Privacy

Listen to the **Chapter Audio** on **mythinkinglab.com**

CASE 1 **Explore** the **Concept** on **mythinkinglab.com**

Psychological Testing at Dayton Hudson

Answer each of the following questions True or False:
I feel sure there is only one true religion.

My soul sometimes leaves my body.
I believe in the second coming of Christ.
I wish I were not bothered by thoughts about sex.
I am very strongly attracted by members of my own sex.
I have never indulged in any unusual sex practices.

In April 1989, Sibi Soroka answered these questions satisfactorily and was hired as a Store Security Officer (SSO) at a Target store in California. Afterward, Soroka felt "humiliated" and "embarrassed" at having to reveal his "innermost beliefs and feelings." So he joined with two rejected job applicants in a class-action suit, charging the Dayton Hudson Corporation, the owner of the Target store chain, with invasion of privacy.[1]

Psychological testing is one of many means for enabling employers to evaluate applicants and select the best employee for a job. In the 1920s, the owner of Frank Dry Goods Company in Fort Wayne, Indiana, noticed that some salesgirls sold two to four times as much merchandise as others.[2] Further investigation revealed that the top sellers came from large working-class families with savings accounts, whereas the low performers were from small families that did not need the money and were opposed to the employment. Accordingly, the company developed a set of test questions for job applicants that asked about family size, the occupations of family members, the amount of income needed for an average family, the attitude of the family about working in the store, and the existence of savings accounts.

Dayton Hudson defended the use of the psychological test, called Psychscreen, on the grounds that an SSO, whose main function is to apprehend suspected shoplifters, needs good judgment, emotional stability, and a willingness to take direction. Psychscreen is a combination of two standard tests that have been administered to applicants for such public safety positions as police officers, prison guards, air traffic controllers, and nuclear power-plant operators. The completed Psychscreen test is interpreted by a firm of consulting psychologists which rates an applicant on five traits (emotional stability, interpersonal style, addiction potential, dependability, and rule-following behavior) and offers a recommendation on whether to hire the applicant. Dayton Hudson does not receive the answers to any specific questions.

Dayton Hudson admitted in court that it had not conducted any studies to show that Psychscreen was a reliable predictor of performance as a security officer, except to administer the test to 18 of its most successful SSOs. The company could not document any improvement in the performance of SSOs after adopting the test or any reduction in shoplifting. An expert witness for the plaintiffs contended that the test had not been proven to be reliable or valid for assessing job applicants in this particular setting. An expert witness for Dayton Hudson admitted that the use of Psychscreen resulted in a 61 percent rate of false positives. Thus, even if every unqualified applicant were identified by the test, more than six in ten qualified applicants would also be rejected as unfit.

Dayton Hudson conceded that the intimate questions in Psychscreen constitute an invasion of privacy but added that the intrusion was minor and was justified by the company's needs. Employment application forms ask for some job-related personal information. Even though questions about religion and sex are not themselves job-related, they enable the interpreters of the test to evaluate psychological traits that are related to the job. Dayton Hudson was no more interested than Frank Dry Goods in the personal life of its applicants for employment. The information gained by intimate questions was merely a means to an end. Left unanswered by this response are whether the company's need to administer the test offset the invasion of the applicants' privacy and if so, whether some less invasive means to achieve this end could have been found.

Some critics argue that psychological testing is an invasion of privacy not only because of the intimate nature of the questions but also because the tests seek personal information, namely psychological traits, in ways that the person does not understand and is unable to control. That is, not only the means but also the end is intrusive. Thus, even if a test could be constructed without questions about religion, sex, or any other intimate subject, these critics hold that the test would still be an invasion of privacy.

INTRODUCTION

Early in the twentieth century, the Ford Motor Company set up a "Sociological Department" in order to make sure that workers, in Henry Ford's words, were leading "clean, sober, and industrious" lives.[3] Company inspectors checked bank accounts to keep Ford employees from squandering their munificent $5-a-day wages. They visited employees' living quarters to see that they were neat and healthful, and they interviewed wives and acquaintances about the handling of finances, church attendance, daily diet, drinking habits, and a host of other matters. Workers who failed to live up to Henry Ford's standards of personal conduct were dismissed.

Employers today would scarcely dare to intrude so openly into the private lives of their employees, but they possess less obvious means for acquiring the information sought by Ford's teams of snooping inspectors—and some information that Henry Ford could not have imagined! Among the tools available to present-day employers are quick and inexpensive drug tests, pencil-and-paper tests for assessing honesty and other personality traits of employees, extensive computer networks for storing and retrieving information about employees, and sophisticated telecommunication systems and concealed cameras and microphones for supervising employees'

work activities. By administering medical insurance plans and providing on-site healthcare and counseling, employers are now in a position to know about employees' medical conditions. Some employers have also conducted genetic testing to screen employees for genes that make them more vulnerable to chemicals in the workplace.

Consumers have joined employees as targets for information gathering by American corporations. The same surveillance techniques that are used to monitor employees are now used to detect theft by store customers. Video cameras are commonplace in retail stores, and some retailers have installed hidden microphones as well. The main threat to consumer privacy comes from the explosive growth of database marketing. The countless bits of information that consumers generate in each transaction can now be combined in vast databases to generate lists for direct-mail and telemarketing solicitations. Public records, such as automobile registrations and real-estate transfers, are also readily available sources of information for the creation of specialized lists. The collection of information about users of the Internet, which is in its infancy, has immense potential for marketers.

Concern about privacy is a relatively recent occurrence. However, a 1979 public opinion survey conducted by Louis Harris for the Sentry Insurance Company revealed that three out of four respondents believed that privacy should be regarded as a fundamental right akin to life, liberty, and the pursuit of happiness and that half of them fear that American corporations do not adequately safeguard the personal information they gather on individuals.[4] Over 90 percent of those who responded said that they favored safeguards to prevent the disclosure of personnel and medical files to outsiders. A law granting employees access to the information collected about them was favored by 70 percent, and 62 percent wanted Congress to pass a law regulating the kind of information that corporations may collect about individuals.

