HM 331:1.2001

Computer Privacy and the Modern Workplace

RABBIS ELLIOT N. DORFF and ELIE KAPLAN SPITZ

Part I: Intrusion

This paper was approved by the CJLS on March 13, 2001, by a vote of 16 in favor, 0 opposed and 6 abstaining (16-0-6). Voting in favor: Rabbis Kassel Abelson, Ben Zion Bergman, Elliot N. Dorff, Paul Drazen, Jerome M. Epstein, Baruch Frydman-Kohl, Nechama D. Goldberg, Arnold M. Goodman, Judah Kogen, Aaron L. Mackler, Daniel S. Nevins, Joel E. Rembaum, James S. Rosen, Joel Roth, Elie Kaplan Spitz, and Gordon Tucker. Abstaining: Rabbis Eliezer Diamond, Myron S. Geller, Alan B. Lucas, Paul Plotkin, Mayer Rabinowitz, and Avram Israel Reisner.

Part II: Disclosure

This paper was approved by the CJLS on March 13, 2001 by a vote of 15 in favor, 0 opposed and 7 abstentions (15-0-7). Voting in favor: Rabbis Kassel Abelson, Elliot N. Dorff, Paul Drazen, Jerome Epstein, Baruch Frydman-Kohl, Nechama Goldberg, Arnold M. Goodman, Judah Kogen, Daniel S. Nevins, Avram Israel Reisner, Joel E. Rembaum, James S. Rosen, Joel Roth, Elie Kaplan Spitz, and Gordon Tucker. Abstaining: Rabbis Ben Zion Bergman, Eliezer Diamond, Myron S. Geller, Alan B. Lucas, Aaron L. Mackler, Paul Plotkin, and Mayer E. Rabinowitz.

Introduction: The Urgency of the Questions.

A Wall Street Journal poll conducted in the Fall of 1999 asked Americans what they feared the most in the new millennium. Privacy loss came out on top (29%), substantially higher than terrorism, global warning, and overpopulation (none higher than 23%).[1] The intense concern over privacy is relatively new. While in 1970 only 34% of people in a Lou Harris-Alan Westen privacy poll were concerned about threats to personal privacy, 88% of people surveyed had such a fear in 1998.[2] This increased fear of privacy loss is due largely to the growing use of computers, with their powerful ability to gather fragments of information and disseminate that information quickly and widely.

Among the important issues in the raging debate over privacy is an employer's right to monitor employees' e-mail, a rapidly growing practice in the workplace. In a 1993 survey of major companies, MacWorld estimated that 22% of the workers of companies surveyed, or twenty million employees, were subject to some type of electronic monitoring while on the job.[3] A survey of nearly a thousand large companies in 1999 by the American Management Association found that 45% monitored the e-mail, computer files or phone calls of their workers, up from 35% two years earlier.[4]

Many employees do not realize that e-mail messages, even when deleted, are electronically stored and can be reviewed by anyone with access and the right equipment. With e-mail messages already in ASCII code, using a computer to search large numbers of e-mails for mention of particular words is as easy as searching in a document being word-processed. There are new software programs, with names like Assentor or Investigator, that are able to screen all incoming or outgoing e-mail for forbidden words and phrases and can automatically forward the suspicious messages to a supervisor for review.[5]

The pervasiveness of e-mail monitoring and the ease with which private network providers may infiltrate employees' accounts are alarming for anyone concerned with personal privacy. Yet, employers also have

rights to make sure that employees are doing their job, maintaining a work environment that is free of harassment, and not misusing the corporate name in their correspondence. Hence, a variety of questions emerge. Should private employers be allowed to have indiscriminate access to e-mail accounts on networks financed, installed, and maintained by corporate funds? Conversely, should, or do, employees have a right to privacy shielding them from this form of corporate surveillance?

There is a whole set of separate questions that emerge from the computer's ability to amass bits of information, put them together into a coherent profile, and then disseminate the information rapidly and widely. Often the party who uses a web-site is unaware that the use of their computer is being monitored, including what it is that they are seeing on the web, how much time they spend reading a page, and what they purchase. New software allows companies to profile their web-site customers, and in many cases that information is sold to third parties. People are legitimately afraid that the commercial incentives to share private information will make their lives transparent. What kind of notice should be required in the gathering of information and in its sale to a third party?

We approach these questions of intrusion and disclosure in the modern workplace through the lens of Jewish law, whose emphasis is different from that of American law. A secular system of law, such as the American system, is based on "rights" and is written for the bad person in order to maintain the basic conditions of social order. In contrast, Jewish law is grounded in "duties" with an emphasis on how a person "ought" to behave in order to be a good person.[6] Consequently, the analysis and guidance that we offer is not intended to describe the responsibilities of a person to respect people's rights before the American courts, but rather our duties before God.

