Privacy

Deborah G. Johnson

SCENARIO 5.1 FUND-RAISING AND POTENTIAL DONORS

Jan Perez began college as a computer science major. She loves computers and has always been very good at figuring out how to do things on the Internet and the Web. However, after a year and a half of college, Jan decides that as much as she likes computing, she doesn't want to major in it; she chooses, instead, a major that is more likely to lead to a career involving contact and interaction with people. She also wants something that involves public service or promoting good causes.

After college, Jan is delighted to find that the development office of a large, private university wants to hire her. She accepts the job enthusiastically, thinking she will do some good by raising money for a great university.

Jan's supervisor is extremely pleased to find out how much Jan knows about computers and the Internet. Within a few months of starting the job, Jan is asked to find out all she can about a Frank Doe. Mr. Doe has never been approached by the university; Jan's supervisor only recently heard from another donor that Mr. Doe has a very positive impression of the university and has the capacity to make a major contribution.

The fund-raising unit needs to know how wealthy Mr. Doe is to determine what kind of contribution to ask for. They need to know about his life and interests to know which of their projects he might want to support. And, they need to know about him personally so they can approach him, put him at ease, and not offend him in any way. Jan is given some suggestions about where to look, but she is also told to find out whatever she can.

Using the Internet, Jan does the following:

1. She searches a variety of public databases which give her information about his real estate holdings, his memberships on the boards of public corporations, a list of corporations for which he is a major stockholder.
2. She searches other databases to find out if he has made contributions to political parties or campaigns.
3. She searches archives of newspapers to see if Mr. Doe has ever been written about in the news.

Deborah G. Johnson, *Computer Ethics,* 3rd ed. © Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.

4. She searches other databases to see if he has had any encounters with law enforcement agencies.
5. She searches other databases to find out what religious organizations he supports.
6. She contacts credit agencies and requests his credit history.
7. Jan wonders if Amazon.com would tell her what types of books, if any, Mr. Doe purchases.
8. Jan wonders which Internet service provider Mr. Doe uses; she contemplates what she could learn about Mr. Doe if his service provider would tell her about his online activities. For example, he may keep a portfolio of stock holdings in his account.
9. Mr. Doe is a local resident. Jan's supervisor mentions in passing that Mr. Doe, she has been told, uses the university's medical complex for all his medical treatment. Jan decides to see whether she can access patient files at the university medical complex. Much to her surprise, she is able to access Mr. Doe's insurance records and this tells her that in the last several years, he has been receiving frequent treatment for a kidney ailment. She wonders if this will make him interested in contributing to the hospital or for kidney research.

At the end of several weeks of research, Jan has an enormous amount of information about Mr. Doe. As she acquired each bit of information from a separate database, there didn't seem anything wrong with doing that; now, however, the cumulative effect of putting all of this information together makes Jan feel uncomfortable. She wonders if this is right. She feels a bit like a voyeur or stalker.

Has Jan done anything wrong?

SCENARIO 5.2 TAKING DATA HOME

Max Brown works in the Department of Alcoholism and Drug Abuse of a northeastern state. The agency administers programs for individuals with alcohol and drug problems and maintains huge databases of information on the clients who use their services. Max has been asked to take a look at the track records of the treatment programs. He is to put together a report that contains information about such factors as number of clients seen in each program each month for the past 5 years, length of each client's treatment, number of clients who return after completion of a program, criminal histories of clients, and so on.

To put together this report, Max has been given access to all files in the agency's mainframe computer. It takes Max several weeks to find the information he needs because it is located in a variety of places in the system. As he finds information, he downloads it to the computer in his office; that is, he copies the information from the mainframe onto the hard disk of his office microcomputer.

Under pressure to get the report finished by the deadline, Max finds that he is continuously distracted at work. He decides that he will have to work at home over the weekend to finish on time. This will not be a problem. He copies the information (containing, among other things, personal information on clients) onto several disks and takes them home. He finishes the report over the weekend. To be safe, he leaves a copy of the report on his home computer as well as copying it onto a disk which he takes up to work.

Was Max wrong in moving personal information from the mainframe to his office computer? In moving the information from his office computer to a disk? To his home computer? In leaving the information on his computer at home? What could happen as a result of Max's treatment of the data? Should the agency for which Max works have a policy on use of personal information stored in its system? What might such a policy specify?

SCENARIO 5.3 WORKPLACE MONITORING

Estelle Cavello was recently hired to supervise a large unit of a medical insurance company. Estelle will be in charge of a unit responsible for processing insurance claims. When she was hired, the vice president made it clear to Estelle that he expects her to significantly increase the efficiency of the unit. The company has targets for the number of claims that should be processed by each unit and Estelle's unit has never been able to meet its target.

