Privacy

Count not him among your friends who will retail your privacies to the world.

-PUBLILIUS SYRUS (100 BCE)

5.1 Introduction

ARE YOU FAMILIAR WITH GOGGLE'S PHONEBOOK SERVICE? If you visit the Google Web site and type in my phone number as a query, it returns a page giving my name and address. Click on a link, and the screen shows a map of the neighborhood around my house. Phonebook can do this because it's easy for a computer to combine information from multiple sources, as long as they share a key. In this case the common key is my home address. Given my phone number, Phonebook accesses telephone directory records to learn my address. It can then consult a geographic information system to determine my home's location from its address [1].

In 2005 a senior at UMass Dartmouth was collecting materials for a research paper on communism he was writing for one of his history classes. The campus library did not have a copy of Mao Tse-Tung's "Little Red Book," so he filled out an interlibrary loan request, giving his name, address, phone number, and Social Security number. A couple of months later, two agents of the Department of Homeland Security visited him. They told him the book is on a "watch list." The student's interlibrary loan request, combined with the fact that he had spent significant time abroad, apparently triggered the visit. His

professor said, "I shudder to think of all the students I've had monitoring al-Qaeda Web sites, what the government must think of that" [2].

Someone in campus security at Georgetown University accidentally sent out to the entire campus community an email crime report containing the names of three students. To protect the privacy of these students, system administrators shut down the email system at Georgetown University for several hours, examined the mailboxes of everyone on campus, and deleted the offending email [3].

On the morning of July 18, 1989, actress Rebecca Schaeffer opened the door to her apartment and was shot to death by obsessed fan Robert Bardo. Bardo got Schaeffer's home address from a private investigator who purchased her driver's license information from the California Department of Motor Vehicles [4]. In response to this murder, the U.S. Congress passed the Driver's Privacy Protection Act in 1994. The law prohibits states from revealing certain personal information provided by drivers in order to obtain licenses. *It also requires states to provide this information to the federal government.*

In this chapter we focus on privacy issues related to the introduction of information technology. We begin by taking a philosophical look at privacy. What is privacy exactly? Do we have a natural right to privacy distinct from other rights, such as the right to property and the right to liberty? What about our need to know enough about others so that we can trust them? How do we handle conflicts between the right to privacy and the right to free expression?

We then survey some of the ways that we leave an "electronic trail" of information behind us as we go about our daily lives. Both private organizations and governments construct databases documenting our activities. A variety of laws have been passed to regulate the collection and distribution of information gathered by private and public entities. We will study what these laws do—and don't do—to protect individual privacy.

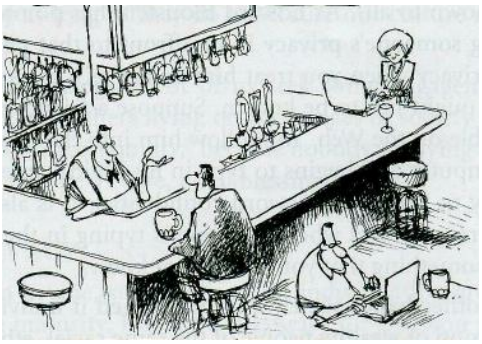
With new technologies have come new ways for governments to intercept the communications of their citizens. We examine the history of covert electronic surveillance by the U.S. government, and how the Fourth Amendment to the Constitution has put boundaries around the surveillance activities of law enforcement organizations. Since 1968, Congress has passed a variety of laws allowing various forms of surveillance by law enforcement and intelligence agencies. Most notable is the USA PATRIOT Act, passed after the September 11, 2001, hijacking of four passenger airliners. Because the Patriot Act gives the government many new powers to collect information, it has generated controversy. We'll examine the major provisions of the Patriot Act and the concerns raised by its detractors.

Next, we take a look at data mining, an important tool for building profiles of individuals and communities. Companies use data mining to improve service and target product marketing to the right consumers. Governments use it to fight crime and enhance national security. The Department of Defense and the National Security Agency have created new data mining programs in response to the terrorist attacks of September 11. Like the Patriot Act, these programs have raised the ire of privacy advocates.

Identity theft is an increasingly common crime. We describe a variety of ways in which thieves steal credit card numbers and other personal and financial information.

The Social Security number has become a commonly used identifier; we study its weaknesses. Some have proposed the creation of a new national identification card for the Unites States. We consider the arguments in favor and against this idea, and we discuss the implications of the REAL ID Act of 2005.

AMP Wtl_ PECWE TM.K 1



© Wiley Miller.

How can people preserve their privacy in the Information Age? One powerful tool is encryption. New encryption technology allows individuals to send messages that are very difficult, if not impossible, for others to decipher. Another tool is digital cash, a technology enabling people to make anonymous transactions in the Information Age. We survey both of these technologies, as well as the attempts by the U.S. government to prevent strong encryption software from being exported to foreign countries.

5.2 Perspectives on Privacy

5.2.1 Defining Privacy

Philosophers struggle to define privacy. Discussions about privacy revolve around the notion *of access,* where access means either physical proximity to a person or knowledge about that person. There is a tug of war between the desires, rights, and responsibilities of a person who wants to restrict access to himself, and the desires, rights, and responsibilities of outsiders to gain access.

Edmund Byrne takes the point of view of the individual seeking to restrict access when he defines privacy as a "zone of inaccessibility" that surrounds a person [5]. You have privacy to the extent that you can control who is allowed into your zone of inaccessibility. For example, you exercise your privacy when you lock the door behind

you when using the toilet. You also exercise your privacy when you choose not to tell the clerk at the video store your Social Security number. However, privacy is not the same thing as being alone. Two people can have a private relationship. It might be a physical relationship, in which each person lets the other person become physically close while excluding others. It might be an intellectual relationship, in which they exchange letters containing private thoughts.