CHALLENGES TO PRIVACY

Privacy has become a major issue in government and business in recent years for many reasons. One is simply the vast amount of personal information that is collected by government agencies. The need to protect this information became especially acute after the passage of the Freedom of Information Act (FOIA) in 1966. Intended by Congress to make government more accountable for its actions, the act had the unforeseen consequence of compromising the confidentiality of information about private individuals. The Privacy Act of 1974 was designed in large part to resolve the conflict between government accountability and individual privacy. So great were the problems that Congress created the Privacy Protection Study Commission to investigate and make recommendations about further action. The National Labor Relations Board has long faced a similar problem with union demands for access to personnel files and other employee records. Unions claim that they need the information in order to engage in fair collective bargaining, but allowing unions to have unlimited access to this information without consent violates the employees' right of privacy.[5]

Employee Privacy

Government is not the only collector of information. Great amounts of data are required by corporations for the hiring and placement of workers, for the evaluation of their performance, and for the administration of fringe-benefit packages, including health insurance and pensions. Private employers also need to compile personal information about race, sex, age, and handicap status in order to document compliance with the law on discrimination. In addition, workers' compensation law and occupational health and safety law require employers to maintain extensive medical records. Alan F. Westin, an expert on privacy issues, observes that greater concern with employee rights in matters of discrimination and occupational health and safety has had the ironic effect of creating greater dangers to employees' right of privacy.[6]

WORKPLACE MONITORING. Monitoring the work of employees is an essential part of the supervisory role of management, and new technologies enable employers to watch more closely than ever before, especially when the work is done on telephones or computer terminals. Supervisors can eavesdrop on the telephone conversations of employees, for example, and call up on their own screens the input and output that appear on the terminals of the operators.[7] Hidden cameras and microphones can also be used to observe workers without their knowledge. A computer record can be made of the number of telephone calls, their duration, and their destination. The number of keystrokes made by a data processor, the number of errors and corrections made, and the amount of time spent away from the desk can also be recorded for use by management. Even the activities of truck drivers can be monitored by a small computerized device attached to a vehicle that registers speed, shifting, and the time spent idling or stopped.

Companies claim that they are forced to increase the monitoring of employees with these new technologies as a result of the changing nature of work. More complex and dangerous manufacturing processes require a greater degree of oversight by employers. The electronic systems for executing financial transactions and transferring funds used by banks and securities firms have a great potential for misuse and costly errors. In addition, employers are increasingly concerned about the use of drugs by workers and the high cost of employee theft, including the stealing of trade secrets. Employers also claim to be acting on a moral and a legal obligation to provide a safe workplace in which employees are free from the risk of being injured by drug-impaired coworkers.[8]

Even efforts to improve employees' well-being can undermine their privacy. Wellness programs that offer medical checkups along with exercise sessions result in the collection of medical data that can be used to terminate employees or defend against workplace injury claims. More than half of all U.S. employees have access to Employee Assistance Plans (EAPs) for help in handling personal problems and drug addictions. Although the information gained is generally held in confidence, it is available for company use when an employee files a workplace injury claim or sues for discrimination, wrongful discharge, or any other wrong. In some instances, employers have used the threat of revealing unrelated embarrassing information in court to dissuade employees from pressing a suit. Although the use of an EAP is usually voluntary, employees are often required to gain approval from an EAP counselor before seeking company-paid mental healthcare. Some employees thus face the choice of revealing their mental health condition to their company or paying for mental health care out of pocket.

ignore

PSYCHOLOGICAL TESTING. One particular area of concern has been psychological testing of the kind conducted by Dayton Hudson (Case 1). Interest in psychological testing was spurred in the first half of the twentieth century by the "scientific management" ideas of Frederick Taylor and the development of the field of applied or industrial psychology. The massive testing programs of the armed forces in two world wars were carried over into civilian life by large American corporations. In the postwar period, American education became increasingly reliant on standardized testing for admission to colleges and universities, not only to identify qualified students but also to prevent discrimination. Tests that measure job-related abilities and aptitudes have raised little opposition. However, employers have increasingly come to recognize that an employee's psychological traits are important, not only for predicting successful job performance but also for identifying potentially dishonest and troublesome employees.

This latter goal is the appeal of integrity tests, which are sold by a handful of publishers and administered to an estimated 5 million job applicants annually. Use of the pencil-and-paper tests has been spurred by the banning of mechanical polygraph testing in 1988 and by the reluctance of former employers to reveal any but the most basic information. Studies by the congressional Office of Technology Assessment and the American Psychological Association have found that some tests have moderate predictive value but that others are virtually worthless. Large numbers of honest people are denied jobs and suffer a stigma because of faulty testing, and a few rogues slip through.

Some critics have charged that no one can pass an integrity test without a little dishonesty. Ironically, the highly honest may be among the most frequent victims of mistakes because they are more forthcoming in their answers. The use of integrity tests also assumes that people are honest—or not—and ignores the role of the work environment in promoting honesty—or dishonesty. Some employees steal when they believe that they are being cheated or abused, for example. One benefit of integrity tests, therefore, may be to enable employers to recruit a work force that will tolerate shabby treatment without retaliating.

Consumer Privacy

Concern about consumer privacy has focused primarily on the gathering and use of information in database marketing. Businesses have discovered that it pays to know their customers. For example, grocery stores that issue identification cards that are scanned along with the universal product code on each product are able to construct detailed profiles of each customer's purchasing preferences. This information may be used in many ways, including the making of offers that are tailored to appeal to specific customers. However, the main value of a database of consumer information lies in the capacity to generate customized mailing lists. If a company can identify the characteristics of potential customers by age, income, lifestyle, or other measures, then a mailing list of people with these characteristics would enable the seller to reach these customers at relatively low cost. Such targeted selling, known as direct mail, is also potentially beneficial to consumers, because a customized mailing list is more likely to produce offers of interest to consumers than is a random mailing.

The growth in database marketing has been facilitated by computer technology, which is able to combine data from many sources and assemble them in usable form. For example, by merging information about an individual with census data for that person's zip-code-plus-four area, it is possible to make reliable inferences about income, lifestyle, and other personal characteristics. Companies that specialize in data collection can provide direct marketers with customized mailing lists that target groups with the desired characteristics. Although American consumers are concerned about the threat to privacy posed by the use of personal information for this purpose, one survey showed that over two-thirds of respondents approved of the use of customized mailing lists to offer goods and services to people who are likely to be interested.[9] However, when Lotus Development Corporation announced plans in April 1990 for the database program Lotus Marketplace: Households, a set of compact discs containing information on 120 million Americans, a storm of protest ensued. This episode showed that consumers believe that there are limits on the use of personal information for marketing purposes and that this product had crossed a line.

ignore

ISSUES IN CONSUMER PRIVACY. One issue in the use of databases to generate mailing lists is the right of control over information. If we reveal some information about ourselves to a company, does that company "own" the information? For example, does a magazine have a right to sell a list of its subscribers to a direct marketer? We voluntarily provide our name and address to the magazine for the purpose of obtaining a subscription, just as we reveal our annual income to a bank in order to obtain a loan. These are examples of the *primary* use of information. The use of information for some other purpose is labeled *secondary*. Some privacy advocates hold that there should be no secondary use of information without a person's knowledge and consent. Thus, some magazines inform subscribers that they make their list available for direct mail and allow subscribers to "opt out" by removing their name and address from the list. In general, the secondary use of any information in a loan application is prohibited by law.