One of the first things Estelle does when she starts this job is to install a software system that will allow her to monitor the work of each and every claims processor. The software allows Estelle to record the number of keystrokes made per minute on any terminal in the unit. It also allows her to bring the work of others up on her computer screen so that she can watch individual work as it is being done. As well, Estelle can access copies of each employee's work at the end of each day. She can find out how much time each worker spent with the terminal off; she can see what correspondence the person prepared; she can review e-mail that the worker sent or received; and so on.

Should Estelle use this software to monitor her employees?

SCENARIO 5.4 DATA MINING

Ravi Singh works for one of the major credit card companies in their data-processing center. The company is continuously developing new products to offer to customers and add revenue to the corporation. He is an avid reader of computer magazines and recently has been reading about data-mining tools that are now available for a reasonable cost. Ravi goes to his supervisor with the suggestion that their unit purchase one of these tools and use it to find out more about their customers. The information may be telling in terms of customer interest and capability.

The supervisor likes the idea. After exploring the systems that are available, the unit purchases one and Ravi is assigned to explore patterns in the database of information on the company's customers and their purchasing habits.

Ravi discovers that certain zip codes are highly correlated with loan defaults. These zip codes must be in low-income areas, for the mined and analyzed data indicate that the company could reduce its losses significantly by refusing to extend credit to anyone living in 25 zip codes while at the same time not significantly reducing their revenues. In other words, on average, losses due to default generated by individuals in those zip codes were greater than revenue generated.

Ravi continues with his data mining. Next he discoverers a correlation between those who use their credit cards to make contributions to Hindu charitable organizations and those who charge over $40,000 a year on their credit cards. This information seems important. If the company made a special effort to solicit Hindus as customers, it might be able to increase its revenues significantly.

Ravi goes to his supervisor with the suggestion that they adopt these strategies. Has Ravi done anything wrong? If his company adopts these strategies, have they done anything wrong?

These scenarios depict just a few of the ways that information can be created, gathered, moved, and used with computer technology. Of all the social and ethical concerns surrounding computer technology, the threat to personal privacy was probably the first to capture public attention. And this issue persists in drawing public concern and leading to action by policy makers. One hears about it frequently in the popular media; major studies continue to be undertaken; new books continue to be written; and new legislation continues to be passed to regulate electronic information. It will be helpful to begin by laying out just why and how computer technology facilitates information gathering and seems to threaten personal privacy.

IS THERE ANYTHING NEW HERE?

I suggest that computer and information technology, like other new technologies, creates new possibilities; it creates possibilities for behavior and activities that were not possible before the technology. Public concern about computers and privacy arises for precisely this reason. Computers make it possible (and in many cases, cheap and easy) to gather detailed information about individuals to an extent never possible before. Federal, state, and local government agencies now maintain extensive records of individual behavior including such things as any interactions with criminal justice agencies, income taxes, employment history for social security, use of human services agencies, motor vehicle registration, and so on. As well, private organizations maintain extensive databases of information on individual purchases, airline travel, credit worthiness, health records, telephone or cellular phone usage, employment, and so on.

We have the technological capacity for the kind of massive, continuous surveillance of individuals that was envisioned in such frightening early twentieth-century science fiction works as George Orwell's *1984* (1949) and Zamyatin's *We* (1920). The only differences between what is now possible and what was envisioned then is that much of the surveillance of individuals that takes place now is done by private institutions (marketing firms, insurance companies, credit agencies), *and* much of the surveillance now is via electronic records instead of by direct human observation or through cameras. . . .

We can ask whether there is anything fundamentally different about today as compared to 50 years ago or a century ago. Record keeping is far from a new phenomenon. Government agencies and private corporations have been keeping records for thousands of years and using this information in a variety of ways. So, is there anything different about the kind or degree of privacy that we have today as compared to 50 or 100 years ago?

Computer technology has changed record-keeping activities in a number of undeniable and powerful ways. First, the *scale of information gathering* has changed. Second, the *kind of information* that can be gathered has changed. And, third, the *scale of exchange* of information has changed enormously.

In the precomputer, "paper-and-ink" world, the mere fact that records were paper and stored in file cabinets, imposed some limitations on the amount of data gathered, who had access, how long records were retained, and so on. Electronic records do not have these limitations. We can collect, store, manipulate, exchange, and retain practically infinite quantities of data. The point is that technology no longer limits what can be done; now only time and money and, perhaps, human capabilities impose limits on the quantity of information that can be gathered and processed.

The kind of information that it is now possible to collect and use is also new. Think about the workplace monitoring scenario at the beginning of this chapter. Employers can keep records of every keystroke an employee makes. Before computers, finger movements of this kind would not have been thought to be important, let alone the kind of thing that could be recorded. Employers can monitor their employees' uses of the Web, their participation in chat rooms, not to mention their e-mail.