When we look at privacy from the point of view of outsiders seeking access, the discussion revolves around where to draw the line between what is private and what is public (known to all). As Edward Bloustein has pointed out, stepping over this line and violating someone's privacy is an affront to that person's dignity [6]. You violate someone's privacy when you treat him or her as a means to an end. Put another way, some things ought not to be known. Suppose a friend invites you to see a cool movie trailer available on the Web. You follow him into the computer lab. He sits down at an available computer and begins to type in his login name and password. While it is his responsibility to keep his password confidential, it is also generally accepted that you ought to avert your eyes when someone is typing in their password. Another person's password is something that you should not know.

On the other hand, society can be harmed if individuals have too much privacy. Suppose a group of wealthy people of the same racial, ethnic, and religious background forms a private club. The members of the club share information with each other that is not available to the general public. If the club facilitates business deals among its members, it may give them an unfair advantage over others in the community who are just as capable of fulfilling the contracts. In this way privacy can encourage social and economic inequities, and the public at large may benefit if the group had less privacy (or its membership were more diverse).

Here is another example of a public/private conflict, but this one focuses on the privacy of an individual. Most of us distinguish between a person's "private life" (what they do at home) and their "public life" (what they do at work). In general, we may agree that people have the right to keep outsiders from knowing what they do away from work. However, suppose a journalist learns that a wealthy candidate for high public office has lost millions of dollars gambling in Las Vegas. Does the public interest outweigh the politician's desire for privacy in this case?

In summary, privacy is a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information.

5.2.2 Harms and Benefits of Privacy

HARMS OF PRIVACY

Giving people privacy can result in harm to society. Some people take advantage of privacy to plan and carry out illegal or immoral activities. Ferdinand Schoeman observes that most wrongdoing takes place under the cover of privacy [7].

Edmund Leach suggests that increasing privacy has caused unhappiness by putting too great a burden on the nuclear family to care for all of its members. He notes that in the past, people received moral support not just from their immediate family, but also from other relatives and neighbors. Today, by contrast, families are expected to solve their own problems, which puts a great strain on some individuals [8].

On a related note, family violence leads to much pain and suffering in our society. Often, outsiders do not even acknowledge that a family is dysfunctional until one of its members is seriously injured. One reason dysfunctional families can maintain the pretense of normality as long as they do is because our culture respects the privacy of each family [9].

Humans are social beings. Most of us seek some engagement with others. The poor, the mentally ill, and others living on the fringes of society may have no problem maintaining a "zone of inaccessibility," because nobody is paying any attention to them. For outcasts, privacy may be a curse, not a blessing.

BENEFITS OF PRIVACY

According to Morton Levine, socialization and individuation are both necessary steps for a person to reach maturity. Privacy is necessary for a person to blossom as an individual [10].

Jeffrey Reiman has defined privacy as the way in which a social group recognizes and communicates to the individual that he is responsible for his development as a unique person, a separate moral agent [11]. Stanley Benn reinforces this point when he says that privacy is a recognition of each person's true freedom [12].

Charles Sykes argues that privacy is valuable because it lets us be ourselves, suggesting the following example [13]. Imagine you are in a park playing with your child. How would your behavior be different if you knew someone was carefully watching you, perhaps even videotaping you, so that he or she could tell others about your parenting skills? You might well become self-conscious about your behavior. Few people would be able to carry on without any change to their emotional state or physical actions.

In a related observation, Gini Graham Scott points out that privacy lets us remove our public persona [14]. Imagine a businessman who is having a hard time with one of his company's important clients. At work he must be polite to the client and scrupulously avoid saying anything negative about the client in front of any coworkers, lest he demoralize them, or even worse, lose his job. In the privacy of his home he can "blow off steam" by confiding in his wife, who lends him a sympathetic ear and helps motivate him to get through the tough time at work. If people did not have privacy, they would have to wear their public face at all times, which could be damaging to their psychological health.

Other philosophers have pointed out the ways in which privacy can foster intellectual activities. Constance Fischer has pointed out that privacy allows us to shut out the rest of the world so that we can focus our thoughts without interruption [15]. Robert Neville describes how privacy is needed to live a creative life [16]. Joseph Keegan argues

that privacy is needed for spiritual growth, the opportunity to become intimate with the Absolute Being [17].

Charles Fried goes a step further, stating that privacy is the only way in which people can develop relationships involving respect, love, friendship, and trust. According to Fried, "privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable" [18]. Fried refers to privacy as "moral capital." People use this capital to build intimate relationships. Taking away people's privacy means taking away their moral capital. Without moral capital, they have no means to develop close personal relationships.

James Rachels voices a similar sentiment, when he writes that "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people" [19]. Charles Sykes echoes Rachels when he says that each person has a "ladder" of privacy [13]. At the top of the ladder is the person we share the most information with. For many people this person is their spouse. As we work our way down the ladder, we encounter people we would share progressively less information with. Here is an example of what someone's ladder of privacy might look like:

spouse
priest/minister/rabbi
brothers and sisters
parents
children
friends
in-laws
coworkers
neighbors
marketers
employers
government
news media
ex-spouses
potential rivals/enemies

On the other hand, Jeffrey Reiman is critical of suggestions that tie intimacy too closely to sharing information [11]. A woman might tell her psychoanalyst things she would not even reveal to her husband, but that does not imply she experiences deeper intimacy with her psychoanalyst than with her husband. Intimacy is not just about sharing information, it's also about caring. The mutual caring that characterizes a healthy marriage results in a greater level of intimacy than can be gained simply by sharing personal information.

SUMMARY

To summarize our discussion, allowing people to have some privacy has a variety of beneficial effects. Giving people privacy is one way that society recognizes them as adults and indicates they are responsible for their own moral behavior. Privacy allows people to develop as individuals and to truly be themselves. Privacy gives people the opportunity to shut out the world, be more creative, and develop spiritually. Privacy gives each of us the opportunity to create different kinds of relationships with different people. Privacy also has numerous harmful effects. Privacy provides people with a way of covering up actions that are immoral or illegal. If a society sends a message that certain kinds of information must be kept private, some people caught in abusive or dysfunctional relationships may feel trapped and unable to ask others for help. Weighing these benefits and harms, we conclude that allowing people at least some privacy is better than denying people any privacy at all. That leads us to our next question: Is privacy a natural right, like the right to life?

