnel files (that's illegal under federal law)? Does your insurer or health-maintenance plan share information with your employer? If so, who sees it and how is it used?
- Do not give out your Social Security number unless you have to. This number can be used to track a great deal of information on you, including workers' compensation records and credit files. Never provide health information over the phone and make sure your health-care providers won't release your medical records without your written authorization.
- Call or write your congressman or congresswoman and tell him/her you want a comprehensive medical privacy law that does not include a universal "health identification number" and that restricts medical information only to health-care providers and insurers.

The Patient Safety Institute (PSI) announced on December 11, 2001, that it is developing a system to electronically link medical databases using the same confidential computer systems now used to facilitate on-line banking. The PSI system will allow doctors, hospitals, and pharmacies to access patient information about a patient's medical history, allergies, medications, and vaccinations at any time and from any location.³⁹

On-line Privacy

On-line companies routinely collect a great deal of personal information about the people who visit their Web sites or buy their products. Internet retailers and other companies regularly create and share profiles of their customers and those who visit their Web site. The profile may actually be of your Internet address rather than of you because it is created based on the Web sites

you visit. However, the problem is becoming more acute as Web addresses are now being linked to actual identities. The threat is that the FBI might come knocking on your door if you happened to view a Web page related to bomb making, or that your insurance company will cancel your health insurance if it finds out you accessed information about cures for cancer. In August 2001, the Yankee Group released the results of a poll that found that 83 percent of consumers are somewhat or very concerned about privacy on the Internet.⁴⁰

Web surfers leave behind a trail of electronic footprints, often unknowingly. Every time users visit a Web site, their Internet address and the Web page they most recently visited is communicated to the host site. It is now common for companies to sell or trade individuals' personal information, often without those individuals' knowledge or consent. Companies create extensive on-line profiles of Internet users that include sites visited, the length of the visits, terms searched for, and whether or not the user responds to unsolicited banner ads. This practice has an unprecedented impact on personal privacy. Your demographic data combined with an extensive profile of your interests (preferences for books, magazines, travel, restaurants, entertainment, etc.) represents a gold mine for marketers who can use the information to target their advertising.

In some cases, the biggest asset many Internet companies have is the resale value of the names, addresses, and e-mail addresses of their customers. Companies value this information because those names become the target of direct mail or e-mail advertising campaigns. As a result, many individuals experience the problem of receiving unsolicited e-mails (spam) or direct mail offers from companies they have never contacted. This is why users often notice they receive target messages or advertisements about certain topics that they recently searched for on the Web.

The on-line profiles are created when a Web site places a "cookie" (ID number) on the user's hard drive. Cookies can be used to identify users returning to a Web site. Session cookies last only while the user is visiting the Web site. However, persistent cookies remain on the hard drive and can be used by advertisers to track the browsing habits of users. Cookies can also be placed on users' computers via invisible images or "Web bugs." According to Privacy International, one advertising service, DoubleClick, has agreements with over 11,000 Web sites and maintains cookies on 100 million users.⁴¹ Some customers have learned to foil cookies by setting their computers to reject them. There are also many on-line privacy tools that consumers can use to protect their Internet privacy. These tools include snoop-proof e-mail, encryption, anonymous re-mailers, and cookie busters. (See Appendix X "Recommendations for Protecting Your Privacy" for additional information and insights into protecting your privacy. This Appendix can be found by accessing the book's companion Web site at www.wiley.com/go/privacy.)

Approximately 18 states have anti-spam laws. The courts in Washington and California recently voted to uphold those laws to protect consumer privacy. In December 2001, the Webmaster for Peacefire.org won \$2,000 in damages in small claims court by invoking Washington's anti-spam law that prohibits sending commercial e-mail containing misleading information in its subject line or using a bogus return address or third-party domain name return address without permission. In January 2002, a court ruled that California has the right to force e-mail marketers to include accurate subject headers and valid contact information in every spam message sent to California residents. The California law specifically requires spam messages to include "ADV" (for advertisement) in their subject headers and makes failure to do so a misdemeanor.⁴²

In January 2002, Toys “R” Us Inc. agreed to pay \$50,000 and change its Internet privacy policies to end a New Jersey state inquiry into how the toy company protected personal information about its customers. Toys “R” Us, which cooperated fully with the state, signed the consent order with Consumer Affairs without admitting any wrongdoing or liability. In December 2000, Consumer Affairs and the Attorney General’s Office subpoenaed records from Toys “R” Us to investigate whether the company had adhered to its written pledge to protect the privacy of consumers’ personal information gathered from its Web site. Coremetrics Inc., a company that worked briefly with Toys “R” Us, gathered the consumer data—addresses and credit card numbers—from cookies which were placed on on-line shoppers’ hard drives. The investigation heightened concerns about the undisclosed use of cookies by on-line merchants. Toys “R” Us agreed to maintain “a clear and conspicuous link to [its] privacy policy on the initial Web page consumers are brought to when they enter the Web addresses *www.toysrus.com* and/or *www.babiesrus.com*.” The agreement also calls for all data transmitted to Coremetrics from the Toys “R” Us Web site to be returned to consumers or destroyed. At the time of this writing, a class-action suit against Toys “R” Us is still pending in California.⁴³

In 2001, Monster.com, an on-line job resource, announced that it was going to sell information contained in its resume database to marketers. The company had already supplied AOL-TimeWarner with information from its database without disclosing the fact to its users. More than 8.6 million people have their resumes listed on Monster.com, with 25,000 new listings each day. The Privacy Foundation states that most people who list their resumes with on-line services have no idea their information may be sold. Furthermore, many resumes may be stored for several years, and may be misused for data mining and identity theft. Also unknown to many job seekers, some resumes that are sent to corporate Web sites often end up being forwarded to third-party resume databases for searching by other employers. Even worse, job sites might forward personal information such as name, address, age, gender, and work history to advertisers.⁴⁴ Monster.com’s potential impact on privacy continues to grow. In June 2001, Monster.com and the U.S. Department of Labor entered into a partnership agreement that will require the sharing of data between the two entities. Monster.com will provide a link to the federal government’s career placement site and cross-list job postings throughout its network. The Privacy Foundation quotes the president of Recruiters Online Network as saying Monster.com probably has “more information on people than anyone outside of the federal government.”⁴⁵