In some ways, the threats to privacy posed by computers in our time resemble the hazards our ancestors faced when they sought to protect privacy, for they too were worried about intrusion and disclosure and took steps to protect people from them. Computers, though, expand the potential for intrusion and disclosure well beyond anything ever contemplated before our time. This difference of degree sometimes even rises to a difference in kind, as we find that the very nature of the privacy we can assume in our society has changed and, along with it, our own sense of identity and security. This responsum, then, seeks to address the Jewish concern for privacy in the new venue of the age of computers and the Internet in order to restate and reinforce traditional Jewish norms where they apply directly to the modern workplace and to apply Jewish beliefs, values, and laws to some of the genuinely new questions that the electronic age raises.

The Value of Privacy: A Religious Perspective

Privacy is necessary for human dignity. The loss of privacy entails the fear that others will misjudge us and even harm us by using fragments of information taken out of context. Confidence in privacy furthermore enables creativity to flourish, for when privacy is assured, nonconformist people feel sufficiently safe and protected from interference to experiment.[7] In addition, privacy is a prerequisite for the bond of friendship, which includes sharing confidential feelings and vulnerabilities.[8] A free and tolerant society needs an assurance of privacy, because each person has secrets that "concern weaknesses that we dare not reveal to a competitive world, dreams that others may ridicule, past deeds that bear no relevance to present conduct or desires that a judgmental and hypocritical public may condemn."[9]

Moral concerns such as these are central in Judaism not only because Judaism concerns itself with the relations of people with each other, but also because we are supposed to model ourselves after God. We who are "created in the image of God (Genesis 1: 27), are repeatedly directed in the Torah to follow God's ways: "You shall be holy, for I, the Lord your God, am holy" (Leviticus 19:2); "Walk in all His ways" (Deuteronomy 11:22); and "Follow the Lord your God" (Deuteronomy 13:5). The Rabbis understood these biblical verses as establishing the principle of *imitatio dei*, of modeling ourselves after God: "As God is gracious and compassionate, ...you too must be gracious and compassionate; as the Holy One is righteous, ...you too must be righteous; as the Holy One is loving, ...you too must be loving."[10] At the same time, Jewish texts depict God as

in part known and in part hidden; God is made manifest to human beings through revelation and through divine acts in history, but no human being, even Moses, can know God's essence (Exodus 3:6; 33:20-23).[11] Furthermore, the Mishnah declares that one who probes God's essence beyond what God has chosen to reveal to us should not have been born, for, as the Jerusalem Talmud explains, to know more about God than the Holy One chooses to reveal to us is an affront to God's dignity.[12]

As God keeps His own confidences, then, we too must preserve both our own privacy and that of others to enable us to be like God.[13] Moreover, since human beings are created in God's image (Genesis 1:27), when we honor God's creatures we honor God, and, conversely, degrading people is tantamount to dishonoring God.[14] Furthermore, God intends that the Israelites be "a kingdom of priests and a holy people" (Exodus 19:6), not just a nation that observes the minimal necessities of maintaining order and providing for basic needs. As the Torah specifies, to be a holy people requires, among other things, that a lender not intrude on a borrower's home to collect on a loan (Deuteronomy 24:10-11), and that nobody be a talebearer among the people (Leviticus 19:16). Thus both intrusion and disclosure are forbidden so that a person's home, reputation, and communication are all protected as part of the effort to create a holy people.

Part I: Intrusion

שאלה

Are there conditions under which employers may monitor their employees' e-mail or internet usage?

תשובה

The Prohibited Forms of Intrusion.

One category of privacy violation is intrusion, defined as the unauthorized entry into another's property or the use of that property without permission. In interpreting the biblical laws prohibiting intrusion (Deuteronomy 24:10-11), the Rabbis maintain that these laws bar not only physical trespass, but also visual penetration of a person's domain (*hezek re'iyah*). They interpret Balaam's praise of the tents of the Israelites — "How fair are your tents, O Jacob, your dwelling places, O Israel," (Numbers 24:5) — as arising from his observation that the Israelite tents were so situated that the tent openings did not face each other. The Rabbis thus insist that two joint landowners contribute equally to erect a wall between their respective halves of the property to serve as a deterrent to visual intrusion, and they prohibit making a hole in the wall opposite the neighbor's window. They also deny the option to either or both parties to waive their rights to this protection of their mutual privacy because the wall was not only supposed to safeguard the privacy of each party but was also intended to deter each one from the temptation to intrude on the other.[15]

In the Middle Ages, when the mail system expanded, Rabbenu Gershom (Mayyence, Germany, 960-1028) issued a decree prohibiting mail carriers and others from reading other people's mail lest they learn trade secrets or spread gossip. According to the decree, violators would be subject to excommunication even if they did not publicize the improperly read letter. Privacy was thus recognized as an important value in its own right apart from its importance in protecting people from harm.[16] Moreover, intrusion, as understood in Jewish sources, is thus not limited to forbidden entry (physical, visual, or aural) into another person's property or personal space, but also forbidden use of what one learns when one does that: I may not read another person's letter without permission, and, if I do, I may not tell anyone else the contents. That is, intrusion includes the prohibitions against unauthorized entry (Deuteronomy 24 and the Rabbinic extension of that to *hezek re'iyah*) and also the prohibition against talebearing (*rekhilut*, cf. Leviticus 19:16).