One particularly important new form of information is referred to as transaction generated information (TGI). TGI includes purchases made with a credit card, telephone calls, entry and exit from intelligent highways, and so on. As you move about in the world, your activities (transactions) are automatically recorded. . . .

There is no single government or private organization accumulating all of the information. TGI gathering seems to be fragmented and, therefore, seems not to pose the threat of Big Brother.

Indeed, in the very early days of computing, especially in the 1960s and 1970s, many social commentators expressed concern about the information gathering potential of computer technology and these fears were articulated as fears of Big Brother—fears that all the information would be funneled to a highly centralized U.S. government. The fear was that electronic information gathering practices would give too much power to government. It would create a potentially totalitarian government, a surveillance society. Those fears waned in part because legislation was passed that restricted government information gathering.

Fear also weakened because computer technology changed. It became smaller and cheaper, and, consequently, became available much more widely. On the one hand, this diffused fear of Big Brother because it promised computer power in the hands of "many" rather than just big government. At the same time, however, smaller computers in the hands of many companies and individuals facilitated the exchange of information to an extent previously unimaginable. Typically information of one kind will be gathered and stored separately from information of another kind; for example, marketing firms will gather and store information on buying habits, one government agency will record income tax information, another government agency will record criminal justice activities, and so on.

With computer technology, however, it is technically possible to combine all this information. In the private sector this is done routinely. Think of the fund-raising example at the beginning of this chapter. Within government this happens less frequently because the Privacy Act of 1974 restricted data matching. . . .

The restriction on matching mentioned in the Privacy Act of 1974 did not apply to private organizations, just to the federal government. What was called "matching" in the 1970s is today called data mining and is quite common in private organizations. Indeed, you can now purchase data-mining tools, sometimes called knowledge discovery instruments (kdi) that help find patterns of behavior among groups of individuals. Their use is described in Scenario 5.4.

Add to these changes in the scale and kind of information gathered with computer technology, a further element. Because computerized information is electronic, it is easy to copy and distribute. Before computers were connected by telephone lines, information could be fairly easily copied using tapes or disks. Now that computers are connected via telecommunication lines, information can go anywhere in the world where there are telephone lines. Hence, the extent to which information can be exchanged is now practically limitless. Once information about an individual is recorded in a machine or on a disk, it can be easily transferred to another machine or disk. It can be bought and sold, given away, traded, and even stolen. The information can spread instantaneously from one company to another, from one sector to another, and from one country to another.

The Max Brown case (Scenario 5.2) is illustrative here. He takes sensitive data home on a disk. From a technical point of view, he could have simply accessed the data from home. But in either case, the data moves around. Once it moves out of its source, it is very difficult to keep track of all the places it might exist, be it on disks or hard drives.

Movement of data happens when you subscribe to a magazine and your name and address are sold to a marketing firm. The marketing firm infers from the subscription that you have certain tastes and begins sending you a variety of opportunities to buy the things you like. Forester and Morrison (1990) report the case of a woman who took her landlord to court after he refused to do anything about the pest problem in her apartment. He did not show up for court but evicted her shortly after the court date. When she went looking for another apartment, she found that she was repeatedly turned down by landlords. She would look at an apartment, notify the landlord that she wanted it, and within a few days hear back that the apartment was already rented to someone else. It turned out that a database of names of individuals who take landlords to court is maintained and the information is sold to landlords. Needless to say, landlords don't want to rent to individuals who may take them to court.

As far as the technology goes, the distribution of information can take place with or without the knowledge of the person whom the information is about, and it can take place intentionally as well as unintentionally. There is an unintentional distribution when records are provided that contain more information than is requested. As well, when information is stolen, the exchange is unintentional from the point of view of the agency that gathered or maintained the records. Think again of the Max Brown scenario; Brown's wife, children, or friends might (while using his home computer) inadvertently access the data on individuals in the state's treatment programs and see the names of clients in the state programs.

If all of this were not cause enough for concern, there is more. Information stored in a computer can be erroneous, and, at the same time, can be readily distributed. The effect of a small error can be magnified enormously. Information can be erroneous due to unintentional human error or because someone has intentionally altered it to harm a competitor or enhance their own records. It is important to remember that databases of information are not always as secure as we would like them to be. When computers are connected via telecommunications lines, the possibilities of data's being tampered with or stolen are increased. . . .