There are several organizations and Web sites dedicated to preserving personal privacy. TRUSTe is an independent, non-profit privacy initiative dedicated to building users’ trust and confidence on the Internet and accelerating growth of the Internet industry. TRUSTe has developed a third-party oversight program that awards a trustmark seal to Web sites that adhere to established privacy principles and agree to comply with TRUSTe’s oversight and consumer resolution process. TRUSTe claims that the trustmark signifies to on-line users that the Web site will openly share, at a minimum, what personal information is being gathered, how it will be used, with whom it will be shared, and whether the user has an option to control its dissemination. With this information, TRUSTe believes users can make informed decisions about whether or not to release their personally identifiable information (e.g., credit card numbers) to the Web site.⁴⁶

In December 2001, a consortium of consumer privacy groups launched an on-line guide for protecting security and privacy on the Internet. ConsumerPrivacyGuide.org offers tips on how to read and understand the privacy policies of on-line retailers and other Web sites that collect information about visitors. It also offers how-to guides for getting rid of “cookies,” the small tags that Web sites leave on users’ hard drives to track their preferences and other information the next time

they return to the site. The site is co-sponsored by six consumer groups: the Center for Democracy and Technology (CDT), the National Consumers League, Consumer Action, Common Cause, Call for Action, and Privacy Rights Clearinghouse. The site was launched to bring Internet privacy and security issues back into focus, group members say. Protecting on-line privacy has fallen out of favor since the September 11 attacks on the United States, with Congress and the Bush administration giving law enforcement agencies more power to snoop on digital communication.⁴⁷

In August 2002, TRUSTe and Watchfire Corporation, a provider of Web site Management software and services, announced a strategic partnership to strengthen TRUSTe's certification and compliance efforts.

TRUSTe will deploy Watchfire WebXM to perform Web site content analysis of its members' sites to identify issues affecting privacy compliance. WebXM's privacy management module, Privacy XM, enables organizations to collect, audit, and report on privacy-related Web site management issues such as identifying secure and unsecured forms, P3P cookie issues, Web site data collection practices, and Web beacons. PrivacyXM gives companies the ability to understand their site's data collection, use, and potential sharing practices, helping them to avoid privacy glitches and better manage their ongoing compliance efforts.

In December 2002, TRUSTe strengthened its privacy certification requirements with the release of its version 8-license agreement. Changes to the license agreement adopted in version 8 include:

- Requiring companies to provide consumers with the choice to opt out before sharing their personal information with any third party unless the sharing is part of a third-party service relationship. Choice no longer hinges on a company's definition of its primary business purpose.
- Requiring licensees to adhere to user preferences for a specified period of time. These preference changes, also known as "Shelf Life Preferences", must be maintained for no less than 12 months with up-front disclosure of intended changes. Furthermore, companies must notify consumers as to the length of time their preferences will remain fixed at the time of registration and via e-mail when preferences expire.
- Requiring companies to gain TRUSTe approval on all notices of a change in practice to better ensure clarity and robust notice.
- Clarifying the requirement that companies ensure that their Comprehensive Privacy Statement is consistent with all other privacy disclosures, such as FAQs and P3P statements.

TRUSTe has implemented these changes in an effort to put more "teeth" into its ability to monitor the privacy practices of Web sites that display TRUSTe's "seal of approval." In upgrading and revising their licensing requirements, TRUSTe has risen the bar for privacy monitoring and compliance.

Many on-line companies have responded to public concerns by posting their privacy policies on the organization's Web site. The policies vary in content and the level of protection they ensure. However, most policies contain a statement of how and why a company collects information, what it does with it, how the information is stored, and what the site does to ensure that the information remains secure. Consumers can use the information contained in the privacy policy to decide whether or not to provide personal information to the site.

ConsumerPrivacyGuide.org provides a list of questions consumers should try to answer when reviewing a company's on-line privacy policy:⁴⁸

- What information is being collected? Is the information personally identifiable?
- Why is it necessary to collect this information? Is the data collection appropriate to the activity or transaction? If not, why does the site need it?

- How is the data being collected? Does the site set cookies? Does the site maintain Web logs?
- How is personal information used once it is collected? Is it ever used for purposes other than those that a visitor intended? (If so, the visitor should be informed of the use.) Has the visitor consented to it? Does the visitor have the option to prohibit such secondary use? Can a visitor prohibit it and still enjoy the site?
- Does the site offer different kinds of service depending on user privacy preferences? Does a user have a choice regarding the type and quantity of personal information that the site collects? Does the site disadvantage users who exercise data collection choices?
- Can users access information that has been collected about them? Are users able to correct inaccurate data?
- How long is personal information stored? Is it kept any longer than necessary for the task at hand?
- What is the complaint and redress process? Whom can users contact?
- What laws govern the collection? Is it a federal government site regulated by the Privacy Act?
- Is the entity collecting information regulated by another privacy law?
- When reviewing the policy, be careful to distinguish information about information collection and privacy from language included to market to you or to encourage you to reveal information.

The *Washington Post* provides the following tips for protecting on-line privacy:⁴⁹

- Read the privacy policies of Web sites.
- Ask how your data will be used.
- Set your browser to alert you to cookies and to reject unnecessary ones.
- Use an anonymizer to hide personal information while browsing. One site to try is www.Anonymizer.com.
- “Opt out” of list sharing. Check individual sites for their policies or look at Operation Opt-out for help.
- Get separate addresses for personal e-mail and for e-mail addresses you give to Web sites.