At the same time, there are limits to the expectation of privacy in Judaism, for there are times in Jewish life when the tradition prefers the value of community togetherness over that of individual privacy. Thus, for example, invitations are not traditionally required to console mourners in their home or to enter a private dwelling to celebrate the brit milah (ritual circumcision) of a newborn boy with his parents. These moments are intended to be public because our tradition directs us to link life-cycle events with community.

Yet in daily life, we need and should have privacy. The Rabbis specifically point out, for instance, that although after the wedding the bride and groom are allowed to engage in sexual relations, the wedding guests are forbidden to mention that fact out of respect for the couple's privacy and dignity.[17] From the viewpoint of Judaism, sexual relations between husband and wife are a good thing, but a private thing. In sharp contrast to life-cycle events and to other clearly public occasions like worship, one's personal life must remain private. Thus the Rabbis, as we have mentioned, conscientiously sought to insure that people would not spy on others and that, conversely, people would value their own privacy enough to erect walls to protect it. Moreover, they insisted that we take steps to shield both parties from their temptations to intrude.

In the work place, people's expectations of privacy are, and should be, different from those in their own home. The Jewish tradition emphasizes that an employee has a clear duty to do a fair day's work.[18] To prevent employees from idling on the employer's time, Jewish law prohibits workers to stand up in deference to a rabbinic scholar while engaged at work, and Abba Hilkiah, according to the Talmud, even refused to return a greeting to a delegation of rabbinical scholars while working as a day laborer.[19] Similarly, the Talmud instituted an abridged form of Grace after Meals, dropping the fourth blessing, for day workers eating lunch in order to impinge as little as possible on the employer's time; later, though, employers customarily and voluntarily allowed their workers to add the fourth blessing, and the right to do so ultimately became an implicit condition of the employment of the day laborer.[20] Workers were also not allowed to "moon-light" or to starve themselves, even to provide food for their families, for then they could not produce a fair day's work for their primary employer.[21] Conversely, employees have the positive duty to work at their jobs with all their power, modeling themselves after Jacob who, according to the Torah, proclaimed to his wives, "You know that I worked for your father with all my strength," (Genesis 31:6).[22]

Given these provisions of Jewish law, employers have the right to monitor their employees to assure that they are not wasting time but are rather carrying out their responsibilities fairly and faithfully. As the Talmud says, "Whoever is left much money by his parents and wishes to lose it should... hire workers and not watch over them," for then the workers will either fail to plow the land properly, so that the subsequent crop is a poor one (Tosafot's explanation), or they will cause direct damage to the crops by driving the ox carts carelessly over the crops when engaged in harvesting (Rashi).[23] That is, unsupervised workers might either fail to carry out their responsibilities altogether or do so poorly. In times past, employers would simply look to see what their employees were doing. Now that many forms of work involve use of the computer and the Internet, employers need to monitor what employees do on those instruments in order to assess the quality of their employees' work. Employers do not, as a matter of course, have a right to know what their employees are thinking or writing, but employers certainly do have the right to insist that their employees spend their time at the computer on business and not on playing games or trading on the stock market for their personal benefit, for, after all, the employees are being paid to do work. Thus employers do have the right to monitor employees' use of their office computers as a corollary of their right to oversee and evaluate their employees' work.

An English journalist, Roger Dobson, recently wrote in London's *The Independent*:

> Not long ago, computer abuse at work was limited to an occasional game of minesweeper or solitaire. Not any more. The huge growth in internet use means thousands of employees are doing myriad private jobs online, from trading stock and placing bets, to researching their children's homework…. As much as 59 per cent of internet use at the office is estimated as not work-related. And, as a result of all this inappropriate use, increasing numbers of employees are being sacked for unwarranted internet abuse.[24]

How shall we balance the employee's right to privacy with the employer's right to a fair day's work? In order to clarify expectations, employers should notify employees of their intent to monitor the use and

content of what their employees do on their office computer. Without such notification, employees could easily infer an expectation of privacy at work, especially because the employer arranges for the employee to have a personal password to gain access to the company's system. To avoid any misunderstanding, an employer who plans on monitoring employees' internet usage and e-mail should provide employees, at the time of hiring, with both an oral and a written notice of company policy about this matter. The notice should state that computers are company property intended for business purposes. The employer will therefore retain the right of access to all written messages on the system and will monitor employees' use of the computers to advance the company's legitimate business interests. Employers should also insist at that time that candidates for employment sign a copy of this policy, acknowledging that they understand that they can have no legitimate expectation of privacy when using their company computers. That way employees will have ample knowledge ahead of time as to whether or not they can reasonably expect protection from intrusion in their use of the office computer, e-mail facilities, and internet access.[25] Employers should also specify both orally and in writing at the time of hiring an employee whether personal use of company machines is totally forbidden or allowed for given purposes and given amounts of time. This written notice should include the company policy on personal use not only of the computer, but also of the telephone, fax, and copy machine. That way the lines between legitimate use and theft will become clear.