Suppose John A. Smith's file is inadvertently combined with John B. Smith's. John A. Smith is turned down for a loan on the basis of erroneous information since John A. has *never* failed to pay his debts, has a good job, and has a sizeable holding of stocks, but John B. has a low-paying job, declared bankruptcy 3 years ago, and is once again deeply in debt. John A. is wronged when he is turned down for a loan. Moreover, suppose that after a series of inquires and complaints by John A., the error is identified, and John A.'s file is corrected. (This is not always as easy as it sounds. Companies are often very slow in responding to complaints about errors in records.) John A. asks his bank to send for the updated report, and the bank changes its mind about the loan when it sees the accurate information. It would appear that the injury to John A. has been remedied. Not necessarily. The inaccurate information may have been given to other companies before it was corrected, and they, in turn, may have given it to others. As a result, it may be difficult, if not impossible, to track down all the databases in which the error is now stored. It may be impossible to completely expunge the erroneous information from John A.'s records.

When information is stored in a computer, there is little incentive to get rid of it; hence, information may stay with an individual for a long period of time. Information stored in a computer takes up very little space and is easy to maintain and transfer. Because of this, details can be carried in a record forever. Something insignificant that happened to an individual when he was 10 years old may easily follow him through life because the information has been recorded once and there is little motivation to delete it. In the past, the inconvenience of paper served to some degree as an inhibitor to keeping and exchanging apparently useless information.[1]

Because it is so easy to keep information, some fear that individuals will get categorized and stigmatized at early stages in their lives. One way to see this is to imagine what it would be like if elementary and secondary school records were put into a national database where prospective employers, government agencies, or insurance companies could get access. We might find decisions being made about us on the basis of testing done when we were in elementary school or on the basis of disciplinary incidents in our teenage years.

When decision makers are faced with making decisions about individuals, they want data. They want data both to insure a good decision and to justify their decision to others. When they must choose between making a decision on the basis of little or no data, and making it on the basis of lots of data known to be unreliable, many prefer the latter. Hence, information tends to get used if it is available even though it may not be relevant or reliable.

In summary, while record keeping is, by no means, a new activity, it appears that computer and information technology has changed record-keeping activities in the following ways: (1) it has made a *new scale* of information gathering possible; (2) it has made *new kinds* of information possible, especially transaction generated information; (3) it has made *a new scale of* information *distribution and exchange* possible; (4) the *effect* of erroneous information can be *magnified*; and (5) information about events in one's life may *endure* much longer than ever before. These five changes make the case for the claim that the world we live in is more like a panopticon than ever before.

As an aside here, you may be tempted to say that computers are not really the problem or the cause of the problem. It is individuals and organizations that are creating, gathering, exchanging, and using information. Computers, according to this line of argument, are simply tools: if there is a problem, the problem is the people who use computers, not the computers themselves.

While there is some truth to this, it is important to remember that computer technology facilitates certain kinds of activities. Computer technology makes it possible for individuals to do things they could not do before. Individuals and organizations are more likely to engage in activities when they are possible (not to speak of easy and inexpensive). For example, in Scenario 5.4, Estelle would not have monitored employees to the extent she did or in quite the way that she did if computers and the monitoring software were not available. Individuals choose actions because they find themselves in a world which has certain possibilities; in a world with different possibilities, they would behave differently. Insofar as computer technology changes what it is possible for human beings to do, it can be a major factor in determining what people do and the kind of society in which we live.

UNDERSTANDING THE "COMPUTERS AND PRIVACY" ISSUE

Uses of Information

Information about individuals would not exist if organizations did not have an interest in using it. Information is created, collected, and exchanged because organizations can use it to further their interests and activities. Information about individuals is used to make decisions about those individuals, and often the decisions profoundly affect the lives of those individuals whom the information is about. Information about you, stored in a database, may be used to decide whether or not you will be hired by a company; whether or not you will be given a loan; whether or not you will be called to the police station for interrogation, arrest, or prosecution; whether or not you will receive education, housing, social security, unemployment compensation, and so on.

The computers and privacy issue is often framed as an issue that calls for a balancing of the needs of those who use information about individuals (typically government agencies and private institutions) *against* the needs or rights of those individuals whom the information is about. Later in this chapter, I will argue against this framing of the issue on grounds that it is biased in favor of information gathering, but for the moment it is important to understand why organizations want information.

In general, those who want information about individuals want it because they believe that it will help them to make better decisions. Several examples quickly illustrate this point. Banks believe that the more information they have about an individual, the better they will be able to make judgments about that individual's ability to pay back a loan or about the size of the credit line the individual can handle. The FBI's National Crime Information Center (NCIC) provides criminal histories of individuals to all the states. Law enforcement agencies justify the existence of this database on grounds that the more information they have about individuals, the better they will be able to identify and capture criminals. We might also bring in examples from the insurance industry where decisions are made about which individuals to insure at what rate, or from the Department of Health and Human Services where decisions are made about who qualifies for various welfare and medical benefits. And, of course, don't forget the fund-raising organization, data-mining, and workplace monitoring scenarios at the beginning of this chapter. In theory, the more and better the information these organizations have, the better their decision making will be.