Other issues concern access to information and potential misuse. Although an individual's annual income is generally regarded as personal, people may not be upset to learn that this information is used to generate a mailing list—as long as no one has access to the information itself. A direct marketer has no interest in knowing a particular person's income but only whether that person is a likely prospect, and the fact that a person's name and address is on a list does not

reveal to anyone that person's income. However, some information is considered too sensitive to be included in a marketing database. Health information has generally fallen into this category, but pharmaceutical companies now seek mailing lists of patients with particular conditions. For example, *Reader's Digest* succeeded in obtaining completed questionnaires on health problems from 9 million subscribers, and the magazine was planning to make this information available for direct mail on specific pharmaceutical products.[10] Patients' records, prescription data from pharmacies, and even calls to the toll-free numbers of pharmaceutical companies are resources for information gatherers.[11] Companies that sell lists also have a responsibility to screen buyers to ensure that direct mailings are for legitimate purposes and do not involve consumer fraud.

Ethical questions about employee and consumer privacy are unavoidable because obtaining and using personal information is essential in both employment and marketing. But everyone has a legitimate interest in maintaining a private life that is free from unwarranted intrusion by business. Finding the right balance between the rights of everyone concerned is not a simple task. A set of guidelines or a company code on employee and consumer privacy must address an immense number of different questions. Before we make the attempt to find a balance between these competing rights, though, it is necessary for us to inquire into the meaning of privacy as an ethical concept.

THE MEANING AND VALUE OF PRIVACY

A definition of privacy has proven to be very elusive. After two years of study, the members of the Privacy Protection Study Commission were still not able to agree on one. Much of the difficulty is due to the diverse nature of the many different situations in which claims of a right of privacy are made. Even the narrower concept of privacy for employees and consumers is applied in such dissimilar circumstances that it is not easy to find a common thread running through them.

History of the Concept

As a legal concept, privacy dates only from the late nineteenth century. There is no mention of privacy in the original Constitution or the Bill of Rights. Although a number of rights related to privacy have long been recognized in American law, they have generally been expressed in terms of freedom of thought and expression, the right of private property, protection from "unreasonable searches and seizures," and other constitutional guarantees. The first sustained discussion of privacy occurred in an 1890 article in the *Harvard Law Review* written by two young attorneys, Samuel Warren and Louis Brandeis (who later became a famed justice of the Supreme Court).[12]

The theory of privacy presented by Warren and Brandeis was slow to gain acceptance. It was rejected by the courts in a number of cases around the turn of the century in which the names and pictures of prominent persons were used to advertise products. The public uproar over one of these cases prompted the New York legislature to enact a law prohibiting the commercial use of a person's name or likeness without permission.[13] Gradually, most states followed the lead of New York in granting persons a right to be free of certain kinds of intrusion into their private lives. But it was not until 1965 that the Supreme Court declared privacy to be a constitutionally protected right. The decision came in *Griswold* v. *Connecticut*, which concerned the right of married couples to be free of state interference in the use of contraceptives.[14]

Some philosophers and legal theorists have argued that the concept of privacy does not introduce any new rights into the law but merely expresses several traditional rights in a new way. Consequently, our legal system already contains the resources to protect individuals against these wrongs without creating a distinct right of privacy.[15] For example, disclosing embarrassing facts about a person or intruding into his or her solitude might be described as inflicting mental distress; and the publication of false accusations could be said to constitute libel or defamation of character. What, these critics ask, does the concept of privacy add to other, better-established rights?

Definitions of Privacy

The literature contains many attempts to elucidate privacy as an independent right that is not reducible to any other commonly recognized right. Three definitions in particular merit examination. One, which derives from Warren and Brandeis and finds expression in *Griswold* v. *Connecticut*, holds that privacy is the right to be left alone. Warren and Brandeis were concerned mainly with the publication of idle gossip in sensation-seeking newspapers. The aim of privacy laws, they thought, should be to protect "the privacy of private life" from unwanted publicity, and their proposals all deal with limits on the publication of information about the private lives of individuals. In his celebrated dissenting opinion in *Olmstead* v. *United States*, a 1928 case concerning the constitutionality of telephone wiretapping, Brandeis wrote that the right of privacy is "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[16]

A similar view of privacy was expressed by the majority in *Griswold*. Laws governing the use of contraceptives intrude into an area of the lives of individuals where they have a right to be let alone. Justice William J. Brennan expressed the view in a subsequent birth control case that

> If the right to privacy means anything, it is the right of the individual, married or single, to be free from unwarranted government invasion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.[17]

Many critics have pointed out that the phrase "to be let alone" is overly broad.[18] Individuals have a right "to be let alone" in matters of religion and politics, for example, but legal restrictions on religious practices, such as snake handling, or on political activities, such as the making of political contributions, do not involve violations of privacy. At the same time, the Warren and Brandeis definition is too narrow, because some violations of privacy occur in situations where there is no right to be let alone. Workers have no right to be free of supervision, for example, even though it can be claimed that their privacy is invaded by the use of hidden cameras to monitor their activity secretly.

These objections, in the view of critics, are merely symptoms of a deeper source of error in the Warren and Brandeis definition, which is the confusion of privacy with liberty. These examples show that a loss of liberty is neither a necessary nor a sufficient condition for a loss of privacy. Perhaps greater clarity is achieved by limiting the concept of privacy to matters involving information and not stretching the concept to include all manner of intrusions into our private lives. Thus, cases in which companies refuse to hire smokers are better analyzed as limitations of liberty rather than invasions of privacy.

This suggestion is reflected in a second definition in which privacy is defined as control over information about ourselves.[19] According to Alan F. Westin, "Privacy is the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[20] This definition is open to the same charge: It is at once too broad and too narrow. Richard B. Parker observes, "Not every loss or gain of control over information about ourselves is a gain or loss of privacy."[21] Furthermore, all definitions of privacy as exercising control flounder on the fact that individuals can relinquish their own privacy by voluntarily divulging all sorts of intimate details themselves.[22] There is a loss of privacy under such circumstances but not a loss of control. Therefore, privacy cannot be identified with control.

A third, more adequate definition of privacy holds that a person is in a state of privacy when certain facts about that person are not known by others. W. A. Parent, in an important 1983 article, "Privacy, Morality, and the Law," defines privacy as "the condition of not having undocumented personal knowledge about one possessed by others."[23] By the phrase "personal knowledge," Parent does not mean all information about ourselves but only those facts "which most individuals in a given society at any given time do not want widely known."[24] It is necessary that the definition be restricted to *undocumented* personal information, because some facts that individuals commonly seek to conceal are a matter of public record and can be known without

prying into their private lives. A person does not suffer a loss of privacy, for example, when a conviction for a crime becomes known to others, because court records are public documents. Similarly, there is no loss of privacy when an easily observable fact, such as a person's baldness, is known to others, even if the person is sensitive about it and prefers that others not be aware of it.