5.2.3 Is There a Natural Right to Privacy?

Most of us agree that every person has certain natural rights, such as the right to life, the right to liberty, and the right to own property. Many people also talk about our right to privacy. Is this a natural right as well?

LEVINE: PRIVACY RIGHTS EVOLVE FROM PROPERTY RIGHTS

Morton Levine has shown how our belief in a right to privacy grew out of our property rights [10]. Historically, Europeans have viewed the home as a sanctuary. The English common law tradition has been that "a man's home is his castle." No one — not even the King — can enter without permission, unless there is probable cause of criminal activity.

In 1 765 the British Parliament passed the Quartering Act, which required American colonies to provide British soldiers with accommodations in taverns, inns, and unoccupied buildings. After the Boston Tea Party of 1773, the British Parliament attempted to restore order in the colonies by passing the Coercive Acts. One of these acts amended the Quartering Act to allow the billeting of soldiers in private homes, breaking the centuries-old common law tradition and infuriating many colonists. It's not surprising, then, that Americans restored the principle of home as sanctuary in the Bill of Rights.

THIRD AMENDMENT TO THE UNITED STATES CONSTITUTION

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

In certain villages in the Basque region of Spain, each house is named after the person who originally constructed it. Villagers refer to people by their house names,

even if the family living in the house has no relation to the family originally dwelling there.

These examples show a strong link between a person and his property. From this viewpoint, privacy is seen in terms of control over personal territory, and privacy rights evolve out of property rights.

WARREN AND BRANDEIS: CLEARLY PEOPLE HAVE A RIGHT TO PRIVACY

We can see this evolution laid out in a highly influential paper, published in 1890, by Samuel Warren and Louis Brandeis. Samuel Warren was a Harvard-educated lawyer who became a businessman when he inherited a paper manufacturing business. His wife was the daughter of a U.S. Senator and a leading socialite in Boston. Her parties attracted the upper-crust of Boston society. They also attracted the attention of the *Saturday Evening Gazette*, a tabloid that delighted in shocking its readers with lurid details about the lives of the Boston Brahmins.[1] Fuming at the paper's coverage of his daughter's wedding, Warren enlisted the aid of Harvard classmate Louis Brandeis, a highly successful Boston attorney (and future U.S. Supreme Court justice). Together, Warren and Brandeis published an article in the *Harvard Law Review* called "The Right to Privacy" [20]. In their highly influential paper, Warren and Brandeis argue that political, social, and economic changes demand recognition for new kinds of legal rights. In particular, they write that it is clear that people in modern society have a right to privacy and that this right ought to be respected. To make their case, they focus on—you guessed it—abuses of newspapers.

According to Warren and Brandeis:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy the prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers . . . The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. [20]

Meanwhile, Warren and Brandeis argue, there are no adequate legal remedies available to the victims. Laws against libel and slander are not sufficient because they do not address the situation where malicious, but true, stories about someone are circulated. Laws addressing property rights also fall short because they assume people have control over the ways in which information about themselves is revealed. However, cameras and

1. To learn more about the Boston Brahmins, consult Wikipedia (www.wikipedia.org).

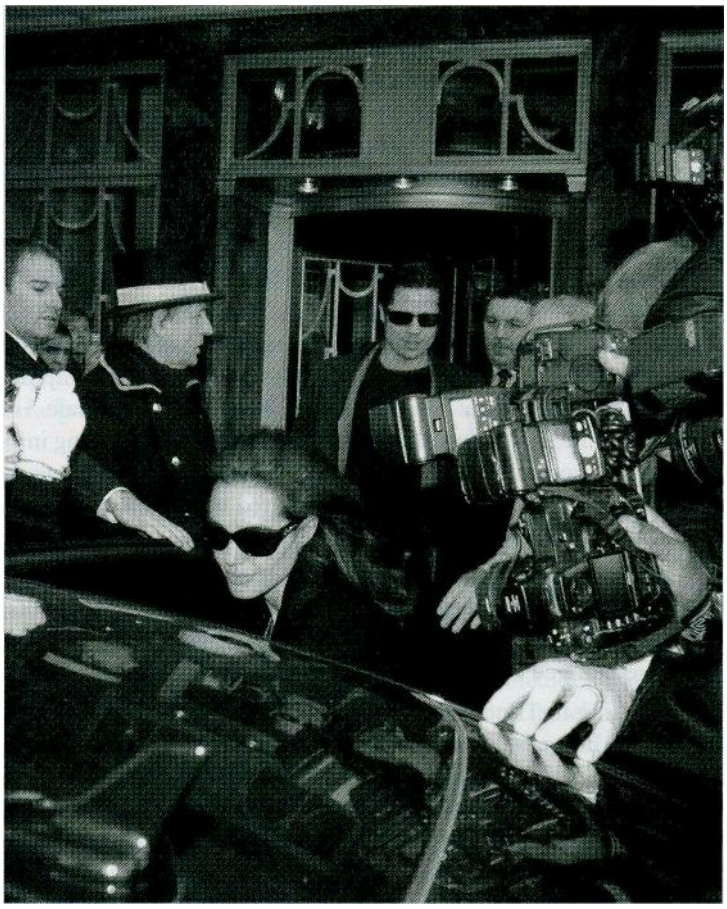


FIGURE 5.1 Warren and Brandeis argued that the legal system should protect people's "right to be left alone." (Chris Uncle / FilmMagic / Getty Images)

other devices are capable of capturing information about a person without that person's consent (Figure 5.1).

Warren and Brandeis pointed out that the right to privacy had already been recognized by French law. They urged the American legal system to recognize the right to privacy, which they called "the right to be let alone" [20]. Their reasoning was highly influential. Though it took decades, the right to privacy is now recognized in courts across America [21].