Companies also claim that they need information about their customers to serve them better. If a company like Amazon.com keeps track of the books that you buy, it can infer from this information what new books you are likely to be interested in. When they send you information on these new books, they claim they are providing a service to you (even if it is one that you didn't ask for and one that happens also to serve their interest in selling more books). If an advertising firm knows what I buy at the grocery store, it can use that information to send me coupons for items I am likely to buy. If television stations know what I watch on television and when I change the channel, they can use that information to develop programming more suited to my tastes. If marketing companies know about my income level and my tastes in clothes, food, sports, and music, they can send me catalogues or special offers for products and services that fit my precise tastes.

In the standard understanding of the computers and privacy issue we have public and private institutions that want information about individuals. They make a powerful case for how this information improves their decision making and helps them to do their job better and more efficiently. In theory, all of that means better serving us, as consumers and citizens. It means, for example, better law enforcement; more efficient government; better, more customized services; and so on.

Personal privacy is generally put on the other side of the balancing scales. The issue is framed so that we have to balance all the good things that are achieved through information gathering and exchange *against* the desire or need for personal privacy. Some even claim that we have a right to personal privacy for if that were true, the scales would weigh heavily on the side of personal privacy. From a legal and constitutional point of view, however, we have, at most, a limited and complex right to privacy.

This framing of the issue seems to be skewed heavily in favor of information gathering and exchange. The only way to counter the powerful case made on behalf of information gathering and exchange is, it would seem, to make a more powerful case for protecting and ensuring privacy in the lives of individuals. Either we must show that there is a grave risk or danger to these information-gathering activities—a danger so great that it counterbalances the benefits of the activity. Or we must show that there is a greater benefit to be gained from constraining these activities. To put this another way, once the benefits of information gathering and exchange are on the table, the burden of proof is on privacy advocates to show either that there is something harmful about information gathering and exchange or that there is some benefit to be gained from constraining information gathering. Either way, there is a daunting hurdle to overcome.

Many of us feel uncomfortable with the amount of information that is gathered about us. We do not like not knowing who has what information about us and how it is being used. Why are we so uncomfortable? What do we fear? Part of the fear is, no doubt, related to our mistrust of large, faceless organizations, and part of it is related to mistrust of government. The challenge is to translate this discomfort and fear into an argument that counterbalances the benefits of information gathering.

Odd as it may seem, the case for protecting personal privacy has not been easy to make. From the point of view of public policy, arguments on behalf of personal privacy have not "won the day." I am going to discuss a number of ways that the case for individual privacy can be and has been made, but I am also going to argue for a somewhat different framing of the issue. At least part of the problem, I believe, lies in framing the issue as a matter of balancing the interests of private and public institutions against the interests of individuals. We ought, instead, to recognize that privacy is both an individual and a social good, one that goes to the heart of the kind of beings we are and important to the realization of a democratic society.

Personal Privacy

Two big questions have dominated the philosophical literature on privacy: What is it and why is it valuable? Needless to say, the two questions are intertwined. Neither has been easy to answer. The term *privacy* seems to be used to refer to a wide range of social practices and domains, for example, what we do in the privacy of our own homes, domains of life in which the government should not interfere, things about ourselves that we tell only our closest friends. Privacy seems, also, to overlap other concepts such as freedom or liberty, seclusion, autonomy, secrecy, and controlling information about ourselves. So, privacy is a complex and, in many respects, elusive concept. A variety of arguments have been put forward to explain the value of personal privacy.

As we review several of these, it will be helpful to keep in mind a distinction between privacy as an instrumental good and privacy as an intrinsic good. When privacy is presented as being valuable because it leads to something else, then it is cast as an instrumental good. In such arguments, privacy is presented as a means to an end. Its value lies in its connection to something else. On the other hand, when privacy is presented as good in itself, it is presented as a value in and of itself. As you might predict, the latter argument is harder to make for it requires showing that privacy has value even when it leads to nothing else or even when it may lead to negative consequences.

The most important arguments on behalf of privacy as an instrumental good have focused either on its being necessary for special relationships or on its being necessary for democracy. Charles Fried (1968), for example, argued that we have to have privacy to have relationships of intimacy and trust. In a society in which individuals were always being observed (as in the panopticon), he argued, friendship, intimacy, and trust could not develop. If we want such relationships, we must create domains of privacy. Others argue that privacy is necessary for democracy. Here the important idea is that if individuals are constantly being observed, they will not be able to exercise the kind of independent thinking that is essential for democracy to work.