In the remaining discussion, the concept of privacy is limited to matters involving information and, in particular, to the access of others to undocumented personal information, as described by Parent. The two other definitions—as a right to be let alone and to have control over information about ourselves—confuse privacy with other values. Having gained some understanding of the concept of privacy, we can now turn to the question of why privacy is a value.

Utilitarian Arguments

Why do we value privacy so highly and hold that it ought to be protected as a right? Certainly, we desire to have a sphere of our life in which others do not possess certain information about us. But the mere fact that we have this desire does not entail our having a right of privacy; nor does it tell us how far a right of privacy extends. Some arguments are needed, therefore, to establish the value of privacy and the claim that we have a right to it. Most of the arguments developed by philosophers and legal theorists fall into one of two categories. One category consists of utilitarian arguments that appeal to consequences, and the second is Kantian arguments that link privacy to being a person or having respect for persons. To a great extent, these two different kinds of arguments express a few key insights about privacy in slightly different ways.

One of the consequences cited by utilitarians is that great harm is done to individuals when inaccurate or incomplete information collected by an employer is used as the basis for making important personnel decisions. The lives of many employees have been tragically disrupted by groundless accusations in their personnel records, for example, and the results of improperly administered polygraph and drug tests. Even factual information that ought not to be in an employee's file, such as the record of an arrest without a conviction, can cause needless harm. The harm from these kinds of practices is more likely to occur and to be repeated when employees are unable to examine their files and challenge the information (or misinformation) in them.

A drawback to this argument is that it rests on an unproved assumption that could turn out to be false. It assumes that on balance more harm than good will result when employers amass files of personal information, use polygraph machines, conduct drug tests, and so on. Whatever harm is done to employees by invading their privacy has to be balanced, in a utilitarian calculation, against the undeniable benefits that these practices produce for both employers and employees.

Furthermore, the argument considers only the possible harmful consequences of privacy invasions. However, some practices, such as observing workers with hidden cameras and eavesdropping on business conducted over the telephone, are generally considered to be morally objectionable in themselves, regardless of their consequences. Honest workers, for example, have nothing to fear from surveillance that is designed to protect against employee theft, and indeed the use of hidden cameras in a warehouse can even benefit those who are honest by reducing the possibility of false accusations. Still, workers have a right to complain that secret surveillance of their activities on the job violates the right of privacy. It is the fact that they are subjected to constant observation and not any possible consequence of being observed that is morally objectionable.

ignore

EXPANDING THE SCOPE OF CONSEQUENCES. This objection is avoided by more sophisticated utilitarian arguments that do not locate the harmful consequences solely in the harm that occurs when information is misused. According to these arguments, a certain amount of privacy is necessary for the enjoyment of some activities, so that invasions of privacy change the character of our experiences and deprive us of the opportunity for gaining pleasure from them. Monitoring and surveillance in the workplace, for example, affect job satisfaction and the sense of

dignity and self-worth of all workers. They send a message to employees that they are not trusted and respected as human beings, and the predictable results are a feeling of resentment and a decline in the satisfaction of performing a job.

An illustration of this point is provided by a truck driver with 40 years' experience with the Safeway Company who reports that he used to love his job because "you were on your own—no one was looking over your shoulder. You felt like a human being." After the company installed a computerized monitoring device on his truck, he decided to take early retirement. He complains, "They push you around, spy on you. There's no trust, no respect anymore." A directory-assistance operator reported, "I've worked all those years before monitoring. Why don't they trust me now? I will continue to be a good worker, but I won't do any more than necessary now."[25]

ignore

PRIVACY AND IDENTITY. Some writers argue that privacy is of value because of the role it plays in developing and maintaining a healthy sense of personal identity. According to Alan F. Westin, privacy enables us to relax in public settings, release pent-up emotions, and reflect on our experiences as they occur—all of which are essential for our mental well-being. A lack of privacy can result in mental stress and even a nervous breakdown.[26] Another common argument appeals to the importance of privacy in promoting a high degree of individuality and freedom of action among the members of a society. Critics of these arguments object, however, that there is little evidence that privacy has the benefits claimed for it or that the predicted harm would follow from limiting people's privacy.[27] Many societies function very well with less room for solitude than our own, and the experiences of human beings in prisons and detention camps are cited by critics to refute these arguments.

Kantian Arguments

Two Kantian themes that figure prominently in defense of a right to privacy are those of autonomy and respect for persons. Stanley I. Benn, for example, notes that utilitarian arguments for a right of privacy are not able to show what is morally wrong when a person is secretly observed without any actual harm being done. "But respect for persons," Benn claims, "will sustain an objection even to secret watching, which may do no actual harm at all." The reason, he explains, is that covert spying "deliberately deceives a person about his world," which hinders his ability to make a rational choice.[28] Benn's argument thus appeals to both Kantian themes by arguing that invading a person's privacy violates the principle of respect for persons *and* prevents a person from making a rational choice as an autonomous being.

Hyman Gross argues in a similar vein that what is morally objectionable about being observed unknowingly through a hidden camera or having personal information in a data bank is that a person loses control over how he or she appears to others.[29] If people form incomplete or misleading impressions of us that we have no opportunity to correct, then we are denied the possibility of autonomous or self-directed activity, which is a characteristic of human beings. Hence, invasions of privacy diminish an essential condition for being human.

In a very influential discussion, Charles Fried argues that privacy is of value because it provides a "rational context" for some of our most significant ends, such as love, friendship, trust, and respect, so that invasions of privacy destroy our very integrity as a person.[30] The reason that privacy is essential for respect, love, trust, and so on is that these are intimate relations, and intimacy is created by the sharing of personal information about ourselves that is not known by other people. In a society without privacy, we could not share information with other people (because they would already know it), and hence we could not establish intimate relations with them. Thus, monitoring, in Fried's view, "destroys the possibility of bestowing the gift of intimacy, and makes impossible the essential dimension of love and friendship."[31] Similarly, trust cannot exist where there is monitoring or surveillance, because trust is the expectation that others will behave in a certain way without the need to check up on them.

The arguments of Benn, Gross, Fried, and others seize upon important insights about the value of privacy, but many critics have found flaws in the details of their arguments. Jeffrey H. Reiman, for one, objects that it is too strong to assert that all instances of people being watched unknowingly result in deceiving people and depriving them of a free choice. Otherwise, we would be violating people's right of privacy by observing them strolling down a street or riding a bus.[32] Intimate relations such as love and friendship do not consist solely in the sharing of information but involve, as one writer says, "the sharing of one's total self—one's experiences, aspirations, weaknesses, and values."[33] Consequently, these relations can exist and even flourish in the absence of an exclusive sharing of information.