THOMSON: EVERY "PRIVACY RIGHT" VIOLATION IS A VIOLATION OF ANOTHER RIGHT

ludith larvis Thomson has a completely different view about a right to privacy. She writes: "Perhaps the most striking thing about the right to privacy is that nobody seems

to have any very clear idea what it is" [22]. Thomson points out problems with defining privacy as "the right to be let alone," as Warren and Brandeis have done. In some respects, this definition of privacy is too narrow. Suppose the police use an X-ray device and supersensitive microphones to monitor the movements and conversations of Smith in his home. The police have not touched Smith or even come close to him. He has no knowledge they are monitoring him. The police have let Smith alone, yet people who believe in a right to privacy would surely argue that they have violated Smith's privacy. In other respects, the definition of privacy as "the right to be let alone" is too broad. If I hit Jones on the head with a brick, I have not let him alone, but it is not his right of privacy I have violated—it is his right to be secure in his own person.

Thomson argues that whenever the right to privacy is violated, another right is violated as well. For example, suppose a man owns a pornographic picture. He doesn't want anyone else to know he owns it, so he keeps it in a wall safe. He only takes it out of his safe when he has taken pains to prevent others from looking into his home. Suppose we use an X-ray machine to look into his home safe and view the picture. We have violated his privacy, but we have also violated one of his property rights—the right to decide who (if anybody) will see the picture.

Here is another example. Suppose a Saudi Arabian woman wishes to keep her face covered for religious reasons. When she goes out in public, she puts a veil over her face. If I should walk up and pull away her veil to see her face, I have violated her privacy. But I have also violated one of her rights over her person—to decide who should touch her.

According to Thomson, there are a cluster of rights associated with privacy, just as there are a cluster of rights associated with property and a cluster of rights associated with our physical self. However, every violation of a privacy right is also a violation of a right in some other cluster. Since this is the case, there is no need to define privacy precisely or to decide exactly where to draw the line between violations of privacy and acceptable conduct.

BENN AND REIMAN: AUTONOMOUS MORAL AGENTS NEED SOME PRIVACY

Instead of referring to privacy as a natural right, Stanley Benn proposes that privacy principles be based on the more fundamental principle that each person is worthy of respect [12]. We give each other privacy because we recognize privacy is needed if people are to be autonomous moral agents able to develop healthy personal relationships and act as free citizens in a democratic society.

Jeffrey Reiman expands on Benn's view. He writes:

> The right to privacy protects the individual's interest in becoming, being, and remaining a person. It is thus a right which *all* human individuals possess—even those in solitary confinement. It does not assert a right never to be seen even on a crowded street. It is sufficient that I can control whether and by whom my body is experienced in some significant places and that I have the real possibility of repairing to those places. It is a right which protects my capacity to enter into intimate relations, not because it protects my reserve of generally withheld information, but

> because it enables me to make the commitment that underlies caring as *my* commitment uniquely conveyed by *my* thoughts and witnessed by *my* actions. [11]

Note Reiman's fairly restricted view of privacy. He carefully points out areas where privacy is necessary. He does not argue that privacy is a natural right, nor does he suggest that a person has complete control over what is held private.

CONCLUSION: PRIVACY IS A PRUDENTIAL RIGHT

In conclusion, people disagree whether there is a natural right to privacy. Even if there is no natural right to privacy, most commentators cite the benefits of privacy as a reason why people ought to have some privacy rights. Alexander Rosenberg calls privacy a *prudential right.* That means rational agents would agree to recognize some privacy rights, because granting these rights is to the benefit of society [23].

APPLICATION: TELEMARKETING

Telemarketing provides a good example of how privacy is treated as a prudential right. After being sworn in as Chairman of the Federal Trade Commission (FTC) in 2001, Timothy Muris looked for an action that the FTC could take to protect the privacy of Americans. It did not take long for the FTC to focus on telemarketing. A large segment of the American population views dinner-time phone calls from telemarketers as an annoying invasion of privacy. In fact, Harris Interactive concluded that telemarketing is the reason why the number of Americans who feel it is "extremely important" to not be disturbed at home rose from 49 percent in 1994 to 62 percent in 2003 [24]. Responding to this desire for greater privacy, the FTC created the National Do Not Call Registry (www.donotcall.gov), a free service that allows people who do not wish to receive telemarketing calls to register their phone numbers. The public reacted enthusiastically to the availability of the Do Not Call Registry by registering more than 50 million phone numbers before it even took effect in October 2003 [25, 26].

The Do Not Call Registry will not eliminate 100 percent of unwanted solicitations. The regulations exempt political organizations, charities, and organizations conducting telephone surveys. Even if your phone number has been registered, you may still receive phone calls from companies with which you have done business in the past eighteen months. Still, the Registry is expected to keep most telemarketers from calling people who do not wish to be solicited. The creation of the Registry demonstrates that privacy is seen as a prudential right: the benefit of shielding people from telemarketers is judged to be greater than the harm caused by putting limits on telephone advertising.

5.2.4 Privacy and Trust

While many people complain about threats to privacy, it is clear upon reflection that we have more privacy than our ancestors did [27]. Only a couple of centuries ago our society was agrarian. People lived with their extended families in small homes. The nearest community center was the village, where everyone knew everyone else and people took a keen interest in each other's business. The Church played an important role in everyday

life. In this kind of society there was a strong pressure to conform [14]. There was greater emphasis on the community and lesser emphasis on the individual.

Charles Sykes writes: "Over the past two centuries, the rise of the modern has been the rise of the individual" [13]. He points out that prosperity, the single-family home, the automobile, television, and computers have contributed to our privacy. The single-family home gives us physical separation from other people. The automobile allows us to travel alone instead of on a bus or train in the presence of others. The television brings entertainment to us inside the comfort of our homes, taking us out of the neighborhood movie theater. With a computer and an Internet connection, we can access information at home rather than visit the public library [13]. These are just a few examples of ways in which modern conveniences allow us to spend time by ourselves or in the company of a few family members or friends.

In the past, young people typically lived at home with their parents until they were married. Today, many young unmarried adults live autonomously. This lifestyle provides them with previously unthought-of freedom and privacy [27].