PROTECTING CHILDREN’S ON-LINE PRIVACY

The privacy of children is especially vulnerable on the Internet. A Web site called kidsprivacy.com provides tips for keeping kids safe on-line. This organization believes the involvement of parents, child care providers, and teachers is the key to helping children have a safe experience on the Internet. Kidsprivacy.com lists the following recommendations for helping young people use the Internet wisely:⁵⁰

- First and foremost, children need to know that just because they are asked for personal information, that does not mean they have to give it out. Even if the request is from a familiar animated character from a television show or a request to fill out a questionnaire to enter a site, play a game, or participate in a contest, a child still needs to ask a grownup first.
- Discuss what personal information is. Many children understand name and address, but should also know that hobbies, pet names, favorite cereal, and amount of allowance are part of their private information and should not be given out on a Web site without asking permission.

- Talk with your child about the Children's Online Privacy Protection Act (COPPA) and why Congress thought the issue of children's privacy on the Web was important enough to pass a law to protect it.
- Look at a Web site's privacy policy together. This tells you what information a child might be asked for and how it might be used. Discuss what you find there.
- Selling on the Web is big business—and expanding rapidly. Talk about how advertising and marketing works. Children understand the world differently than adults, making them especially vulnerable to advertising and marketing. They need to rely on an adult's analytical abilities, judgment and experience. Explain that no matter how cute or clever the Web site, the main reason it's on the Internet is to get a child to want a company's products and services. Keep in mind that some Web sites are aimed at children as young as four to six years old.
- Be around when your child is on-line. Put the computer in a highly visible place and check in periodically. Children can move through Web sites quickly and the enticements to give up personal information are numerous. Children also tend to be particularly trusting of computers and more open to interacting with them.
- If you think that a Web site is collecting information inappropriately, send an e-mail message to register your objection to the company sponsoring the site. And, notify the Federal Trade Commission, which is in charge of enforcing COPPA: Federal Trade Commission's Consumer Response Center at Room 130, 600 Pennsylvania Ave. NW, Washington, DC 20580, or call toll-free 1-877-FTC-HELP (1-877-382-4357). You can also go to the FTC Web site www.ftc.gov and fill out an on-line complaint form.
- Look for sites other than the more well-known, product-based sites. Many of them are just as much fun and interesting. The American Library Association's list of "700+ great sites for kids" at www.ala.org/parents/ is a good place to start.
- Teach children that the Web is a resource, not just a place to play games. Work with them on the Web on family projects—plan a family vacation, research a charity for a donation, find a book on a hobby, build a family Web page.

Lawmakers recently introduced legislation mandating the creation of a ".kids" Internet domain, also called the "Dot Kids Domain Name Act of 2001." Rep. John Shimkus (R—Illinois) and Rep. Edward Markey (D—Massachusetts) co-sponsored the bill because the Internet Corporation for Assigned Names and Numbers (ICANN) had failed to create such a domain. The bill required ICANN to include ".kids" alongside ".com," ".net," and ".org" in the Internet's worldwide addressing system. The domain ".kids" would join domains like ".aero," ".biz," ".coop," ".info," ".museum," ".name," ".gov" and ".pro" that were created since ".com," ".net," and ".org" more than a decade ago. The ".kids" domain received strong support from pro-family groups as a means of identifying the content of on-line material. However, the Congress's Child Online Privacy Protection Act Commission has not recommended the creation of a ".kids" domain because different countries have different standards of what constitutes child-appropriate material. The Commission argued that "kids" is a term not used or understood in many other nations.⁵¹

Other children's privacy resources include:⁵²

- America Links Up (www.americalinksup.org) is a public awareness and education campaign sponsored by a group of non-profits, education groups, and corporations concerned with providing children a safe and rewarding experience on-line. This site

contains resources for parents and kids, and offers a way for individuals and groups to get involved nationwide by planning or attending teach-ins.

- Center for Media Education (www.cme.org) is a non-profit organization dedicated to improving the quality of electronic media, especially on behalf of children and families. The Center for Media Education is involved in investigating the children's on-line marketplace.
- Children's Advertising Review Unit (CARU) (www.bbb.org/advertising/childrensmonitor.asp) is a unit of the Council of Better Business Bureau and is intended to provide voluntary standards for the protection of children under the age of 12.
- The Federal Trade Commission's Kidz Privacy site (www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html) is an educational Web site produced by the FTC surrounding the enactment of the Children's Online Privacy Protection Act. This site offers guidance to parents and children, as well as Web site operators, on the dos and don'ts of children's on-line privacy.
- GetNetWise (www.getnetwise.org) is a resource for families and caregivers to help kids have safe, educational, and entertaining on-line experiences. The Web site includes a glossary of Internet terms, a guide to on-line safety, directions for reporting on-line trouble, a directory of on-line safety tools, and a listing of great sites for kids to visit.
- Online Public Education Network, or Project OPEN (www.internetalliance.org/project-open/about.html) was founded in 1996 as a partnership of the Internet Alliance, the National Consumers League, and leading Internet companies to help consumers get the most out of going on-line. Two guides, "How to Get the Most Out of Going Online" and "Child Safety on the Information Highway," provide tips for parental empowerment.
- Wired Kids (www.wiredkids.org) is the official North American site of UNESCO's Innocence in Danger program. The site's mission is to allow children to enjoy the vast benefits of the Internet while at the same time protecting them from cyber-criminals.
- CyberAngels (www.cyberangels.org) finds and reports illegal on-line material, educates families about on-line safety, works with schools and libraries, and shares basic Internet tips and help resources.
- The United States Department of Justice maintains a "kidspace" on its Web site (www.usdoj.gov/kidspage/) that offers kids a variety of tips for staying safe on-line.