The Role of Privacy in Socialization

Several philosophers have suggested that the key to a more satisfactory theory of privacy can be constructed by understanding the way in which individuals are socialized in our culture.[34] Privacy, in the view of these philosophers, is neither a necessary means for realizing certain ends nor conceptually a part of these ends. Nevertheless, we are trained from early childhood to believe that certain things are shameful (e.g., public nudity) and others strictly our own business (e.g., annual income). There is no intrinsic reason why our bodies or our financial affairs should be regarded as private matters. People at different times and places have been socialized differently with regard to what belongs to the sphere of the private, and we might even be better off if we had been socialized differently. Still, we have been socialized in a certain way. In our culture, certain beliefs about what ought to be private play an important role in the process by which a newborn child develops into a person and by which we continue to maintain a conception of ourselves as persons.

This argument is broadly utilitarian. The consequences that it appeals to, however, are not the simple pleasures and pains of classical utilitarianism or even the notions of mental health and personal growth and fulfillment of more sophisticated utilitarian arguments. The argument goes deeper by appealing to the importance of privacy for personhood, a concept that is more commonly used by Kantian theorists. Unlike Kantian arguments, though, this one recognizes that privacy is not necessary for all people in all times and places but is merely a value specific to contemporary Western culture. There are societies that function very well with less privacy than we are accustomed to; however, given the role privacy plays in our socialization process, a certain amount is needed for us to develop as persons and have a sense of dignity and well-being.

Both utilitarian and Kantian arguments point to a key insight: Privacy is important in some way to dignity and well-being. They claim too much, however; privacy is not absolutely essential to either one, except insofar as we have come to depend on it. For better or worse, privacy has become an important value in our culture, and now that it has, it needs to be maintained. Privacy is like the luxury that soon becomes a necessity, but "necessary luxuries" are not less valuable just because we could formerly get by without them. The justification of privacy just offered is thus the most adequate one we have.

THE PRIVACY OF EMPLOYEE RECORDS

The arguments in the preceding section show that privacy is of such sufficient value that it ought to be protected. There are many instances, however, in which other persons and organizations are fully justified in having personal information about us and thereby in intruding into our private lives. The task of justifying a right of privacy, then, consists not only in demonstrating the value of privacy but also in determining which intrusions into our private lives are justified and which are not.[35]

As an example, consider the issues that must be addressed in developing the case for a right of privacy in employee records and in formulating a company privacy protection plan for these records. Among the issues are the following:

1. The kind of information that is collected.
2. The use to which the information is put.
3. The persons within a company who have access to the information.
4. The disclosure of the information to persons outside the company.
5. The means used to gain the information.
6. The steps taken to ensure the accuracy and completeness of the information.
7. The access that employees have to information about themselves.

The first three issues are closely related, because the justification for an employer's possessing any particular kind of information depends, at least in part, on the purpose for which the information is gathered. Some information is simply of no conceivable use in company decision making and constitutes a gratuitous invasion of employee privacy. It is more often the case, however, that an employer has a need or an interest that provides some justification for intruding into the private lives of employees. An invasion of employee privacy is justified, however, only when the information is used for the intended purpose by the individuals who are responsible for making the relevant decisions.

Companies are generally justified in maintaining medical records on employees in order to administer benefit plans, for example, and to monitor occupational health and safety. If these are the purposes for which a company gathers this kind of information, then it follows that (1) only medical information that is essential for these purposes can be justifiably collected; (2) only those persons who are responsible for administering the benefit plans or monitoring the health and safety of employees are justified in having access to the information; and (3) these persons must use the information only for the intended purposes. There are three corresponding ways in which employees' right of privacy can be violated. These are when (1) personal information is gathered without a sufficient justifying purpose; (2) it is known by persons who are not in a position that is related to the justifying purpose; and (3) persons who are in such a position use the information for other, illegitimate purposes.

WHAT JUSTIFIES A PURPOSE? Obviously, the notion of a justifying purpose plays a critical role in determining the exact scope of the right of privacy in employment. There is considerable room for disagreement on the questions of whether any given purpose is a legitimate one for a business firm to pursue, whether a certain kind of information is essential for the pursuit of a particular purpose, and whether the information is in fact being used for the intended purpose. Companies have an interest and, indeed, an obligation to ensure that employees are capable of performing physically demanding work and are not subjected to undue risk, for example. The purposes for which Henry Ford created the Sociological Department, however, went beyond this concern to include a paternalistic regard for the general welfare of his employees, which is not a legitimate purpose. Even to the extent that the work of the inspectors from the Ford Motor Company was justified by a legitimate purpose, there could still be an objection to the excessive amount of information they sought. Information about the handling of finances, church attendance, and eating and drinking habits is more than the company needed to know.

Determining the purpose for which information is being used can raise difficult questions about intentions. A controversy was sparked in 1980, for example, when it became publicly known that the DuPont Company was routinely screening black applicants at a plant in New Jersey for signs of sickle-cell anemia. The company asserted that the purpose for conducting the screening was to protect black workers, because carriers of the disease, who are mostly black, were thought to be more vulnerable to certain chemicals used at the plant. Such a purpose is arguably legitimate, but some critics of DuPont charged that the company was actually using genetic screening for another purpose, namely to prevent liability suits and to avoid having to protect workers from dangerous chemicals.[36]

RESOLVING DISAGREEMENTS ABOUT PURPOSE. Is there any way in which the notion of a justifying purpose can be clarified so that such disagreements can be resolved? One possibility is to specify the conditions necessary for a business to conduct normal operations. In order to do this, a company must be able to assess the suitability of applicants for employment, supervise their work-related behavior, administer fringe-benefit plans, and so on. In addition, employers must be

able to acquire the information necessary for complying with legal requirements about taxes, social security, discrimination, health and safety, and the like. As a result, employers are justified in asking potential employees about their educational background, past employment, and so on, but not, for example, about their marital status, because this information is not necessary in order to make a decision about hiring. Once employees are hired, a company may have a need to inquire about marital status in order to determine eligibility for medical benefits, but only if the employee in question chooses to participate in a medical insurance plan. Even then, this information should be used only for the purpose of determining eligibility for medical benefits.

Joseph R. DesJardins suggests that questions about the extent of the right of privacy in the workplace can be settled by appealing to a contract model of the employer–employee relationship.[37] Viewing employment as a contractual relation between an employer and an employee provides a basis for granting a set of rights to both parties, because the validity of contracts requires that certain conditions be satisfied. Contracts are valid, first, only if they are free of force and fraud. As a result, an employer has a right to require applicants to provide enough information to make an informed decision about hiring and to submit to tests for measuring relevant aptitudes and skills. Once hired, employees have an obligation to permit employers to monitor work performance, for example, and to gather whatever information is necessary to maintain an ongoing contractual relation.