Conversely, employees who use office equipment for personal communications must take steps to insure that nothing private is seen or heard by others. After all, Jews have the duty to protect themselves from intrusion, a duty dramatically articulated by the Talmudic interpretation of the good qualities Balaam saw in how Israel's tents were arranged. Thus rabbis and educators should refrain from using e-mail for confidential communications, especially on the congregational server, lest others intentionally or accidentally read them. Similarly, if an employer makes clear that any and all communications on cyberspace generated on office equipment is subject to surveillance but that employees may occasionally send short e-mails to friends to set lunch dates and the like, employees must make sure that the employer will see nothing in such messages that should remain private with them. Just as employers must take steps to ensure that employees know what is, and what is not, protected from intrusion, so too employees are responsible to preserve their own integrity and honor by insuring that their communications open to employer scrutiny do not contain information that will harm them. Both parties must take these steps to create clear boundaries of employee privacy for all the moral, legal, and theological reasons described above.

In sum, the employer's duty to protect an employee's privacy from intrusion in the work place must be balanced against the employee's duty to produce an honest day's work. That latter duty, together with the employer's responsibility to judge employees fairly when it comes to decisions about retention and promotion, together establish an employer's right to monitor the use of an employee's time. When the employee's job involves work on the Internet, employers justifiably intrude on their employees' computer usage to monitor their job performance. The employer's duty to protect their employees' right against intrusion is achieved through notice that employees' Internet usage will be monitored, consent, and the duty to avoid harmful disclosure.

Pesak for Part I

In accordance with our understanding of Jewish laws governing intrusion as applied to the new realities of cyberspace:

1. Employers who intend to monitor their employees' input on company computers must announce the rules governing company cyberspace equipment (and telephones and fax machines) to potential employees at the time of hiring, both orally and in writing. Moreover, employers should insist that employees sign a copy of the company policy, thereby acknowledging that the employer has provided ample notice of the company's policies on these matters and that the employee should expect nothing else.

2. Employers must also announce company policy as to whether employees may use company equipment for personal use at all and, if so, employers must clearly specify the parameters of legitimate personal use so that all employees know what is permitted and what is not.

3. Conversely, employees who are permitted to use company computers to communicate on personal matters through cyberspace but whose communications may be examined by employers at any time must take precautions to ensure that their supervisors will see in such communications nothing undermining the employee's integrity or honor.

Part II: Disclosure

שאלה

Are there conditions under which a business may disclose information it gleans from a customer's use of its web-site or registration form?

תשובה

The Scope of the Prohibition of Disclosure in Jewish Law

The Rabbis also took steps to insure that some information would not be disclosed to those who should not, for some reason, know it. A judge, for example, was forbidden to reveal his vote lest the privacy of the other judges on the panel be compromised, and the Talmud records that a student was ejected from the house of study when he revealed his vote a full twenty-two years after the trial![26] Private individuals were also enjoined to maintain confidentiality. According to the Talmud, a person may not reveal a private conversation, even if there is no harm intended or anticipated, unless the original speaker gives explicit permission to do so.[27] Rabbenu Gershom's decree forbidding the opening of other people's mail, mentioned above, prohibits learning about other people's business even when one does not disclose it to others, and how much the more so when one does.

Jewish communities also sought to insure confidentiality in the collection of taxes. Some demanded that the collectors be sequestered while working. The Frankfurt Jewish tax collectors refused to reveal entries in their books even to their superiors, the city treasurers, and the Hamburg community imposed severe fines for breaches of confidence.[28]

Privacy, though, is not an absolute value; it is sometimes set aside to protect an individual, family, or group. Accordingly, the Torah imposes a duty to testify in court when one knows of relevant facts, even though they may be incriminating (Leviticus 5:1).[29] During the Middle Ages, from the thirteenth century on, people would have to declare their assets under oath to the tax collectors, even though some of the tax collectors might be their competitors who would thus gain a competitive advantage.[30] Similarly, the communal good outweighs the rules against disclosure when it comes to fighting crime, and so institutions or companies would have a duty to disclose employee communications to governmental officials investigating a crime. This exception would not extend, though, to morally questionable activities that have not been criminalized. So, for example, the Dean of Harvard Divinity School was recently fired because he had asked a school technician to fix something on his home computer, and the technician found pornographic files. If the technician were Jewish, he should not have disclosed what he found there.