EMPLOYER SPYING

Employers today use many techniques to monitor their employees. The courts have generally upheld employers' rights to monitor employees for security or productivity purposes. Consequently, employers are allowed to conduct background checks and validate the personal histories of potential hires and existing staff. However, in cases where an employee has an expectation of privacy, the courts have generally sided with workers whose privacy has been violated. In any case, employer spying can reduce employee morale and increase anxiety in the workplace.

Video Surveillance

A common method of employer spying is through direct observation of employees. Technological advances have reduced the size and expense of video surveillance to the point where it is common in American workplaces. Employers regularly monitor not only office areas

and production lines, but also traditionally private areas such as employee bathrooms and locker rooms.

Satellite-based tracking systems can be used to monitor the geographic movements of vehicles as well as people. The technology can show the exact position of vehicles at all times to ensure employees are following intended routes and not deviating from approved travel plans.

“Smart” ID cards

These cards include a chip that contains employee information. These high-tech cards use location-tracking technologies used by the military to track the location of personnel throughout the world. Employers have recently begun using the technology to monitor the location of their employees as they move through the office or work site. The technology could be used to determine whether an employee spends too much time on a work break or in the bathroom. One example of a “smart” card is the automated immigration system developed by the U.S. Immigration and Naturalization Service.⁵³ The system identifies people by matching their hand geometry with their hand’s image stored on the “smart” card.

Phone Calls

Although the Electronic Communications Privacy Act of 1986 (ECPA) prohibits the intentional interception of electronic communications in the workplace except for business purposes, phone surveillance is often used in American workplaces. Employers are able to monitor employee phone calls due to a loophole in ECPA that allows employers to listen in on all employee phone calls except personal ones. Obviously, an employer must listen to all phone calls to determine whether each one is personal or not. If a call is deemed personal, employers are supposed to stop listening. However, many employers continue to monitor the length and content of all phone calls, as well as the time of day those calls are made.

Many employers also monitor employee phone calls received via company voice-mail systems. For example, default pass codes installed in some voice-mail systems give managers access to all voice-mail boxes by bypassing employee-selected passwords.

Telephone surveillance or wiretapping can occur in personal as well as business phones. In 1994, the Communications Assistance for Law Enforcement Act (CALEA) required that surveillance capabilities be built into all telephone systems used in the United States.⁵⁴

Computer Monitoring

Many sophisticated techniques are available for employers to use in monitoring how their employees use the computer equipment assigned to them. “Packet sniffing” software packages can analyze and retain all network communications such as an employee’s e-mails, Web sites visited, and files shared. Packet sniffers continuously search employee messages and documents for threatening or sensitive terms or phrases within its search criteria. When these terms are found, administrators can conduct further analysis to determine if the message posed a risk to the company or not. Employers use these computer monitoring tools not only to mitigate risks,

but also to verify that the hardware, software, and communications systems are being used for business purposes only. Some of the monitoring programs employers can use to determine how their employees are using the Internet include the following:⁵⁵

- “LittleBrother” tracks employee Internet usage and provides detailed reports for analysis.
- “SurfWatch” provides Internet monitoring, filtering, and blocking features that can prevent users from accessing unproductive sites. There is also a version that interfaces with CheckPoint’s Firewall-1 and uses some of Firewall-1’s features in conjunction with its own filtering and monitoring capabilities.
- “Internet Manager” tracks most active users and most visited sites.
- “Cyber Snoop” provides Internet monitoring and filtering and allows a system administrator to control sites visited.

Another way employers can monitor computer use is through the use of keystroke loggers that can record every key pressed on a computer keyboard, even if the information was deleted. Keystroke loggers and other programs that can scan data files and e-mails allow employers to monitor Internet usage as it happens. One example of a keystroke logger is “Stealth Keylogger Pro.” Users of computers with this program installed have no idea that it is operating because there is no indication on the task bar or task manager. All keystrokes and application launches are logged to a text file and can be e-mailed to the system administrator.⁵⁶ Employers and law enforcement officials are able to recall the Web sites an employee has visited at any time in the past, even if the Internet history file has been deleted. In this way, records of computer use can assist employers in developing profiles on potential and current employees, as well as assisting in reviews and investigations.

Telecommuters are employees who work from their homes or other remote locations rather than within a business facility. Today there is less distinction than ever before between home and office as telecommuting continues to grow. The privacy issues related to telecommuting continue to unfold. Among the controversial issues still unresolved is how an employer can distinguish between work and non-work activities when monitoring an employee at home, and how an employer can distinguish whether employees or one of their family members is using the office’s equipment. Despite these unresolved issues, employers are increasing their monitoring of how workers with remote Internet access use their e-mail and Web surfing privileges. Employers use software that can record Web sites visited or keystrokes typed, and companies keep copies of e-mails sent through their systems. Thus, employees should be careful about doing personal business on an office computer, even at nights or on weekends, as an increasing number of employees are being fired or reprimanded for inappropriate Internet usage.

Employees who send e-mails or browse the Internet using the workplace network or phone lines should expect very little privacy. Some government employees have argued that employer searches of their e-mails sent from the office violated their rights under the Fourth Amendment to the Constitution, which provides for “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” In *O’Connor v. Ortega*, the Supreme Court extended Fourth Amendment privacy protection to government workplaces. Specifically, the desks and file cabinets of government employees were deemed private places. However, the government may perform searches necessary to promote efficient workplace operations. Government employers may also have a legal right to conduct broader searches of employee offices and equipment if they inform the employees that their desks, computers, and lockers may be searched.