The consequence of all this privacy is that we live among strangers. Many people know little more about their neighbors than their names (if that). Yet when we live in a society with others, we must be able to trust them to some extent. How do we know that the taxi driver will get us where we want to go without hurting us or overcharging us? How do parents know that their children's teachers are not child molesters? How does the bank know that if it loans someone money, it will be repaid?

In order to trust others, we must rely on their reputations. This was easier in the past, when people didn't move around so much and everyone knew everyone else's history. Today, society must get information out of people to establish reputations. One way of getting information from a person is through an ordeal, such as a lie detector test or a drug test. The other way to learn more about individuals is to issue (and request) credentials, such as a driver's license, key, employee badge, credit card, or college degree. As Steven Nock puts it, "A society of strangers is one of immense personal privacy. Surveillance is the cost of that privacy" [27].

5.2.5 A Taxonomy of Privacy

If you've been reading carefully, you've noticed that we *still* haven't defined privacy. We've said that privacy discussions often mention access to a person or access to information about that person, that there can be both benefits and harms to privacy, and that there is often a tension between the desires of the individual and the needs of society. Privacy is hard to define precisely because many different kinds of activities have privacy implications, and the privacy protections associated with different activities can vary widely. For example, pop-up windows can be an unwelcome interference to people who want to surf the Web without being bothered, and erroneous information in credit reports can be an unfair obstacle to people in need of a loan. People may use the word "privacy" when discussing each of these issues, but finding a way to block unwanted pop-up windows is not at all like devising a process for people to correct mistakes in their credit reports.

Daniel Solove suggests that we should take a pluralistic view toward privacy; in other words, we should recognize that a wide variety of activities can lead to privacy concerns [28] .[2] Solove has created a taxonomy that groups privacy-related activities into four categories:

1. *Information collection* refers to activities that gather personal information. Information collection activities often raise privacy concerns. For example, how much personal information should you have to reveal in order to rent DVD movies? If cities install closed-circuit television cameras at intersections to reduce the number of drivers who run through red lights, should other law enforcement agencies have access to those video streams?
2. *Information processing* refers to activities that store, manipulate, and use personal data that has been collected. Some privacy issues arise when information is misused. For example, identity theft can result when sensitive information falls into the wrong hands. Other issues can emerge from the aggregation of data. A government may combine data from bank transactions and credit-card purchases to determine if a citizen should be investigated as a possible domestic terrorist.
3. *Information dissemination* refers to activities that spread personal information. Activities that can raise privacy concerns include breach of confidentiality, disclosure, exposure, and distortion. Here are three examples. A person may betray a confidence by forwarding a private email message to other people. Posting an embarrassing photo of someone on Facebook can expose that person to humiliation or ridicule. Starting or perpetuating a rumor that contains false or misleading information about someone else can damage the victim's reputation.
4. *Invasion* refers to activities that intrude upon a person's daily life, interrupt a person's solitude, or interfere with someone's decision making. Information technology has increased privacy concerns in this category as well. Here are two examples. Spam and pop-up windows are examples of intrusions into a person's solitude. Regulations that require pharmacists to report the names and addresses of people who purchase certain prescription and non-prescription drugs can make people think twice before getting these medications.

5.2.6 Case Study

Jim and Nancy Sullivan are the proud parents of a baby girl. Nancy was on maternity leave, but now she has returned to her full-time job, and they have hired a nanny, after interviewing her and calling a couple of her references. Jim and Nancy's friends tell them horror stories about abusive nannies, and they recommend a software program called LiveSecurityWatch that would let them monitor what's happening at home from a remote computer. Jim and Nancy purchase LiveSecurityWatch and install it on a laptop computer placed in the family room. With the system in place, Jim and Nancy can use

2. Reproduced by permission of the publisher from UNDERSTANDING PRIVACY by Daniel J. Solove, p. 103, Cambridge, Mass: Harvard University Press, Copyright © 2008 by the President and Fellows of Harvard College.

their workplace computers to see and hear how the nanny interacts with their baby. The nanny has no idea that the Sullivan's computer is being used as a surveillance system.

Is it wrong for Jim and Nancy Sullivan to secretly monitor the behavior of their baby's nanny?

ACT UTILITARIAN EVALUATION

We consider the anticipated consequences of the Sullivans's decision on the parties most likely to be affected: Jim and Nancy Sullivan, their baby, and the nanny. The Sullivans interviewed the nanny and called a couple of her references. They believe the nanny is well qualified to take good care of their baby, and they are probably right. They spent time and money setting up the monitoring system, and this is a negative consequence of their course of action. What is most likely to happen is that their observations of the nanny will confirm their view that the nanny will not harm their child. This will give the Sullivans peace of mind, a positive consequence. If the monitoring remains a secret, it seems there will be no positive or negative consequences to the baby or the nanny. However, if the nanny discovers that she has been monitored, she may quit, which would have several negative consequences. The nanny would be unemployed until she could find a new job, and the Sullivans would have to spend time and money looking for a replacement. If word gets out regarding what they have done, some qualified nannies may be not interested in applying for the job, which would make the Sullivans's task more difficult.

There is a slight chance that the Sullivans's covert observations of the nanny will reveal that the nanny is abusing their baby. In this case, they will be able to fire the nanny and save their child from harm, a significant positive benefit to themselves and their baby. Getting fired would be a negative consequence to the nanny.

Whether the total happiness of the affected parties increases or decreases as a result of the Sullivans's decision to secretly monitor the nanny depends upon the probability that the nanny is not harming the baby, the probability that the nanny will discover that the monitoring is taking place, and the weights assigned to each of the possible benefits and harms we have considered.

RULE UTILITARIAN EVALUATION

If all parents monitored their nannies or child care providers and took actions when warranted, such as firing nannies who did not perform well, it is unlikely such monitoring would remain a secret for long. Under these circumstances, nannies would be much more careful to be on their best behavior. This would potentially have the long-term effects of reducing the instances of child abuse and increasing the peace of mind of parents. On the other hand, the harms of the monitoring would be significant in terms of increasing the stress and reducing the job satisfaction of nannies and child care providers. After all, who wants to be monitored constantly? These negative aspects of the job could lead to an increased turnover rate of nannies. Less experienced nannies might well provide lower quality care to the babies they tend. The harms of having all parents monitoring their nannies or child care providers appear to be greater than the benefits. Hence we conclude it is wrong for the Sullivans to secretly monitor their nanny.