Jewish law also insists on breaking confidentiality when it would harm someone in non-judicial settings, based on the Torah's command, "Do not stand idly by the blood of your neighbor" (Leviticus 19:16).[31] Rabbi Israel Meir Ha-Kohen Kagan (Radin, Lithuania, 1838-1933), the "Hafetz Hayyim," taught, based on that verse, that A must warn B of potential problems in a business deal that B is contemplating with C if five conditions apply:

1. A must thoroughly examine the extent to which B will be harmed by the business deal;
2. A must not exaggerate the extent of the potential harm;
3. A must be motivated solely by the desire to protect B and not by dislike of C, let alone by A's own financial gain;
4. A can enable B to avoid the partnership without defaming C to B;
5. A must only harm C to the extent of thwarting the partnership and must not tell B anything that will cause C to be publicly embarrassed.[32]

In sum, individuals, under Jewish law, have a right to decide who will have access to their correspondence and private information. Exceptions to the duty against disclosure occur only when there is an overriding communal need to prevent harm, such as a revelation of private facts necessary to investigate a crime or to prevent an ill-fated business partnership. When the disclosure is not in response to a legal case, such exceptions are circumscribed by the requirement that the person making the revelation has no personal gain in breaching confidentiality and that the potential harm is substantial.

Disclosure of a Customer's Profile

Businesses have a profit incentive to gather information about current customers. Knowledge of buying habits and personal taste enable businesses to better serve their customers' needs and to market new products to their existing customers and to potentially new ones more effectively. Although the desire to gather information is as old as business, the computer dramatically changes the capacity of a business to quickly piece together a customer profile from small bits of information. Moreover, an internet company can gather information with little or no awareness of the surveillance on the part of the consumer. A consumer's on-line searches may provide companies with minute details of individuals' buying habits, including the internet sites they browsed, the amount of time they spent on a page, and the purchases they made.

A computer user may be unaware that his or her internet use is being monitored through the use of a "cookie." A "cookie" is a small file placed on the hard drive by the web-browser that allows web-sites and advertising networks to monitor online movements with great precision. Double-Click is the Internet's largest advertising placement company. After Double-Click sends you a cookie, you may find yourself targeted by ads from any of its 2500 clients. For instance, if you visit AltaVista's auto section, you might find unsolicited ads following from GM or Ford.[33]

The ability of businesses to collect information in this way, though, is not only a boon to those interested in selling someone something: it also can aid the consumer. For instance, when customers go online to Amazon.com, they may appreciate knowing about recommended new books in areas of their interest, as indicated by their past purchases. It may be of interest to know "people who bought this book also bought" and then have a list. Thus "cookies" are not, in and of themselves, objectionable from the perspective of Jewish law; here, as in most technology, the moral and legal valence of the technology depends upon how it is used.

At the same time, though, Amazon and other companies are not regulated in the United States or Canada with what they do with their client information. The key motivation for self-regulation is fostering a reputation of trustworthiness. In 1999, for instance, Amazon.com shocked privacy advocates by posting the book, music, and video tastes of its best corporate customers online. As a result of the public protest, it reversed itself and said it would allow shoppers in the future to keep their buying habits to themselves.[34]

In many cases, however, consumer information is treated as a company asset and is sold to other marketers. Beyond our buying habits, companies may access much private information about our lives from searching data-bases on line or from businesses that sell such information. A person's school transcripts, credit reports, and medical histories, together with his or her home's purchase price and current standing in the payment of taxes, are all potentially available. No wonder Americans worry about diminished privacy.

In response to consumer alarm over loss of privacy, companies are beginning to offer notice as to their information gathering practices and what they will do with the information. Increasing numbers of companies are providing people with the choice to opt in or out of the company's gathering of data about them. Companies are also being pushed by public opinion to adopt policies to protect the privacy of the people covered by their database. Companies then often distribute written copies of their procedures to protect consumer privacy in order to improve their public relations. The pressure companies feel to protect people from unwanted disclosure is similar to the pressure they are feeling to reveal intrusion through the increasingly familiar announcement regarding telephone use — namely, that your call may be monitored to assure quality of service. In both cases, the public is effectively requiring companies to adopt measures to protect people's privacy even before, and sometimes well beyond, legal demands to do so.

At the same time, there is a debate among business and consumer groups as to how much privacy notice and protection is needed. It is understandable that an online company wishes to make a consumer's online experience as powerful and memorable as any on-land shopping experience, which entails knowledge of a customer's likes and dislikes, advertising demographics and tailoring. The question is how much do they have to disclose to the consumer about what they are learning about him or her in the process of making a sale. Many companies simply do not notify customers that information is being gathered and potentially sold. These companies would argue that information is an asset and that all companies are in the business of gathering information, that buyers should know this, and so buyer beware! Other companies provide some notice, but do so either with jargon that makes it hard to understand or as an "opt-out" box — that is, click here if you do not give us permission to gather or sell information, a box that often goes unread. Moreover, many companies keep their data secret, failing to provide consumers with access to their profiles. That makes it impossible for consumers to correct harmful misstatements. And last, some companies fail to maintain adequate security on their collected information, enabling, if not inviting, other parties' access to private information.