While private employers are not bound by the Fourth Amendment, they must adhere to any applicable laws relating to search and seizure. The courts have generally held that as long as network administrators have the ability to view the contents of e-mails, employees should expect them to be read. Also, e-mails sent from personal computers have been considered private in the same way the contents of a first-class letter are considered private. Personal e-mails can be intercepted and read by law enforcement officials who obtain the proper search warrants. The Electronic Communications Privacy Act of 1986 (ECPA) also allows employers to intercept electronic communications (such as e-mails), if there is an actual or implied consent by the employee. Consent is considered to be implied in cases where employers simply inform employees that their e-mail messages might be monitored. As stated earlier, ECPA also allows employers to monitor employee phone calls, except personal ones.

One major reason employers are concerned about the content of e-mails is sexual harassment. Employers are afraid they will be found liable for sexual harassment in instances where it is perpetuated through the company's computer system. There have been many cases where employees have been fired after sending e-mails that have been deemed inappropriate. However, e-mail messages can be especially susceptible to misinterpretation. The problem is that people often say things in e-mail that they would not say in other settings. E-mail has become a means of informal communication where communicants adopt the slang, jargon, or tone of the person they are communicating with. Also, unlike face-to-face communication, e-mails do not allow the reader to interpret the sender's underlying meaning by observing their body language, tone, or facial expressions. Therefore, an inside joke between two people could be interpreted as a threat or harassment.

Employees also face the problem of receiving e-mails that they did not request or do not want. The content of e-mails is difficult to assess without opening them. Even if opened e-mails are subsequently deleted, the record of them remains on the network file server. Similarly, many Web sites that appear innocent in name may turn out to be pornographic or at least inappropriate to the mission of the organization. Employees who accidentally enter inappropriate Web sites should close them immediately and inform the network administrator that an error was made. Many employers allow for mistakes of this type and monitor Internet and e-mail use to deter or catch the most egregious violators.

Another debate revolves around the difference between using the telephone at work versus the Internet to communicate. Most employers are comfortable with the fact that employees routinely use the telephone at work to call their spouse or to make dinner reservations, yet many of those same employers would be reluctant to allow an employee to make a dinner reservation through the Internet during business hours. The difference is the comfort level associated with the telephone and the relative uncertainty associated with the Internet. Until there is parity between the two mediums, employees should be circumspect in their use of the company's Internet service for personal business.

The courts will continue to address how much privacy employees should be entitled to expect when using office equipment. However, it is clear that companies could be held liable for providing resources that are used to disseminate inappropriate, offensive, or proprietary information. Many companies are responding by developing policies that define the limits of Internet use and that inform employees that their Internet use may be monitored. This trend toward making monitoring policies explicit should help reduce inappropriate Internet use by employees who do not realize the potential implications of what they do on-line.

In order to prevent abuses, the American Civil Liberties Union recommends that employers adopt an electronic monitoring policy that includes the following features:⁵⁷

- Notice to employees of the company's electronic monitoring practices
- Use of a signal to let an employee know when he or she is being monitored
- Employee access to all personal electronic data collected through monitoring
- No monitoring of areas designed for the health or comfort of employees
- The right to dispute and delete inaccurate data
- A ban on the collection of data unrelated to work performance
- Restrictions on the disclosure of personal data to others without the employee's consent

The Internet gives employees great freedom to access information. However, because the service is not free, employers have a right to expect that its employees will use the Internet wisely and for business-related purposes. Telecommuting makes the issue more difficult. If a business supplies an employee with a computer to use at home, does that give the employer the right to read all materials prepared or viewed on that computer? Many people would say that an employee who uses company equipment to view pornography over the Internet is misusing company property, but what about the employee who uses an office laptop to download recipes for chocolate chip cookies?

Employer spying is bound to have a negative influence on employee morale. Most employees are honest, but some are not. Undisclosed spying on everyone in an effort to catch a few thieves can create an atmosphere of distrust throughout the entire organization. As a result, employee dissatisfaction and turnover may increase. Thus, employers are encouraged to clearly communicate their expectations to employees and the methods that will be used to ensure adherence to those expectations.

A recent article on employee spying cited another article by Marsha Woodbury, Ph.D., who wrote, "There is just so much work that can be expected from an employee no matter how many hours he is on the job. If you maintain a happy and trusting atmosphere you are more likely to get more productivity out of those hours that are worked." The article continued to note that, "As a business or corporation you feel that you have a right to protect your business productivity and in fact you do, but doing so in draconian terms can actually hurt your cause rather than help it. In extreme situations such as high security operations or where employee concentration must not be broken by distractions that might endanger the health and safety of others, then employee monitoring is a must. But for most businesses employee monitoring might be best left alone and only put into place if extreme abuse is suspected. In any case, make sure your monitoring policies are known and that your employees can review those policies. Spell out what is acceptable and what is not and what exactly are the consequences for policy violations."⁵⁸

Monitoring e-mail content allows employers to assess the productivity of their workers or to protect trade secrets. Therefore, employers are advised to explicitly warn their employees that their e-mails will be monitored. Companies should develop written privacy policies to address all aspects of privacy, including e-mails. All employees should be required to read and sign a form indicating that they have read and understand the policy.

Monitoring of the U.S. Judiciary

Even federal judges are exposed to workplace monitoring. In May 2001, a group of U.S. federal court judges disabled the Internet connections on their computers after they learned their Web browsing was being monitored by the court administrators who maintained the computers.

The judges, troubled by the privacy and confidentiality issues, argued that the monitoring violated the Electronic Communications Privacy Act of 1986 (ECPA). The administrators felt that monitoring was necessary and sought to institute a policy to inform federal judges and their staff that they should have no expectation of workplace privacy.