SOCIAL CONTRACT THEORY EVALUATION

Social contract theory emphasizes the adoption of rules that rational people would agree to accept because they are to everyone's mutual benefit, as long as everyone else follows the rules as well. As we discussed earlier in this section, privacy is a prudential right. It is reasonable for society to give privacy to people in their own homes, and it is also reasonable for family members within each home to give each other some privacy as well. The nanny wouldn't expect her interactions with the baby in a park or a grocery store to be private, but it is reasonable for her to expect privacy when taking care of the baby inside the Sullivans's home. Hence the Sullivans's decision to secretly monitor the nanny was wrong because it violated her right to privacy.

KANTIAN EVALUATION

Let's consider the morality of acting according to the rule "An employer may secretly monitor the work of an employee who works with vulnerable people." To evaluate the rule using the first formulation of the Categorical Imperative, we universalize it. What would happen if every employer secretly monitored the work of employees who worked with vulnerable people? If that were the case, then employees who worked with vulnerable populations would have no expectation of privacy, and it would be impossible for employers to secretly monitor their work. Hence the proposed rule is self-defeating, and it would be wrong to act according to this rule.

We can also evaluate this situation using the second formulation of the Categorical Imperative. As parents, the Sullivans are responsible for the well-being of their baby. In order to be more confident that their baby is safe in the care of the nanny, they choose to secretly observe the behavior of the nanny. The observation is the means to their desired end of having their baby well cared for. The nanny naturally assumes that her interactions with the baby in the Sullivan residence are private. By not disclosing to the nanny the fact that she is being watched remotely, the Sullivans have treated the nanny as a means to an end. Hence the action of the Sullivans is wrong.

SUMMARY

From the points of view of rule utilitarianism, social contract theory, and Kantianism, we have concluded that it is wrong for the Sullivans to secretly monitor how well their nanny takes care of their baby.

Does this mean that the Sullivans must throw up their hands and simply hope for the best with regard to the quality of their child's care? No. They do have several morally acceptable options that do not involve deceit. They could conduct a more comprehensive interview of the nanny, they could more thoroughly check the nanny's references, or one of them could spend a day or two a home observing the nanny from a distance as she interacted with the baby. The Sullivans could also be candid with the nanny; they could inform her that they would like to install software on their laptop computer that allows them to see and hear what is happening in the apartment. That course of action would respect the moral value of the nanny and give her the freedom to agree to the monitoring, negotiate a different arrangement, or quit.

5.3 Disclosing Information

As we go about our lives, we leave behind an electronic trail of our activities, thanks to computerized databases. Databases record the purchases we make with credit cards, the groceries we buy at a discount with our loyalty cards, the videos we rent by showing our driver's licenses, the calls we make with our telephones, and much more. The companies collecting this information use it to bill us. They also can use this information to serve us better. For example, Amazon.com uses information about book purchases to build profiles of its customers. With a customer profile, Amazon.com can recommend other books the customer may be interested in buying.

It's important to distinguish between public information and public records [29]. A public record contains information about an incident or action reported to a government agency for the purpose of informing the public. Examples of public records are birth certificates, marriage licenses, motor vehicle records, criminal records, and deeds to property.

Public information is information you have provided to an organization that has the right to share it with other organizations. A good example of public information is a listing in a telephone directory. Most of us allow our name, address, and phone number to appear in telephone directories. By doing this, it is easier for our friends and acquaintances to call us or stop by our home. We judge this benefit to be worth the cost to us in the form of less privacy.

Personal information is information that is not public information or part of a public record. You may consider your religion to be personal information. It remains personal information as long as you never disclose it to an organization that has the right to share it. However, if you do disclose your religious affiliation to such an organization, it becomes public information.

Personal information becomes public information or a public record through a voluntary, involuntary, or statutory disclosure (Figure 5.2).

Often people voluntarily make personal information public. Product registration forms and contest entries often ask consumers to reveal a great deal of personal infor-

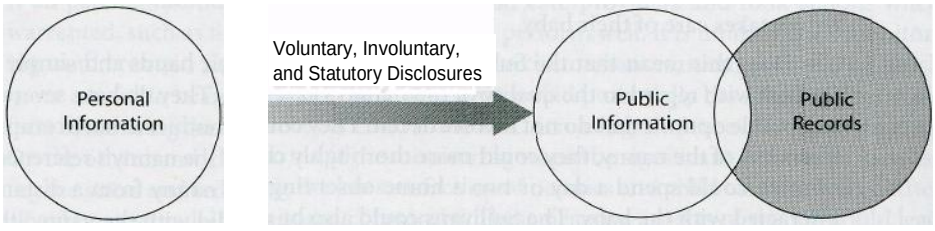


FIGURE 5.2 Personal information becomes public information or part of a public record as the result of a voluntary, involuntary disclosure, or statutory disclosure. The Privacy Act of 1974 puts some restrictions on access to information in public records. (We will discuss the Privacy Act in Section 5.6.4.)

mation. I once received a product preference survey from Proctor & Gamble; it said, in part,

> Your opinions matter to us. That's why we've selected you to participate in one of the most important consumer research surveys we'll do this year. Whether or not you have completed one of our surveys in the past, you can help us continue to create the products that meet your needs. Simply answer the following questions, provide your name and address and mail it back to us. That way, we will be able to contact you if there are any special offers that might be of interest to you.

The questionnaire asked about my family's use of nasal inhalants, coffee, peanut butter, orange juice, laundry detergent, fabric softener, household cleaner, deodorant, toothpaste, detergents, skin care and hair care products, cosmetics, mouthwash, diapers, laxatives, and disposable briefs. It provided a list of 60 leisure activities, ranging from various sports to travel to gambling, and asked me to choose the three activities most important to my family. It also asked my date of birth, the sex and age of everyone living in my home, my occupation, the credit cards we used, and our annual family income. If I had returned the questionnaire (which I didn't), all of this information would have become public.