As students of the Jewish tradition, we bring to the growing discussion of privacy and the workplace a high regard for the duty to refrain from making disclosures without consent. As we apply Jewish law to modern circumstances, we believe that Jewish law demands that businesses take into account their moral duty to give notice that they gather information about consumers, including disclosure of how the information will be used. Companies should collect only timely, relevant, and accurate data; they should take steps to keep it up to date and secure; they should use it only for purposes announced at the time of collection; and they should disclose it only in accordance with stated rules known and accepted by consumers. Furthermore, data about individuals should be removed from files used for marketing, direct mail-advertising, and for use by a third party unless consent is obtained from the consumer. Indeed, companies may gather such information in the first place only with the prior, written consent of the consumer and only if there are easy ways for the consumer to opt-out at any time.

The harm that could be done to an individual by inaccurate information or by mishandling of personal health, financial, or other data is obvious and severe. Therefore, companies that collect and disseminate marketing information about individuals minimally have the duty to ensure that the information they disseminate is accurate, and that duty minimally entails that they provide an easy way for individuals to see and correct such information. Moreover, from a Jewish perspective, such companies also have the duty to allow individuals to delete anything in their file that they do not want disclosed, including the whole file — except, of course, if it is required by governmental authorities investigating crimes. Finally, Jewish law requires that such companies specifically ask permission from individuals to gather and disseminate information about their buying habits; they may not just assume such permission until and unless the individual specifically denies it ("opts out").

Such privacy disclosure procedures will protect consumers from unwanted commercial solicitations. Gaining greater control of the information about us may also help to protect us from unwanted discrimination because knowledge of our status, choices, and communication behavior may all too easily form the basis of unwanted distinctions, labeling, and prejudice.

Pesak for Part II

In order to comply with Jewish law, a business may disclose information to a third party gleaned from individuals' registration forms or their use of its web-site only if the consumer provided informed consent with an opt-in declaration to the gathering and specific use of the information. In addition, a company has a duty to provide a consumer with access to the private information it collects about him or her and to provide an easily usable means to correct inaccurate information, thereby protecting the consumer against the use of false and harmful information. The presumption of privacy protection is rebutted by a legitimate communal need, such as the duty to testify in a court case, the duty to assist law enforcement agencies in investigating a crime, and even the duty to prevent a potentially harmful relationship under the conditions delineated by the Hafetz Hayyim, as described above. Informed consent for disclosure helps assure greater control over the private facts in our lives, a control that offers us greater dignity and the opportunity to lead holy lives.

Notes

1 Cited in Privacy Rights Clearinghouse, National Association of Attorneys General Annual Conference, June 22, 2000, Seattle, Washington- web site: www.privacyrights.org/ar/nagg-mill.htm.

2 *Supra*.

3 See Charles Piller, "Bosses with X-Rays," *Macworld*, July 1993, at 118, 120.

4 Jeffrey Rosen, "The Eroded Self," *NY Times Magazine*, April 30, 2000, p. 46, 50.

5 *Supra.*

6 See Moshe Silberg, "Laws and Morals in Jewish Jurisprudence," 75 Harvard Law Review 306 (1961) and Robert Cover, "Obligation: A Jewish Jurisprudence of the Social Order," in *Narrative, Violence, and the Law*, Martha Minow, Michael Ryan, and Austin Sarat, eds. (Ann Arbor, Michigan: The University of Michigan Press, 1995), pp. 239-248. But see David Novak, *Covenantal Rights: A Study in Jewish Political Theory* (Princeton: Princeton University Press, 2000), who argues that the Jewish covenant actually forms the basis for individual rights.

7 Gavison, "Privacy and the Limits of the Law," 89 Yale Law Journal 421, 447 (1980).

8 Fried, Privacy, 77 Yale Law Journal 475 (1983).

9 Bazelon, "Probing Privacy", 12 Gonzaga Law Review 587, 589 (1977). See also E. Shils, The Torment of Secrecy, 22-24 (1956); Martin Bulmer, Censuses, Surveys and Privacy (London: Macmillan, 1979); and P. Westin and F. Allan, Privacy and Freedom (New York: Atheneum,1967). These sources and those cited in the previous two notes are suggested in Elie Spitz, "Jewish and American Law on the Cutting Edge of Privacy: Computers in the Business Sector" (Los Angeles: University of Judaism, 1986), p. 1. This responsum, in fact, is the result of our joint effort to expand the work that he originally did in that paper.