The arguments on behalf of privacy as an instrumental good begin to cross over into privacy as an intrinsic good when they suggest a connection between privacy and autonomy. You'll remember from the discussion of Kantian theory that autonomy is not just one among many values; autonomy is fundamental to what it means to be human, to our value as human beings. If privacy is essential to autonomy, then the loss of privacy would be a threat to our most fundamental values. But the connection between privacy and autonomy is often presented not exactly as a means–ends relationship. Rather the suggestion is that autonomy is inconceivable without privacy.

It will take us too far afield to explore all of these arguments. In what follows, I am going to explore several of the most salient arguments on behalf of privacy, and I will move from a focus on privacy as an individual good to privacy as a *social good.*

Information Mediates Relationships

To begin with what seems most clear, information about an individual seems to be a fundamental precondition for establishing a relationship with that individual. Moreover, the information determines the character of the relationship. James Rachels (1975) has argued that people need to control information about themselves in order to maintain a diversity of relationships. His insight is that individuals maintain a variety of relationships (e.g., with parents, spouses, employers, friends, casual acquaintances, and so on), and each of these relationships is different because of the different information that each party has. Think, for example, about what your best friend knows about you as compared with what your teacher, your employer, or your dentist knows about you. These diverse relationships are a function of differing information.

Take your relationship with your dentist. Suppose she has been your dentist for 5 years but she knows relatively little about you, except, of course, for what she knows about your teeth. Now suppose you need extensive work done on your teeth, and you begin to go to her office regularly at a time of the day when she is not rushed. You strike up conversations about your various interests. Each time you talk to her, she learns more about you and you learn more about her. Suppose you discover you have several hobbies and sports interests in common. She suggests that if you schedule your appointment next week so you are her last appointment, you could go out and play tennis afterward. The story can go on about how this relationship might develop from one of patient–professional, to good friends, perhaps to one of intimate friends. The changes in the relationship will in large measure be a function of the amount and kind of information you acquire about one another.

Rachels uses this insight to argue that privacy is important because it allows us to maintain a diversity of relationships. If everything were open to all (that is, if everyone knew the same things about you), then diversity would not be possible. You would have similar relationships with everyone.

Rachels seems right about the way information affects relationships. We control relationships by controlling the information that others have about us. When we lose control over information, we lose significant control over how others perceive and treat us. However, while Rachels seems right about this, his analysis does not quite get at what is worrisome about all the information gathering that is facilitated by computer technology. That is, the information gathering and exchange that goes on via computer technology does not seem, on the face of it, to threaten the diversity of personal relationships each of us has. For example, despite the fact that huge quantities of data now exist about my purchases, phone calls, medical condition, work history, and so on, I am able to maintain a diversity of personal relationships. Rachels seems slightly off target in putting the emphasis on the diversity of relationships, rather than simply on the loss of control of relationships that comes with loss of control of information. Perhaps, this is not surprising given that Rachels focused on personal relationships rather than relationships between individuals and organizations.

What happens when you lose control of information is better thought of on the model of an everyday case in which gossip generates some (false) information about you and the information is spread from one person to another. You are interested in being viewed and treated in a certain way and you know the information (true or false) will affect the way people see you and treat you. Once the information begins to move from person to person, you have no way of knowing who has heard it. If it is false information, you have no way contacting everyone and correcting their repository of information about you. Even if the information is true, there may be individuals that will treat you unfairly on the basis of this information and yet since you don't know who has it, you can't protect yourself. So, loss of control of information reduces your ability to establish and influence the relationships you have and the character of those relationships.

Individual–Organization Relationships

In trying to understand the threat to privacy posed by the new type and scale of personal information gathering made possible by computer technology, the relationships most at issue are those between *individuals and formal organizations.*[2] In these relationships what is important to the individual is that the individual have some power or control in establishing or shaping the relationship (not that he or she has a diversity of such relationships). Information about us is what allows an organization such as a marketing firm, a credit card company, or a law enforcement agency to establish a relationship with us. And information determines how we are treated in that relationship. One is sent an offer to sign up for a credit card when the credit card company gets your name and address and finds out how much you earn and/or own. How much credit is extended depends on the information. Similarly, a relationship between you and your local police force is created when the police force receives information about you; the nature of the relationship depends on the information received.

Currently, organizations may establish (or try to establish) a relationship with you without any action on your part. That is, you may subscribe to a magazine or open a bank account and establish a relationship with one organization, but when that organization sells information about you, another organization creates a file on you and begins to evaluate you for their purposes.