In September 2001, the Judicial Conference, the policy-making body of the federal judiciary, decided in favor of the judges. The Conference rejected the administrators' proposed policy to eliminate all judicial expectation of privacy in the workplace and voted to end monitoring of the judges' e-mails. However, the Conference approved limited monitoring of Internet use and prohibited the use of certain file-sharing programs.⁵⁹

Profiling

Employers are increasing their use of psychometric or aptitude testing to evaluate potential employees. Such tests can measure intelligence, personality traits, character, honesty, and work skills. Most employers also conduct extensive background checks before hiring a new staff member. After employees are hired, many can expect to be subjected to regular drug testing. Easy-to-use kits allow companies to administer tests that give immediate results without the need for special laboratory equipment or medical training. The common tests use hair or urine samples and can detect a variety of drugs in the system. However, because tampering with the tests to avoid a positive reading is common, employees may be forced to give a urine sample in the presence of the test administrator. The personal privacy concerns in this case are obvious. Workers subjected to frequent drug tests often feel mistrusted and unmotivated, which can negatively affect productivity. Employers, however, argue that drug tests are necessary to help ensure a safe working environment.

There is increasing concern that future hiring and promotion decisions could be based in part on DNA test results, which could be used to predict a worker's behavioral patterns or predisposition to health problems. A study conducted by the American Management Association in 2000 found that 15 percent of major U.S. firms were using genetic testing or similar tests to predict susceptibility to workplace hazards.⁶⁰ The concern is that these tests will be used to discriminate against certain ethnic or religious groups.

CHANGES TO PERSONAL PRIVACY FOLLOWING SEPTEMBER 11, 2001

On September 11, 2001, the terrorist attacks on the World Trade Center and Pentagon shook the world. In response to those attacks, there have been numerous new laws and policies implemented to reduce the threat of terrorism. However well intentioned these measures, some people have become worried that the increased security measures will have a negative effect on personal privacy. Yet many Americans remain supportive of the intrusions into their private lives brought about by increased surveillance, searches, and other measures. Robert B. Reich, Secretary of Labor under President Bill Clinton, summed up the concerns of privacy advocates when he said, "I'm surprised there hasn't been more of an outcry. The president [George W. Bush] is by emergency decree getting rid of rights that we assumed that anyone within our borders legally would have. We can find ourselves in a police state step by step without realizing that we have made these compromises along the way."⁶¹

New Airport Security Laws

The Aviation and Transportation Security Act (P.L. 107-71), signed by President Bush on November 19, 2001, created the Transportation Security Administration (TSA) in the Department of Transportation. The law makes many fundamental changes in the way transportation security will be performed and managed in the United States. For the first time, aviation security will become a direct federal responsibility, overseen by the new Under Secretary of Transportation for Security (in charge of the TSA), who will report directly to the Secretary of Transportation. In addition, all transportation security activities will be managed by one agency.

The TSA will be very visible to air travelers because it operates the passenger screening process in over 400 communities around the country. The mission of the TSA is broader than aviation and its activities will be more than screening.

The job of the TSA is to look at threats across the national transportation system and prevent disruption by terrorists. The TSA will work with all of the agencies of the United States government to take advantage of the best available intelligence information. The TSA will design and operate a system of overlapping systems—some that are visible to the public, and others that are not. Sophisticated uses of information and advanced technology will be among the tools of a flexible, well-trained, and equipped security force.

Although TSA took over the screener contracts in 2002, federal screener personnel replaced these contracts on November 19, 2002. In addition, according to the law, explosive detection systems are to be in place to screen all checked baggage by December 31, 2002.⁶²

The law allows for more aggressive and extensive search of passengers' bags, and other measures to counter terrorism. The law also allows airlines to use one of four methods to better track baggage: (1) explosive-detection machines, (2) hand searches, (3) bomb-sniffing dogs, or (4) matching checked luggage to passenger lists. Airlines are required to inspect all checked luggage and have a law enforcement officer stationed at every screening station at major airports. Passengers are now subject to more extensive and thorough hand searches of luggage and more computer cross-checks with watch lists maintained by the FBI and other law enforcement groups.

Anti-Terrorism Law

On October 26, 2001, President Bush signed into law the PATRIOT (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act, an anti-terrorism package giving the government access to more personal data and communications. The law, which applies to criminal and intelligence investigations as well as to terrorism investigations, contains the following provisions:⁶³

- It allows government agents to collect undefined new information about Web browsing and e-mail without meaningful judicial review.
- It allows Internet service providers, universities, and network administrators to authorize surveillance of "computer trespassers" without a judicial order.
- It allows the FBI to compel disclosure of any kind of records, including sensitive medical, educational, and library borrowing records, if they are connected with an intelligence investigation.
- It allows law enforcement agencies to search homes and offices without notifying the owner for days or weeks after the search.
- It allows the FBI to conduct wiretaps and secret searches in criminal cases.

The concern of the Center for Democracy and Technology (CDT) is that the law will cut government agencies loose from standards and judicial controls, which could result in the government casting an even wider net and collecting more information on innocent people. The CDT called upon Congress to exercise its oversight powers to conduct review of how the law will be interpreted and applied. The CDT is also looking at the privacy implications of other changes following September 11, such as proposals to allow increased telephone and Internet surveillance, to implement national ID cards, or to increase the use of biometrics (e.g., face recognition technology) at United States borders and in other situations.⁶⁴

Increased Surveillance

In October 2001, the Pentagon issued a rush appeal for ideas for fighting terrorism by asking contractors for new surveillance technologies that could be used for military or civilian purposes. The requested items included a computer system for tracking anyone who buys material that could be used in making bombs, a portable polygraph machine for questioning airline passengers, facial-recognition systems, computer programs that can predict terrorist behavior, scanners for spotting people who have handled weapons of mass destruction, and voiceprint software for automatically recognizing people speaking Middle Eastern languages. The Senate also approved a bill that would greatly expand the ability of law enforcement and intelligence agencies to tap phones, monitor Internet traffic, and conduct other forms of surveillance in pursuit of terrorists.⁶⁵

SUMMARY

Intrusions on personal privacy are increasing at a rapid pace. Business owners expect to know where their employees are and what they are doing, marketers ravenously seek out personal information to build clientele, and the government diligently tries to fulfill its obligation to make sure public places are safe and secure. Meanwhile, the Internet has made vast amounts of information, including private data, available and transferable at the click of a mouse button. But even as the fences guarding our privacy are under siege, new technologies and strategies are being developed to help protect our information, identity, and property.