Second, valid contracts also require mutual voluntary consent, so a contract model of employment would not permit employers to collect information without the knowledge and permission of the employees affected. Covert searches, surveillance by hidden cameras, the use of private investigators, and so on would be incompatible with the view of employment as a contractual relation. Similarly, objections could be raised to employer demands that employees either submit to drug tests and interrogation with a polygraph machine or be dismissed, because an employee has little choice but to comply. Union contracts in which employees are able to exercise effective choice often contain provisions prohibiting such practices.

Disclosure to Outsiders

The fourth issue—concerning the disclosure of personal information to persons outside a company—arises because of the practice, once very common, of employers sharing the content of personnel files with landlords, lending agencies, subsequent employers, and other inquiring persons without the consent of the employees involved. Even when there is a legitimate purpose that would justify these various parties having the information, it can be argued that an employer has no right to provide it, because the employer is justified in collecting and using information only for purposes connected with the employer–employee relationship. What is morally objectionable about an employer's disclosing personal information to an outside party, in other words, is not necessarily that the outside party is not justified in having it but that the employer has no justification for giving it out.

Thus, medical records collected by a former employer ought not to be passed along to a subsequent employer without the employee's consent. The former employer presumably had a purpose that justified the gathering of that information, and the new employer might also have a similar purpose in gathering the same information. But with the former employer, the information pertains to that employment relation, and can be justifiably used only for purposes connected with it. The subsequent employer must proceed in the same way as the former employer.

This argument points up an important difference between personal information and other kinds of corporate records. Databases of various kinds are generally regarded as resources that are *owned* by a company. Ownership, however, generally entails an exclusive and unrestricted right of access and control, which employers do not have with respect to personal information. A mailing list, for example, is a kind of property that a company can use in any way it pleases, with no restrictions. Medical records, by contrast, can be compiled by a company only for a specific purpose, and any use unrelated to this purpose is prohibited. The fact that employers bear a burden of proof for justifying the collection and use of personal information shows that the notion of ownership is inappropriate in this case.[38]

It is also inappropriate to describe the information in personnel files as belonging to employees, because they relinquish some rights to it by virtue of entering into the employment relation. Neither an employer nor an employee, therefore, can be said to own the information in a company's personnel files. Such information is simply not property in the usual sense, unlike other kinds of data gathered by corporations. It is necessary, therefore, to develop a conceptual model for personal information other than that of ownership.

The Means Used to Gather Information

Justifying the means used to gather information, which is the fifth issue, involves a different set of considerations. Use of certain means may violate an employee's right of privacy, even when the information gathered is of a kind that an employer is fully justified in possessing. Examples of impermissible means are polygraph testing and pretext interviews. (Pretext interviews are inquiries made under false pretenses, as when an employer seeks information from an applicant's family while posing as a market researcher.) Even if employers are justified in asking certain questions on a job application, they are not, for that reason, justified in using a polygraph machine or a pretext interview to verify the accuracy of a person's responses.

A major consideration in evaluating the means used to gather information is whether less intrusive means are available. In general, less intrusive means are morally preferable to those that are more intrusive. Employers are justified in seeking information about drug use by employees in the workplace, for example, but such means as searches of lockers and desks, hidden cameras in rest rooms, random drug tests, and the like are not justified when sufficient information could be gathered by less intrusive means, such as closer observation of work performance and testing only for cause. (Some means are not justified, of course, even if less intrusive means are not available. Hidden cameras and random drug tests are possible examples.)

What makes some means more intrusive than others depends on several factors. Such practices as conducting strip searches and watching while a urine sample is produced involve an affront to human dignity. An objection to constant monitoring, personality tests, and the use of polygraph machines is that they collect more information than is necessary and that they collect it indiscriminately. Honesty tests, for example, often inquire into personal habits and interests, family relations, and sexual adjustment—matters that are extraneous to the ostensible purpose.[39] Improperly administered polygraph tests can easily become "fishing expeditions," which result in the revelation of information that an employer is not justified in having.

Another reason why some practices such as monitoring and surveillance by hidden cameras and polygraph testing are unusually intrusive is that they deprive persons of an opportunity to exercise control over how they appear to others, which is essential for being an autonomous individual. An employee who is unaware of being observed, for example, might be unwittingly led to reveal facts that he or she would otherwise keep from others. George G. Brenkert argues, very perceptively, that because a polygraph machine measures physical characteristics such as breathing rate, perspiration, and blood pressure over which we have little or no control, it "circumvents the person" and undercuts the "way by which we define ourselves as autonomous persons."[40] As a person, one can shape how one appears to others and create an identity for oneself. A machine that registers involuntary responses denies people the power to do that.

Accuracy, Completeness, and Access

The last two issues are concerned primarily with matters of fairness. If the information in personnel files and other corporate databases is going to be used to make critical decisions about wage increases, promotions, discipline, and even termination of employment, then it is only fair that the information be as accurate and complete as possible and that employees have access to their personnel files so that they can challenge the contents or at least seek to protect themselves from adverse treatment based on the information in them.

Employers who maintain inaccurate or incomplete files and deny employees access to them are not invading the privacy of their employees, as the concept of privacy is commonly defined. What is at issue is not the possession of personal information by an employer but its use in ways that are unfair to employees. The right that employers violate is a right of fair treatment, which is not the same as a right of privacy. Still, because these issues are involved in the handling of personal information, they must be considered in devising policies or laws dealing with employee privacy.

Another objection to drug tests and polygraph machines is their unreliability. A number of factors, including the use of prescription drugs and careless laboratory work, can result in false positives, especially in simpler, less-expensive drug tests. Polygraph machines are inherently unreliable, because they register only bodily responses and not the mental experience that triggers them. An investigator might conclude that a subject is lying when the responses recorded by the machine are actually due to a different kind of association. One study, in which 14 polygraphers were asked to evaluate the charts of 207 criminal suspects, found that 50 percent of the experts thought that innocent suspects gave deceptive answers and 36 percent of them considered the guilty suspects to be telling the truth.[41] After a review of the studies to date, the U.S. Office of Technology Assessment concluded in 1983 that polygraph testing was useless for screening in preemployment contexts.[42]

In summary, determining the exact limits of the right of employees to privacy in the workplace requires that we address a number of issues. Questions about four of these issues—those concerning the kind of information collected, the use to which it is put, and the persons both inside and outside the company who have access to it—can be answered largely by appealing to the notion of a legitimate purpose. The issue of the means used to gain information involves different questions about whether some means are inherently objectionable and whether others are objectionable because less-intrusive means are available. Finally, the remaining issues involve the fair treatment of employees, which is not, strictly speaking, part of a right of privacy but is still related to the handling of personal information.