Sometimes you must disclose information in order to get something you want. If you want to fly on an airplane, you must allow others to search your luggage. You may even be subjected to a body search. You cannot refuse these searches if you want to travel by air. If you want to get a loan from a bank, you must provide the bank with your full name and Social Security number (so it can do a credit check), as well as detailed information about current income, your assets, and your liabilities. If you want to get married, you must fill out a marriage license and submit yourself to whatever tests are required by the local jurisdiction.

At other times, personal information becomes a public record without your consent. Police agencies and courts maintain records of arrests and convictions. Divorce records are public, and they can contain a significant amount of personal information.

Finally, information is sometimes gathered without our knowledge. There are more than four million closed-circuit television cameras installed in public places in England [30]. A resident of London may be captured on tape many times every day. A principal reason for installing these cameras is to reduce crime. However, detractors of this system point to abuses. Some allege that prosecutors have destroyed video footage that may have cleared a suspect. Others say that camera operators have acted like high-tech peeping Toms, using the cameras to watch people having sex [31].

5.4 Public Information

In this section we survey just a few of the many ways that personal information can become public information.

5.4.1 Rewards or Loyalty Programs

Rewards or loyalty programs for shoppers have been around for more than 100 years. Your grandparents may remember using S&H Green Stamps, the most popular rewards program in the United States from the 1950s through the 1970s. Shoppers would collect Green Stamps with purchases, paste them into booklets, and redeem the booklets by shopping in the Sperry and Hutchinson catalog for household items.

Today, many shoppers take advantage of rewards programs sponsored by grocery stores. Card-carrying members of the store's "club" save money on many of their purchases, either through coupons or instant discounts at the cash register. The most significant difference between the Green Stamps program and a contemporary shopper's club is that today's rewards programs are run by computers that record every purchase. Companies can use information about the buying habits of particular customers to provide them with individualized service.

For example, Safeway has unveiled computerized shopping carts at two of its stores in northern California. The shopping cart, called Magellan, has a small computer on the front handle and a card reader on the side. Customers identify themselves by swiping their Safeway Club card through the card reader. The computer taps into the database with the customer's buying history and uses this information to guide the customer to frequently purchased products. As the cart passes through the aisles, pop-up ads display items the computer predicts the customer may be interested in purchasing. It also lets customers purchase some products at sale prices unavailable to others [32].

Critics of grocery club cards say that the problem is not that card users pay less for their groceries, but that those who don't use cards pay more. They give examples of club-member prices being equivalent to the regular product price at stores without customer loyalty programs [33].

Some consumers respond to the potential loss of privacy by giving phony personal information when they apply for these cards. Others take it a step further by regularly exchanging their cards with those held by other people [34].

5.4.2 Body Scanners

Looking good is important to many, if not most, of us. Computer technology is making it possible for us to save time shopping and find clothes that fit us better (Figure 5.3).

In some stores in the United Kingdom, you can enter a booth, strip to your undergarments, and be scanned by a computer, which produces a three-dimensional model of your body. The computer uses this information to recommend which pairs of jeans ought to fit you the best. You can then sit in front of a computer screen and preview what various pairs of jeans will look like on you. When you have narrowed down your search to a few particular brands and sizes, you can actually try on the jeans.

Body scans are also being used to produce custom-made clothing. At Brooks Brothers stores in the United States, customers who have been scanned can purchase suits tailored to their particular physiques [35].

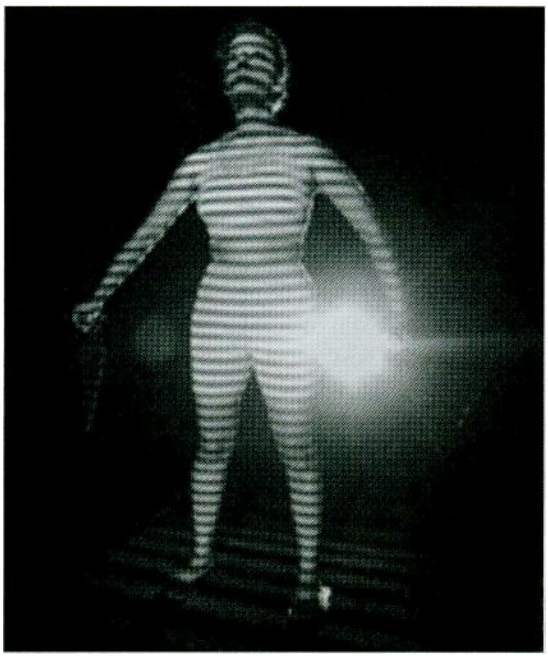


FIGURE 5.3 A computer takes a customer's measurements. (AP/Wideworld Photos)

5.4.3 Digital Video Recorders

TiVo, Inc. manufactures a digital video recorder (DVR), which is similar to a VCR except that it records TV programs on a hard disk instead of videotape. TiVo also provides a service that allows its subscribers to more easily record programs they are interested in watching later. For example, with a single command a subscriber can instruct the TiVo to record every episode of a TV series. What many consumers may not know is that TiVo sells detailed information about the viewing habits of its customers. Because the system monitors the activities of the user second by second, its data are more valuable than that provided by other services. For example, TiVo's records show that 54 percent of its customers skip commercials [36].

5.4.4 Automobile "Black Boxes"

You probably know about airplane flight data recorders, also called "black boxes," which provide information useful in postcrash investigations. Did you know that modern automobiles also come equipped with a "black box"? A microprocessor attached to the car's airbag records information about the speed of the car, the amount of pressure being put on the brake pedal, and whether the seat belts are connected. After a collision, investigators can retrieve the microprocessor from the automobile and view data collected in the five seconds before the accident [37].

5.4.5 Enhanced 911 Service

All cell phone providers in the United States are required by law to be able to track the locations of active cell phone users to within 100 meters. The safety benefit of this capability is obvious. Emergency response teams can reach people in distress who have dialed 911, even if they are unable to speak or do not know exactly where they are.