The major components of privacy are information privacy, bodily privacy, communications privacy, and territorial privacy. Some of the major threats to these aspects of privacy come from surveillance, eavesdropping, wiretapping, office searches, alcohol and drug testing, ethnic and racial profiling, identity theft, biometrics, and unsolicited e-mails, phone calls, or mail. In the future, people could be asked to carry national ID cards that hold their personal information on a computer chip, or the chip with that data could be implanted directly into their bodies.

The attacks of September 11, 2001, have resulted in more measures that affect personal privacy. In the days following the attacks, the government passed new airport security laws and anti-terrorism laws that resulted in more searches of personal belongings and increased surveillance.

But just as new privacy threats appear, new privacy protection ideas are introduced. More and more people are beginning to protect their privacy by opting out of mail and phone lists, by using on-line privacy tools such as anonymous re-mailers and cookie busters, and by restricting outside access to their personal data whenever possible. It is clear that as threats to

privacy increase, more people will be demanding to know why information is being collected, how it will be used, and how it will be kept private.

Chapter 9 discusses in more depth the various means, methods, and tools available to provide individuals with privacy protection.

ENDNOTES

1. Robert Ellis Smith, *Privacy* (Garden City, NJ: Archer/Doubleday, 1980), 323. ISBN: 0385142706
2. Privacy and Human Rights 1999: An International Survey of privacy laws and Developments, Privacy International and the Electronic Privacy Information Center, www.privacyinternational.org/survey/Overview.html#Heading2.
3. Id., www.privacyinternational.org/survey/Overview.html#fn9.
4. Id., www.privacyinternational.org/survey/technologies.html.
5. Feder, B.F., "The Face of Security Technology," *The New York Times* (January 20, 2002), www.nytimes.com/2002/01/20/business/yourmoney/20PROF.html?todayshheadlines.
6. Id.
7. Electronic Privacy Information Center, "Face Recognition," www.epic.org/privacy/face_recognition/ (accessed January 2002).
8. "ACLU Opposes Use of Face Recognition Software in Airports Due to Ineffectiveness and Privacy Concerns", http://archive.aclu.org/issues/privacy/FaceRec_Feature.html.
9. Id.
10. Center for Democracy and Technology, "The Nature and Scope of Governmental Electronic Surveillance Activity," September 2001, www.cdt.org/wiretap/wiretap_overview.html.
11. National Fraud Information Center, General Telemarketing Tips, www.fraud.org/telemarketing/teletips/gentips.htm.
12. McCarthy, E., "Studying Consumers' Movements," *Washington Post* (January 14, 2002): E05. Available on-line at www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A40943-2002Jan13¬Found=true.
13. O'Harrow, R., "Next: An ID Chip Planted in Your Body?" *Washington Post* (December 19, 2001):E01. Available on-line at www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A62663-2001Dec18¬Found=true.
14. Center for Democracy and Technology, "How to Opt Out," [ConsumerPrivacyGuide.org](http://www.consumerprivacyguide.org/howto/optout.shtml) at www.consumerprivacyguide.org/howto/optout.shtml.
15. The National Consumers League, "Tips to Remove Your Name from Marketing Lists," available on-line at www.nclnet.org/privacy/printable.htm.
16. American Association of Retired Persons, "Tips for Protecting Against Credit Card Fraud," available on-line at www.aarp.org/consumerprotect-frauds/Articles/a2002-10-01-Frauds-CreditCards.
17. American Association of Retired Persons, "Understanding Debit Cards," available on-line at www.aarp.org/financial/Articles/a2002-08-14-ManagingMoneyDebitCards.
18. Privacy International's Frequently Asked Questions report on national ID cards, www.privacyinternational.org/issues/idcard/idcard_faq.html.
19. O'Harrow, R., "States Seek National ID Funds Motor Vehicle Group Backs High-Tech Driver's Licenses," *Washington Post* (January 14, 2002): A04. Available on-line at www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A41032-2002Jan13¬Found=true.