10 *Sifre Deuteronomy***,** Ekev**.**

11 See also Deuteronomy 29:28, according to which, "secret matters belong to the Lord our God, while revealed matters are for us and for our children forever to carry out the words of this Torah." Similarly, in the visions of the Heavenly Chariot in Isaiah (Chapter 6) and Ezekiel (Chapter 1), both prophets can only see God's attendants and not God Himself.

12 M. *Haggigah* 2:1; J. *Haggigah* 2:1 (8b).

13 Norman Lamm makes this point; see his article, "The Fourth Amendment and Its Equivalent in the Halacha," *Judaism* 16:4 (Fall, 1967), pp. 300-312; reprinted as "Privacy in Law and Theology," in his *Faith and Doubt: Studies in Traditional Jewish Thought* (New York: KTAV, 1971), pp. 290-309, esp. pp. 302-3. *There are, of course, important differences between God and human beings, and we cannot imitate God in some divine characteristics (e.g., God's ability to know our innermost thoughts, God's power, etc.) and perhaps should not imitate God in others (e.g., God's apparent arbitrariness on some occasions, God's jealousy, God's wrath, etc.). Here, however, we both can and should imitate God's concern for privacy, as biblical and Rabbinic law spell out.*

14 *Mekhilta*, *Yitro*, on Exodus 20:23 (ed. Horovitz-Rabin [Jerusalem: Bamberger and Wahrman, 1960], p. 245); *Sifra*, *Kedoshim*, on Leviticus 19:18 (also in J. *Nedarim* 9:4 and *Genesis Rabbah* 24:7); *Deuteronomy Rabbah* 4:4.

15 B. *Bava Batra* 60a; see also 2b, 3a. M.T. *Laws of Neighbors* 2:14. The legal requirements mentioned were enforced

through monetary fines and, if necessary, excommunication; see Nahum Rakover, *The Protection of Individual Modesty* (Jerusalem: Attorney General's Office), pp. 7, 8 (Hebrew). See also "*Hezek Re'iyha*," *Encyclopedia Talmudit* 8:559-602 (Hebrew); and Lamm, *ibid*., pp. 294-5.

16 Louis Finkelstein, *Jewish Self-Government in the Middle Ages* (New York: Jewish Theological Seminary of America, 1924), pp. 31, 171ff, 178, 189. "*Herem d'Rabbenu Gershom*," *Encyclopedia Talmudit* 7:153, footnotes 877-904 (Hebrew), cites Ashkenazic and Sephardic codes and responses that adopted and extended Rabbenu Gershom's mail decree.

17 B. *Shabbat* 33a.

18 Isaac Abravanel (Spain-Italy, 1437-1508) maintains that the employee's duties actually come logically before the employer's duties, and that is why, he suggests, Leviticus 19:13 says, "Do not oppress your neighbor and do not steal, do not keep your employee's wages overnight": First the verse warns the employee not to oppress the employer and not to steal from him, but rather the employee must do his work faithfully, and then, after that, the verse warns the employer not to keep the wages of the employee with him overnight. Cited in *Mai'am Lo'ez*, Deuteronomy, p. 940.

19 B. *Ta'anit* 23a; M.T. *Laws of Hire* 13:7; S.A. *Yoreh De'ah* 244:5; S.A. *Hoshen Mishpat* 337:20.

20 B. *Berakhot* 16a; M.T. *Laws of Hire* 13:7; S.A. *Hoshen Mishpat* 337:20. The subsequent customary acceptance of workers taking the time to say the fourth blessing of Grace after Meals: Rabbi Meir Ha-Kohen (Germany, 13th century), *Haggahot Maimoniyot* on M.T. *Laws of Blessings,* I; S.A. *Orah Hayyim* 110:2; 191:2.

21 The prohibitions of moon-lighting and of starving oneself: T. *Bava Metzia* 8:2; J. *Demai* 8:3; *Rif,* B. *Bava Metzia* 90b.

22 M. T. *Laws of Hire* 13:6; S.A. *Hoshen Mishpat* 337:19.

23 B. Bava Metzia 29b-30a; Rashi (on 30a), s. v. *de-nafish p'sidyhu*; Tosafot (on 30a), s. v. *b'torei d'nafish p'sidyhu*.

24 Roger Dobson, The Independent-London, September 13, 2000- Foreign; Issue: PSA-2682; Business section; http://special.nothernlight.com/privacy/big_brother.htm.

25 While a current West 2000 search indicates that United States law and court decisions on e-mail and internet usage on company computers is sparse, these recommendations accord with the guidelines that have emerged so far. Specifically, the omnibus Crime Control and Safe Streets Act of 1966 established rules for wiretapping and other electronic interceptions. It was amended at Title III by the Electronic Communications Privacy Act of 1986 (ECPA), Public Law #99-508, 100 Stat. 1848, 18 U.S.C. Section 2510, to include protections of electronic communications, including e-mail, from hackers and other people who have no legitimate interest in the communications, but this act specifically excludes employees working on computers belonging to their employers when employees have consented explicitly or even by implication to their employers' monitoring of their communications on company computers: see 18 U.S.C. Sections 2511(2)(c); 2701 (c)(1); and 2702 (b)(3). It is obvious that explicit, written acknowledgment by the employee of the employer's right to do this is best, but employees also agree to this stipulation by implication if they accept employment in a company where employees are warned that company computers are for business purposes only and where employees' e-mail and internet communications are in fact monitored routinely for legitimate business purposes.