PRIVACY ON THE INTERNET

Imagine that most of the stores you entered created a record of your visit including not only your purchases but also what merchandise you looked at, how long you took, what route you followed through the store, what other stores you had visited, and what you bought there. Imagine further that, in many instances, the store could connect this information with your name, address, telephone number, and perhaps your age, income level, and lifestyle. You would probably have the feeling that your shopping activity was being closely scrutinized and that you lacked virtually any privacy while browsing.

This situation, which most people would find alarming in a shopping mall, is routine on the Internet. A 1999 study found that 92.8 percent of the websites surveyed collected at least one piece of personal information, such as name and e-mail address, and 56.8 percent collected at least one type of demographic data, such as age, gender, or zip code. Only 6.6 percent of these sites collected no information.[43] Some information is provided *overtly* by the user as a condition of making a purchase or gaining access to Web pages. Other information is obtained *covertly*, without the user's knowledge or consent.

The most common method for obtaining information covertly is the installation of a "cookie," which is a file placed on a user's hard drive that recognizes a repeat user and stores information from past visits. Cookies benefit users by eliminating the need to enter information each time, but they can also provide the site owner with "clickstream" data about what pages are visited and how much time is spent on each one. Because cookies identify only a user's computer (by tagging it with a unique number), this tool is considered to preserve anonymity. However, personal information can be obtained by combining cookie data with larger databases that identify and profile individuals. Once users are identified, site owners can share the information derived from cookies to form more complete profiles in a process know as "cookie synchronization."

A Boston technology company called Pharmatrak places cookies on the computers of visitors to the health-information pages of pharmaceutical companies and records the kind of information they seek.[44] If this information could be combined with individual names, then drugs could be marketed to Web users with specific ailments. To date, Pharmatrak has not taken this extra, morally questionable step, but another company, DoubleClick, aroused a storm of protest when it proposed something similar. DoubleClick, which places banner ads on 1,500 websites using profiles based on information from cookies, purchased Abacus Direct Corporation, which has personal information on more than 80 million households. By merging the two databases, DoubleClick could tailor the banner ads on a website to match the user's purchasing preferences. Stung by vociferous protests, the company announced that it would wait until government and industry agreed on standards.[45] However, one observer said that although the industry was letting DoubleClick take the heat, the company is "not doing anything that anyone else isn't doing."[46]

The explosive growth of the Internet as a consumer marketplace is a benefit to consumers and businesses alike. The success of websites depends crucially on the collection of information. One reason is that anonymous sales with cash are not possible. Furthermore, sites that offer free content depend on advertising, and advertising space is much more valuable if it can be tailored to individual users. However, the collection of information on the Internet appears to pose threats to users' privacy. So we need to ask, first, what is the danger? What harm, if any, is done by websites collecting information? Are any rights violated? Second, given the need for government regulation or industry self-regulation, what standards should be applied, and what should be the goal in setting standards? Finally, by what means should these standards be implemented? A variety of organizations have already been formed to offer resources for developing privacy policies and to certify compliance by awarding seals of approval.

What's Wrong with Information Collection?

Although consumers may feel a lack of privacy when browsing the Internet, is this feeling well-grounded? Scott McNealy, the chairman and CEO of Sun Microsystems, once remarked, "You have zero privacy anyway. Get over it!"[47] Much of the information compiled is publicly available; the Internet only makes its compilation easier and cheaper than in the past. Store owners, if they wish, could follow consumers around to see what merchandise they examined. Computers do not observe us without our knowledge or intrude into our private lives the way psychological tests or hidden cameras do. The Internet is arguably a public arena, so being online is like walking and talking in the town square. The use to which the information is put is primarily to sell us something. Although fraud is a serious concern, we seek mainly to avoid the annoyance of advertising on the Internet.

If privacy is defined as control over personal information or the dissemination of personal information without our consent, then the practices of Internet companies violate our rights. However, this position assumes that we "own" the information about ourselves and thus have a right of control. Moreover, we give up a great deal of information in order to enjoy the benefits of Internet commerce, and so perhaps some loss of privacy is a trade-off that we voluntarily make. So, following Scott McNealy's advice, should we get over it?

The noted expert Lawrence Lessig, in his important book *Code and Other Laws of Cyberspace*, raises two problems that are unique to computers and the Internet.[48] One risk for Lessig is that our initial contacts with information gatherers form a profile of who we are, and this profile will fit us into a particular mold, which may not be accurate to begin with and may inhibit our ability to change and grow. Lessig writes, "The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins anew."[49] If we develop by selecting from the options available to us, then the choice of options is critical. In life apart from the Internet we can

always seek out new options, but to the extent that we are bound on the Internet by the options presented to us, our possibilities for growth are limited.

Lessig's second risk is that information collection by computers, especially on the Internet, could undermine the traditional American value of equality. The American Revolution was in part a rejection of European society in which innumerable distinctions of rank divided people. According to Lessig, "An efficient and effective system for monitoring makes it possible once again to make these subtle distinctions of rank. Collecting data cheaply and efficiently will take us back to the past."[50] For example, by means of frequent flyer programs, airlines identify their better customers and offer them special treatment. Companies with 800 numbers recognize the telephone numbers of favored customers and put them at the head of the queue. As a result, some people suffer a form of discrimination in which they do not get a flight on standby or endure long waits on the telephone. Businesses have always provided better service to select customers, but any discrimination was limited by the cost of the information. Lessig observes, "Whereas before there was relative equality because the information that enabled discrimination was too costly to acquire, now it pays to discriminate."[51]

Neither of these concerns involves privacy per se; the first affects autonomy, the second, equality. Moreover, the effect may be slight and insignificant. Perhaps Lessig's greatest insight is that the way in which technology is configured, specifically the way in which computer code is written, has social consequences. Furthermore, to the extent that computer code has consequences, it can be rewritten so as to achieve more desirable results. One of the solutions discussed later is Lessig's suggestion that we develop special software that will act as an electronic butler, negotiating with websites the kind of privacy protection that we desire.

Principles for Protecting Privacy

The appropriate standards or principles that should be applied to information gathering on the Internet depend on what we want to achieve or avoid. Three camps can be identified.[52] Those who worry about a "dossier" society, in which every facet of our lives is available to those with power, want strict limits on the kinds and amounts of data collected and on the availability of these data. Those who view personal data as a kind of property that can be "traded" in a market for certain benefits want to ensure that consumers do not trade too cheaply and that this valuable commodity is fairly priced. In the view of this camp, personal information is currently too "cheap" and hence is being overutilized.

The dominant camp consists of people in industry, government, and public interest groups who want to balance people's concerns about privacy—well-founded or not—with the growth of the Internet as a consumer marketplace. They seek to provide consumers with a voice in the development of this important commercial medium. The danger is that the Internet will firmly fix some practices before the public is aware of what is happening. Their goal is primarily to prevent the most egregious abuses by developing standards or principles that safeguard consumers.