20. O'Harrow, R., and J. Krim, "National ID Card Gaining Support," *Washington Post* (December 17, 2001): A01. Available on-line at www.washingtonpost.com/ac2/wp-dyn?page-name=article&node=&contentId=A52300-2001Dec16¬Found=true.
21. Id.
22. Privacy International, "Do ID cards facilitate an increase in police powers?" Identity Cards: Frequently Asked Questions, www.privacy.org/pi/activities/idcard/idcard_faq.html#9.
23. Id.
24. Krebs, B., "National ID-Card Push Roils Privacy Advocates," Newsbytes, September 26, 2001, www.govtech.net/news/news.phtml?docid=2001.09.26-303000000003103.
25. Ho, D., "Is Someone Out To Steal You? Identity Theft On The Rise," Associated Press, January 23, 2002. Available on-line at www.lexisone.com/practicemanagement/pmlibrary/appm012402c.html.
26. American Association of Retired Persons, "Wise Consumer: Identity Theft," available on-line at www.aarp.org/consumerprotect-wise/Articles/a2002-10-03-WiseConsumer-IdentityTheft.
27. U.S. government's central Web site for information about Identity Theft, www.consumer.gov/idtheft/.
28. See note 25.
29. See note 22.
30. AnyBirthday.com, on-line at <http://anybirthday.com/faq.htm>, and <http://anybirthday.com/privacy.htm>, for opt-out procedures.
31. Federal Trade Commission Tips for Consumers, "Id Theft: When Bad Things Happen To Your Good Name," www.ftc.gov/bcp/online/pubs/credit/idtheft.htm#risk.
32. Id., www.ftc.gov/bcp/online/pubs/credit/idtheft.htm#victim.
33. Justice Department, "What Should I Do If I've Become A Victim of Identity Theft?" www.usdoj.gov/criminal/fraud/idtheft.html#What%20Should%20I%20Do%20If%20I've%20Become%20A%20Victim%20OF.
34. U.S. Census Bureau's Confidentiality Protection of Confidential Information—Sections 9 and 214 of Title 13, www.census.gov/main/www/policies.html#confidential.
35. Crowley, Susan L., "Invading Your Medical Privacy: Snoops Finding New Ways to Breach Medical Files," March 2000, www.aarp.org.
36. Wasik, John F., "Protecting Your Medical Privacy," *Consumers Digest* 38, no. 2 (March/April 1999).
37. Federal Trade Commission Privacy Initiatives, "Credit Bureaus: Sample Opt-Out Letter," www.ftc.gov/privacy/cred-ltr.htm.
38. Id.
39. Patient Safety Institute (PSI) "Launch of Patient Safety Institute Empowers New Era In Patient Safety and Quality of Care," news release, www.ptsafety.org/news/nr011211.asp.
40. Yankee Group, "Online Privacy Continues to Be a Major Concern for Consumers" (August 7, 2001), www.yankeegroup.com/webfolder/yg21a.nsf/LatestNews/69E54E0BB8B2BB1885256A9B006F7D26.
41. Electronic Privacy Information Center Washington, DC, USA, and Privacy International London, UK, "Privacy And Human Rights 2001: An International Survey Of Privacy Laws and Developments," p. 45, available on-line at www.privacyinternational.org/survey/phr2001/phr2001.pdf.
42. Krebs, Brian, "Peacefire.org Wins Spam Suits," Newsbytes, 12/12/01, and Mcguire, David, "California Spam Law Upheld As Constitutional — Update," Newsbytes, 1/4/02n.
43. DeMarrais, Kevin, "Deal Set for Net Privacy," *The Hackensack Record*, 1/3/02.
44. Dixon, Pam, "Click You're Hired. Or Tracked . . .," Privacy Foundation, 9/5/01.

45. "A Report on the Privacy Practices of Monster.com," Privacy Foundation, 9/5/01.
46. Truste.org, "The TRUSTe Program: How It Protects Your Privacy," www.truste.org/consumers/users_how.html.
47. Berger, Matt., "Consumer Groups Launch Net Privacy Guide: Privacy Advocates Hope to Draw Attention to Privacy Policies of Major Online Retailers," IDG News Service, 12/18/01.
48. The Center for Democracy and Technology, Consumer Privacy Organization, "How to Read a Privacy Policy," www.consumerprivacyguide.org/howto/readpp.shtml.
49. O'Harrow, R., "Survey: Internet Users Have More Control Over How Data Is Used," *Washington Post* (March 27, 2002), available on-line at www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A25920-2002Mar27¬Found=true.
50. Federal Trade Commission, "How to Protect Kids' Privacy Online," Tips for Consumers, Kidsprivacy.com, www.ftc.gov/bcp/online/pubs/online/kidsprivacy.htm.
51. McGuire, D., "Addressing Authorities Will Tackle Internet Keywords," Newsbytes (January 23, 2002), www.computeruser.com/news/02/01/25/news3.html.
52. Electronic Privacy Information Center (EPIC), Children's Privacy, www.epic.org/privacy/kids, and Online Guide to Practical Privacy Tools, <http://www.epic.org/privacy/tools.html>.
53. Immigration and Naturalization Service, The INS Passenger Accelerated Service System (INSPASS), www.ins.usdoj.gov/text/howdoi/inspass.htm.
54. FCC Again Approves FBI's CALEA Requirements (April 11, 2002), www.epic.org/privacy/wiretap/calea/FCC_order_04_02.pdf.
55. How Do They Spy on You, <http://netsecurity.about.com/library/weekly/aa082100b.htm>, and Electronic Privacy Information Center (EPIC), Work Place Privacy, www.epic.org/privacy/workplace.
56. Id.
57. Privacy in America: Electronic Monitoring, www.aclu.org (accessed 1/23/02).
58. Employer Spying and Morale, <http://netsecurity.about.com/library/weekly/aa082100c.htm>.
59. Electronic Privacy Information Center (EPIC), Work Place Privacy, www.epic.org/privacy/workplace.
60. American Management Association, "Survey of Medical and Workplace Testing (2000)," www.amanet.org/research/archives.htm.
61. Privacy Digest News Page, www.privacydigest.com (accessed 1/26/02).
62. U.S. Department of Transportation, Transportation Security Administration, Overview: The Aviation and Transportation Security Act (P.L. 107-71), www.dot.gov/bib/tsa.html.
63. Doyle, C., Center for Democracy and Technology, American Law Division, "Terrorism: Section by Section Analysis of the USA PATRIOT Act" (December 10, 2001), www.cdt.org/security/usapatriot/011210crs.pdf; and Plesser, R., et al., "Summary and Analysis of Key Sections of USA PATRIOT ACT of 2001," Center for Democracy and Technology (October 31, 2001), www.cdt.org/security/011031summary.shtml.
64. Id.
65. Schneider, G., and R. O'Harrow, "Pentagon Makes Rush Order For Anti-Terror Technology," *Washington Post* (October 26, 2001): A10. Available on-line at www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A53844-2001Oct25¬Found=true.