The courts have upheld these provisions. So, for example, in an unpublished opinion, the California Court of Appeals held that the California Invasion of Privacy Act (Penal Code 630 through 637.5) prohibiting wire-tapping, eavesdropping, recording confidential communications, or disclosing telegraphic or telephonic messages does *not* apply to e-mail in *Bourke v. Nissan Motors* (July 26, 1993) and that the company was therefore within its rights in firing Mr. Bourke for using the company computer for sending personal and sexual messages because (1) employees signed a notice of the company policy limiting computer use on company computers to company business and (2) employees were aware that their e-mail messages were being read by supervisors and not just by their intended recipients.

Several more notes about this. First, sometimes employees assume that their personal password for gaining access to their company computer creates a legitimate expectation of privacy for their messages emanating from there. The courts, however, have specifically denied this claim, maintaining that the facts that the company owns the computer and assigned the password indicates that the company retains rights of access to the computer at any time. Acceptance of a password from the employer to gain access to the company's electronic system, in other words, amounts to acceptance of the company's rules governing that system.

Second, American law draws a distinction between government and private employees, such that government employees have a greater right to assume the privacy of their computer communications than employees of private companies. Therefore, government employees must sign a *consent* form to waive their privacy rights vis-a-vis their computers at the office rather than just an *acknowledgment* of company policy that computer usage will be monitored.

Third, list serves present yet another wrinkle in this whole area. In the California case of *Intel Corporation vs. Hamidi* (California Superior Court, 98AS05067, November 2, 1998), the court held that Mr. Hamidi did not have the right

to organize union activity at Intel by soliciting union membership there through sending a letter to each of 30,000 employees on their internal list serve because the company owned the computer system and therefore had the right to restrict its use. That case, though, involved an internal e-mail system within the company. It is not clear what courts will do with using company computers to contact lists outside the company. In any case, the issue addressed in this *teshuvah* is clearly on the cutting edge of American law as well.

26 M. *Sanhedrin* 3:7; B. *Sanhedrin* 31a.

27 B. *Yoma* 4b. According to Magen Avraham (S.A. *Orah Hayyim* 156:2), even if the party revealed the matter publicly, the listener is still bound by an implied confidence until expressly released. Likewise *Hafetz Hayyim* 10:6.

28 Salo W. Baron, *The Jewish Community* (Philadelphia: Jewish Publication Society, 1942), vol. 2, p. 281.

29 See also B. *Bava Kamma* 56a; Gordon Tucker, "The Confidentiality Rule: A Philosophical Perspective with Reference to Jewish Law and Ethics," 13 *Fordham University Law Journal* 99, 105 (1984); and A. Cohen, *Everyman's Talmud* (New York: Schocken, 1949), p. 307.

30 Irving A. Agus, Urban Civilization in Pre-Crusade Europe (New York: Yeshiva University Press, 1968), vol. 2, p. 472-474. We would like to thank Rabbi Joel Rembaum for this reference.

31 The Rabbis' interpretation (in the *Sifra* on that verse and in *Targum Pseudo-Jonathan* there) was: "Do not stand idly by when your neighbor's blood is shed. If you see someone in danger of drowning or being attacked by robbers or by a wild beast, you are obligated to rescue that person."

32 Israel Meir Kagan, *Be'er Mayyim Hayyim* (Rabbi Kagan's extensive notes to his book, *Hafetz Hayyim*), ch. 9, par. 1. Summarized in Samuel Mordecai Huminer, *Sefer Ikkarei Dinim* (based on the work of Rabbi Kagan), included as part of *Shemirat Ha-Lashon: Ikkarei Dinnim* (Jerusalem: Mercaz Ha-Sefer, 1983), ch. 9, par. 56, p. 62-63, and translated and adapted in Zelig Pliskin, Guard Your Tongue (based on the *Hafetz Hayyim* and his notes in *Be'er Mayyim Hayyim*) (Jerusalem: Aish Ha-Torah, 1975), p. 164; see also Alfred S. Cohen, "Privacy and Jewish Perspective," *The Journal of Halacha and Contemporary Society* 1 (1981), p. 74-78.

33 Jeffrey Rosen, "The Eroded Self," *NY Times Magazine*, April 30, 2000, p.46, 48.

34 Amy Doan, "Amazon Backs Off on Customer Lists," Forbes.com, August 27, 1999.