The ability to identify the location of active cell phone users has other benefits. For example, it makes it easier for cell phone companies to identify where signal strength is weak and coverage needs to be improved.

The downside of enhanced 911 service is a potential loss of privacy. Because it is possible to track the location of active cell phone users, what happens if information is sold or shared? Suppose you call your employer and tell him you are too sick to come into work. Your boss is suspicious, since this is the third Friday this winter you've called in sick. Your employer pays your cell phone provider and discovers that you made your call from a ski resort [38].

5.4.6 RFIDs

Imagine getting up in the morning, walking into the bathroom, and seeing a message on the medicine cabinet's computer screen warning you that your bottle of aspirin is close to its expiration date. Later that day, you are shopping for a new pair of pants. As you try them on, a screen in the dressing room displays other pieces of clothing that would complement your selection.

These scenarios are possible today thanks to a new technology called RFID, short for radio frequency identification. An RFID is a tiny wireless transmitter. Manufacturers are replacing bar codes with RFIDs, because they give more information about the product and are easier to scan. An RFID can contain specific information about the particular item to which it is attached (or embedded), and a scanner can read an RFID from six feet away. When barcodes are replaced by RFIDs, check-outs are quicker and companies track their inventory more accurately (Figure 5.4).

However, because RFIDs are not turned off when an item is purchased, the new technology has raised privacy concerns. Imagine a workplace full of RFID scanners. A scanner in your cubicle enables a monitoring system to associate you with the tags in your clothes. Another scanner picks up your presence at the water cooler. The next thing you know, your boss has called you in for a heart-to-heart talk about how many breaks you're taking. Some privacy advocates say consumers should have a way to remove or disable RFIDs in the products they purchase [39, 40].

The U.S. government plans to replace traditional passports with electronic passports equipped with RFID tags. The RFID tag would duplicate the passport's identifying information and include a digital photograph. By combining the RFID tag's information with new facial recognition technology, the government hopes to improve security at border crossings. Critics of this plan say that RFID tags can be read by anyone within 25 feet who has a powerful enough chip reader. They fear that these tags could make travelers more vulnerable to identity theft [41]. Others wonder if terrorists with power-

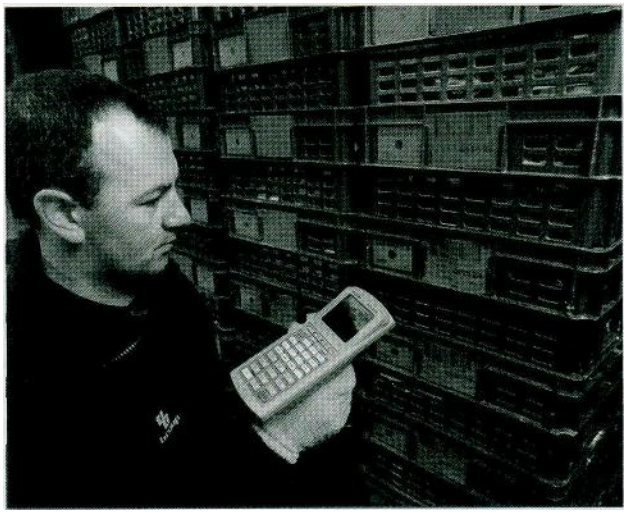


FIGURE 5.4 Employees take inventory more quickly and make fewer errors when items are marked with RFID tags. (Courtesy of Tibbett & Britten)

ful RFID tag readers might begin "scanning" foreign cafes, searching for locations with a high concentration of Americans [42]. Some experts, however, claim that these fears are exaggerated and that RFID tags are difficult to read at a distance [43].

5.4.7 Implanted Chips

In Taiwan every domesticated dog must contain a microchip implant identifying its owner and residence [44]. The microchip, about the size of a grain of rice, is implanted into the dog's ear using a syringe.

Verichip Corporation makes an RFID tag approved for use in humans. More than 2,000 people worldwide have had a Verichip implant. The most common reason for getting an implanted RFID chip is to alert doctors to a medical condition. Even if the patient is unconscious, a doctor can retrieve valuable medical information from the chip [45]. In some trendy European nightclubs, patrons can leave their wallets at home and use their implanted RFID chips as in-house "debit cards" for purchasing food and drinks [46].

Some people believe that parents should implant microchips in their children. They say that the life of a child is more important than any concerns about privacy [47].

5.4.8 Cookies

A cookie is a file placed on your computer's hard drive by a Web server. The file contains information about your visits to a Web site. Cookies can contain login names and passwords, product preferences, and the contents of virtual "shopping carts." Web sites use cookies to provide you with personalized services, such as custom Web pages. Instead

of asking you to type in the same information multiple times, a Web site can retrieve that information from a cookie. Most Web sites do not ask for permission before creating a cookie on your hard drive. You can configure your Web browser to alert you when a cookie is being placed on your computer, or you can set your Web browser to refuse to accept any cookies. However, some Web sites cannot be accessed by browsers that block cookies.

5.4.9 Biometrics

Cookies are one way for companies to provide personalized service over the Internet, but they have a weakness. A cookie makes a link between a Web site and a particular computer. If you are the only person using your computer, that's not a problem, but if you share your computer account with others, all the cookies get lumped together. One way to solve this problem is through biometrics. Imagine a mouse with a fingerprint scanner on the side where you place your thumb. Now all your mouse clicks can be tied back to you personally, giving Web sites the ability to do a better job keeping track of your preferences [48].

5.4.10 Spyware

Spyware is a program that communicates over your Internet connection without your knowledge or consent. Spyware programs can monitor Web surfing, log keystrokes, take snapshots of your computer screen, summon pop-up advertisements, and send reports back to a host computer.

Free software downloaded from the Internet often contains spyware. A 2006 survey of U.S. consumers with broadband Internet connections found that 89 percent of them had spyware on their computers [49].

Some ISPs are responding to the outbreak of spyware by releasing tools to help their customers protect their privacy. For example, America Online includes spyware-detecting tools with its software distribution.