As an aside, let me point out that the twentieth century was a period of enormous growth in the size of public and private organizations (facilitated in part by the development of computer and information technology). This growth is likely to continue in the twenty-first century on a global scale. What this trend means is that instead of interacting with small, local, family-owned businesses wherein one might know or come to know the decision makers personally, most of us now (and in the future will) interact mostly with large national or international organizations operating with complex rules and regulations. Indeed, it is often a computer that makes the decision about our credit line or loan application. We may shop at grocery stores, department stores, or franchises that are local units of national companies. We may purchase items from catalogs or on the Internet and have no idea where the offices of the company are located. We may deal with banks that are national or international, go to large impersonal agencies for government services such as driver's licenses or building permits, attend colleges of 2,000 to 40,000 students, and so on. While our dealings with these organizations may have the most powerful effects on our lives, we may know little about these organizations and the people who own or manage them. Yet they will have (or have access to) an enormous amount of information about us—be it accurate or relevant. And unless we make an exerted effort, we are not likely to know what information they have about us to use when making decisions.

Everything that I have said here was recognized in the 1977 report of the Privacy Protection Study Commission when computer technology was in its early stages of development (i.e., when record-keeping practices were relatively primitive as compared with today's practices). Contrasting face-to-face relationships with relationships to record-keeping organizations, the report explains:

> What two people divulge about themselves when they meet for the first time depends on how much personal revelation they believe the situation warrants and how much confidence each has that the other will not misinterpret or misuse what is said. If they meet again, and particularly if they develop a relationship, their self-revelation may expand both in scope and detail. All the while, however, each is in a position to correct any misrepresentation that may develop and to judge whether the other is likely to misuse the personal revelations or pass them on to others without asking permission. Should either suspect that the other has violated the trust on which the candor of their communication depends, he can sever the relationship altogether, or alter its terms, perhaps by refusing thereafter to discuss certain topics or to reveal certain details about himself. Face-to-face encounters of this type, and the human relationships that result from them, are the threads from which the fabric of society is woven. The situations in which they arise are inherently social, not private, in that the disclosure of information about oneself is expected.
>
> An individual's relationship with a record-keeping organization has some of the features of his face-to-face relationships with other individuals. It, too, arises in an inherently social context, depends on the individual's willingness to divulge information about himself or to allow others to do so, and often carries some expectation as to its practical consequences. Beyond that, however, the resemblance quickly fades.
>
> By and large it is the organization's sole prerogative to decide what information the individual shall divulge for its records or allow others to divulge about him and the pace at which he must divulge it. If the record-keeping organization is a private-sector one, the individual theoretically can take his business elsewhere if he objects to the divulgences required of him. Yet in a society in which time is often at a premium, in which organizations performing similar functions tend to ask similar questions, and in which organizational record-keeping practices and the differences among them are poorly perceived or understood, the individual often has little real opportunity to pick and choose. Moreover, if the record-keeping organization is a public-sector one, the individual may have no alternative but to yield whatever information is demanded of him.

So, private and public organizations are powerful actors in the everyday lives of most individuals in our society, and yet it would seem that individuals have very little power in those relationships. One major factor making this possible is that these organizations can acquire, use, and exchange information about us, without our knowledge or consent. . . .

REFRAMING THE COMPUTERS AND PRIVACY ISSUE—PRIVACY AS A SOCIAL GOOD

A major part of the problem seems to come from the combination of taking a piecemeal approach and then framing the computers and privacy issue as one involving a trade-off between social goods, such as law enforcement and government efficiency, and the interests of individuals in controlling information about themselves. Instead of thinking comprehensively about what record keeping and exchanging practices would be best for our society, the problem has been framed as one in which interests are pitted against one another and business and government seem to be pitted against individuals. This is odd when one remembers that ultimately business and government are justified in terms of their service to individuals as consumers and citizens.

In her 1995 book, *Legislating Privacy,* Priscilla M. Regan examined three privacy policy debates that took place in the United States in recent years—information privacy, communications privacy, and psychological privacy. She concludes that when individual privacy is pitted against social goods such as law enforcement or government efficiency, personal privacy loses. Regan suggests that privacy should be seen not as an individual good but rather as a social good. As an important social good, privacy would be on par with other social goods such as law enforcement or government efficiency. Instead of a social good outweighing an individual good, it would be clear that we have two social goods at stake. In reframing the issue in this way, privacy would be more likely to be treated as equally important, if not more important, than other social goods.

How, then, can the case be made for privacy as a social good? Earlier I argued that loss of control of information about us significantly reduces our autonomy—our power in relationships with formal organizations. Now I want to push this line of thinking even further. Instead of emphasizing loss of control, however, I want to return to the idea of the panopticon. If most everything that we do is recorded, then it would seem that the world that we live in is fundamentally changed from the world that existed in the past. And with this change comes an extremely important loss of freedom. We are unable to go places or do things without a record being created. The act of making a phone call is now the act of making a phone call *and* creating a record. We no longer have the option of making a phone call and not creating a record. Therefore, we have lost a degree of freedom. The loss of this freedom might be justified if you are in prison after having been fairly prosecuted and found guilty. But it hardly seems justified if you have done nothing wrong.