In 1972, the Department of Health, Education, and Welfare developed guidelines for its own handling of information called "fair information practices," which formed the basis for much subsequent action. In 1980, the Organization for Economic Cooperation and Development (OECD) adopted a set of guidelines that underpin most international agreements and self-regulatory policies of multinational corporations. The European Parliament adopted the European Union Privacy Directive, which took effect on October 25, 1998. This law binds not only member countries but also nonmember states doing business in the European Union. Already some major American multinational corporations are being investigated for violations of the EU Privacy Directive. Although many American laws address various aspects of Internet privacy, the United States has preferred a piecemeal legal response instead of adopting an omnibus piece of legislation like the EU Privacy Directive. The Federal Trade Commission, in particular, has attempted to protect Internet privacy by using various consumer-protection laws. Principles of privacy on the Internet have also been developed by industry associations, such as the Online

Privacy Alliance (OPA), and public interest groups, most notably the Electronic Privacy Information Center (EPIC).

Despite this great diversity of sources, a remarkably similar set of standards has emerged. The Federal Trade Commission list of five principles is representative of the many documents on Internet privacy.

1. *Notice/Awareness*. Disclose the identity of the collecting party, the information collected, the means for collecting it, and the uses to which the information will be put. This notice usually consists of a privacy policy that should be prominently displayed and easily understood. Ideally, the home page and every page that asks for information should include a link to the policy. Notice should also be given if the privacy policy is not the same for all linked sites or if data will be shared with other parties with different policies.

2. *Choice/Consent*. Provide a mechanism for choosing whether to allow information to be collected. The mechanism may either require explicit consent (opt-in) or assume consent if a person takes no action (opt-out). One could choose to permit the collection of some information (name and address, for example) but not other (e.g., medical information), or one could consent to some uses of information (to select banner ads, for example) but not others (e.g., providing information to a third party).

3. *Access/Participation*. Allow consumers access to the information collected about them and the opportunity to contest the accuracy or completeness of the data. The right of access may exclude information that a company collects from sources other than the website and any results from processing website data.

4. *Integrity/Security*. Inform users of the steps taken to protect against the alteration, misappropriation, or destruction of data and of the action that will be taken in the event of a breach of security. Also, maintain information so that it is accurate and up-to-date.

5. *Enforcement/Redress*. Assure consumers that the company follows responsible information practices and that there are consequences for failing to do so. Consumers should also have some means for resolving disputes and for receiving an appropriate remedy. One way to ensure enforcement and redress is by contracting with an organization that monitors and certifies the information practices of websites.

Although substantial agreement exists on these five principles, much depends on their interpretation and implementation. In particular, how stringently should the principles be interpreted, and what are the most effective and efficient means for implementing them? Other questions include the responsibility of internet service providers (ISPs). For example, Yahoo! was criticized for revealing to the navy the identity of a sailor who used the pseudonym "Boysrch" in gay chat rooms. (The navy used this information in an attempt to oust the sailor from the service for homosexuality.) The principles do not specify whether they apply to information that websites acquire from sources other than the Internet which are then aggregated with data obtained from users. The most contentious issues are whether the weaker opt-out provision is satisfactory in most instances and in what cases, if any, opt-in ought to be required. Finally, few proposals have been developed for handling enforcement and redress.

Implementing Internet Privacy

Principles are of little value if they cannot be successfully implemented, and the Internet presents unique challenges for implementation. Its decentralized, democratic structure makes centralized, authoritarian approaches ineffective, as does its global reach. Because the Web is worldwide, so too must be any successful regulatory scheme. Although government regulation, as represented by the EU Privacy Directive, creates a powerful incentive to protect privacy, laws must still grapple with the difficult question of the appropriate means. In considering the

problem of protecting Internet privacy, we must ask, first, who should be involved and, second, what means should be used?

Obviously, the principal parties are Internet firms (websites and ISPs), computer companies (both hardware and software suppliers), industry associations, governments and regulatory agencies, public interest groups, and, of course, individual users. The main approach to date has focused on government regulation and self-regulation by the industry, designed in large part to prevent further intrusion by government. Self-regulation has largely taken the form of developing privacy policies and, in some instances, creating the post of chief privacy officer (CPO) to direct company efforts. In this task, websites have been aided by public interest groups which offer resources and certification. Organizations, such as TRUSTe and BBBOnline (a service of the Council of Better Business Bureaus), monitor a firm's compliance with its privacy policy and award a seal that can be displayed on its website.

The most effective solution to a problem created by runaway technology might very well be more technology. We can protect privacy through both *formal* and *material* means.[53] Regulation and certification as described earlier utilize rules or norms that are designed to influence behavior. Such formal means can be supplemented with changes in material conditions that prevent certain kinds of behavior. Although we need laws against theft (formal), we also protect property with locks (material). The suggestion, then, is that we develop technology that will enable Internet users to protect their privacy to the extent they desire. To be effective, this technology must be usable by even the most unsophisticated in order to overcome the problem of the "blinking twelve" (which refers to the number of people who cannot even set the clock on a VCR).

A material solution consists in the development of various privacy enhancing technologies (PETs). Among such means are services that permit "proxy surfing" by hiding the identity of the user's computer and remailers that forward e-mail stripped of any identifying markers. Cookie-management software exists that can block or disable cookies. Intel caused controversy by encoding a unique Processor Serial Number (PSN) in its Pentium III processor, but the company later offered software that would enable a user to suppress this number.[54] These PETs are likely to be used, however, only by very sophisticated users, and so we encounter the "blinking twelve" problem.

The most promising technology follows Lessig's suggestion of creating an electronic butler or a Cyber-Jeeves. This is a software program that would allow a user to answer a few questions about the desired features of a website's privacy policy and then determine whether sites to be visited fit the user's preferences. Such software is the goal of the Platform for Privacy Preferences Project (P3P), which is being conducted by the World Wide Web Consortium. If installed on most personal computers, a Cyber-Jeeves would force websites to adopt the privacy policies that the majority of Internet users desire.

Conclusion

Although privacy is a relatively recent concept—dating in American law to the 1890s—public concern is clearly increasing, primarily in response to privacy-invading technologies. The problems facing employees, consumers, and Internet users are similar, as are the solutions. There is greater agreement, however, on the ends than on the means, but even the ends are in dispute. Americans say that they value privacy, and yet they give up a great deal for convenience and material gain. Without question, the technologies that threaten privacy have brought us many benefits. Finding the right means is a great challenge to business firms which must meet employee and consumer expectations as they utilize new technologies. More than many business ethics problems, protecting privacy requires a coordinated solution involving many parties. Until a solution is found, though, the focus of businesses will remain on developing and implementing privacy policies.