Even more important are the changes that take place in individuals as a result of constant surveillance. When persons are being watched, they tend to take on the perspective of the observer. When you know that decisions will be made about you on the basis of your activities (e.g., your educational records, work records, political activities, criminal activities), you think about that fact before you act. You take on the view of the private and public institutions that will make decisions about you. This can have a powerful effect both on how individuals behave and on how they see themselves. Individuals may come more and more to view themselves as they are viewed by those who watch them.

You may think of this as a good thing insofar as it means more social control and perhaps fewer crimes, fewer loan defaults, people working harder, and so on. The consequences of this kind of social control are, however, insidious. For one thing, it means that formal organizations exert an enormous amount of social control that may or may not be justified. Individuals may be inhibited about what they buy at the grocery store when they learn that their purchases are being recorded and analyzed. Remember that freedom is one of the most fundamental aspects of democracy. Yet freedom is eroded (or at least threatened) when every move is recorded. The result may be individuals who are ill-equipped to live in a democracy.

Consider how Jeffrey Reiman (1995), drawing on other authors, describes the situation:

> To the extent that a person experiences himself as subject to public observation, he naturally experiences himself as subject to public review. As a consequence, he will tend to act in ways that are publicly acceptable. People who are shaped to act in ways that are publicly acceptable will tend to act in safe ways, to hold and express and manifest the most widely-accepted views, indeed, the lowest-common denominator of conventionality. . . . Trained by society to act conventionally at all times, people will come so to think and so to feel. . . . As the inner life that is subject to social convention grows, the still deeper inner life that is separate from social convention contracts and, given little opportunity to develop, remains primitive. . . . You lose both the practice of making your own sense out of your deepest and most puzzling longings, and the potential for self-discovery and creativity that lurk within a rich inner life. . . . To say that people who suffer this loss will be easy to oppress doesn't say enough. They won't have to be oppressed, since there won't be anything in them that is tempted to drift from the beaten path.

The idea of democracy is the idea of citizens having the freedom to exercise their autonomy and in so doing to develop their capacities to do things that have not been thought of and to be critical. All of this makes for a citizenship that is active and pushing the world forward progressively. But if the consequences of trying something new, expressing a new idea, acting unconventionally are too negative, then there is no doubt that few citizens will take the risks. Democracy will diminish.

When the argument for privacy is framed in this way, privacy is shown to be something which is not just an individual good that can be diminished for the sake of a social good; *rather, it is shown to be a social good in its own* right and more important than other social goods such as efficiency and better consumer services. . . .

CONCLUSION

Privacy is, perhaps, the most important of the ethical issues surrounding computer and information technology. I have tried to show this by making clear the importance of privacy to democratic society and the subtle ways in which our lives are changed when we are being watched. Individuals who walk through life knowing that each step creates a record that may or may not end up in a database somewhere are very different from individuals who walk through life feeling free and confident that they live in a open society in which the rules are known and fair.

Protecting personal privacy is not easy and is not likely to get easier. The most effective approach to privacy protection is a many-pronged approach. One thing is for sure, the use of personal information is not going to diminish of its own accord. Information about individuals is extremely valuable both in the private and in the public sector. This issue is not going to go away until we do something about it.

REFERENCES

Fried, Charles. 1968. "Privacy," *Yale Law Journal* 77:477.

Orwell, George. 1949. *1984* New York: Harcourt, Brace & World.

Rachels, James. 1975. "Why Privacy Is Important." *Philosophy and Public Affairs*, 4 (Summer): 323–33.

Regan, Pricilla M. 1995. *Legislating Privacy, Technology, Social Values, and Public Policy.* Chapel Hill, NC: University of North Carolina Press.

Reiman, Jeffrey. 1995. "Hl. Driving to the Panopticon: A Philosophical Exportation of the Risks to Privacy Posed by the Highway Technology of the Future." *Computer and High Technology Law Journal* 11:27–44.

Zamyatin, Yl. 1972. *We.* Harmonsworth, England: Penguin Books. Originally published in Russia, 1920.

NOTES

1. Ironically, it can work the other way as well. Sometimes, that is, changes in technology may result in data's being forgotten. In other words, where paper records stored in boxes in an archive may be obtained (even with difficulty), data stored on an old computer may be much more difficult to access because the technology is obsolete.
2. Of course, information stored in databases could affect personal relationships and gossip can spread on the Internet, but most large-scale, massive databases are maintained by formal organizations who make powerful decisions about individuals.