Journal of Business Ethics (2008) 80:175–180
DOI 10.1007/s10551-007-9449-6

Management and Legal Issues Regarding Electronic Surveillance of Employees in the Workplace

David Halpern
Patrick J. Reville
Donald Grunewald

ABSTRACT. Since the attack on the World Trade Center in New York, and on the Pentagon in the United States, concerns over security issues have been at an all-time high in this country. Both state and federal governments continue to discuss legislation on these issues amid much controversy. One key concern of both employers and employees is the extent that employers, espousing a ''need to know'' mentality, continue to expand their capability and implementation of surveillance of employees in the workplace. With the technology typically growing faster than the speed of legislation, protective or permissive, the management and legal issues involved in electronic monitoring of employee communications in the workplace, are and well should be on the agenda for discussion of every management and legal team in American business today. Companies have a legitimate right to protect their trade secrets from disclosure by disgruntled employees. Similarly, companies also have a duty to protect their good names and reputations from unauthorized employee communications with outside parties, and even other employees, that may damage them. It is also a prime duty of management to ensure, in their direction of their workforces, that the employees execute their responsibilities by working full time on their stated objectives. In this regard, any management that fails to oversee its workforce to ensure that employees are not expending valuable company time, for which they are being compensated, on personal business, including unauthorized communications, is remiss in its responsibilities to its shareholders. The company may see a reduction of the price of its shares in the marketplace if it does not protect the economic interests of its shareholders.

KEY WORDS: security issues, surveillance of employees

Legal analysis

Historical and current statutory authority

In 1986, the United States Congress passed into law the Electronic Communications Privacy Act (ECPA)[1], commonly known as the Federal Wiretap Act. This Wiretap Act was formerly known as the 1968 Omnibus Control and Safe Streets Act. Said statute provides for criminal and civil sanctions for ''any person who...intentionally intercepts, endeavors to intercept, or procures any other person to intercept ... any wire, oral, or electronic communication.''[2]

In addition to said Federal law, virtually every state has some sort of statute dealing with eavesdropping, wiretapping, and the like, setting forth limitations and prohibitions on said activity, by individuals, employers, and governmental authorities. For purposes of this article, we will concentrate on the Federal statute set forth above.

Of key interest is the concept of ''intercept'' and/or what constitutes an ''interception.'' Intercept is defined as ''the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device.''[3] If an electronic communication held in ''electronic storage'' is later examined, as opposed to contemporaneously listened to while happening, the courts have held that this in itself is not an ''intercept within the meaning of the prohibition.[4] So when an employer copied the electronic mail from an employee's hard drive, it did not

violate a statute prohibiting electronic interception of personal telephone calls without a warrant, absent proof that the employee's electronic mail was obtained while it was being transmitted.[5] Yet, the courts have also concluded that one does not have to ''listen in'' on a communication to constitute an interception.[6] For the record, by the way, just what is an ''aural acquisition'' of a communication? Apparently, it simply means to come into possession of same by use of the sense of hearing.[7] But, just because someone comes into possession of an email message by inadvertently seeing same on a computer screen, this alone would not be a violation of the statute, because there would be no unlawful ''interception'' under those circumstances.[8]

The statutory exceptions

The ECPA as set forth above contains a number of exceptions, including: (a) the ''Business Extension'' exception; (b) the ''One Party Consent'' exception; and (c) an exception regarding the Employer protecting its Rights or Property. All three of these deal with ''permitted interceptions'' of communications. In addition, the ECPA allows for access to and examination of (d) ''stored'' employee communications.

(a) The so-called Business Extension exception allows interception of communications by an employer when, as typically is the case, the telephone, equipment, or facility is furnished by the employer and used in the ordinary course of business.[9] Thus, ''listening in'' may constitute an interception, but be at the same time exempt from applicability of the general prohibition of the statute. However, the statutory exception is narrowly interpreted as to what is in the ''ordinary course of business,'' so that a branch manager who used a business extension to monitor an employee's conversation with a former employee, under a suspicion that confidential business information was being disclosed, fell within the exception, while recording 22 hours of employees' personal calls with a device purchased at an electronics store (not provided by the telephone company) was held beyond the scope of the ordinary course of business.

(b) The ''One Party Consent'' exception falls under Sec. 2511(2)(d), which states: ''It shall not be unlawful...for a person...to intercept a wire, oral, or electronic communication where one of the parties to the communication has given prior consent to such interception...'' Obviously, then, a person who records his or her own phone conversations with another does not violate the law. (But what about an employer claiming that employees have consented to the employer intercepting/monitoring/recording communications? It appears that the employer should make it abundantly clear to the employees that communications would be so monitored, as a mere warning to employees that there may be monitoring to cut down on personal use of the telephones would not be enough to fall under the consent doctrine. Advice to an employer: Get the consent provision in writing, make it part of the employee agreement, and even have said provision separately acknowledged.

(c) Should not the employer be able to intercept communications in order to protect its rights to business trade secrets and the like? Sec. 2511(2)(a)(i) answers in the affirmative, as long as it is ''in the normal course of his employment while engaged in any activity, which is a necessary incident to the rendition of his service or to the protection of the rights and property of the provider of that service...'' In *U.S.A. v. Mullins*), the 9th Circuit Court of Appeals upheld and clarified the right of an employer to so protect itself.

(d) Monitoring/retrieving stored communications, as set forth above, would not be considered interceptions under the law. In addition, Sec. 2701 of 18 USC deals with unlawful access to stored communications. This section generally makes it unlawful to access communications in electronic storage, but Sec. 2701(c)(i) contains an exception, in that it expressly states that ''Subdivision (a) of this section does not apply with conduct authorized—(1) by the person or entity providing a wire or electronic communications service.'' As a result, as far as communications stored on the employer's equipment, there is no prohibition of access.

Recent case law

Since its enactment in 1986, there have been numerous cases that have made their ways through the courts, where litigants have attempted to receive

interpretation of the prohibitions and exceptions set forth above. Naturally, as indicated in the citations contained herein, interpretations of terms under prior statutory and case law have been helpful.

In *Fraser v. Nationwide Mutual Insurance Company*, the United States Court of Appeals for the Third Circuit recently dealt with some of the issues set forth hereinabove. Fraser was an independent insurance agent for Nationwide Insurance Company, and got terminated by Nationwide. He sued for wrongful termination under state law, and for damages under the ECPA, claiming unauthorized access to his email account. It was admitted by Nationwide that it had accessed his email, and had found evidence of disloyalty. The court, in citing the Steve Jackson Games case, concluded that there could be no intercept of an email in storage, as an email in storage by definition is not an electronic communication. The court also found that the email was stored on Nationwide's system. The court took some issue with the lower (District) court's interpretation of what constituted "electronic storage," but nevertheless affirmed, concluding (a) that there was no interception, and (b) the Sec. 2701(c) exception applied.

Legal conclusions

In dealing with the management issues set forth herein, care must be given by management to balance its objectives of protection of property rights, bolstering productivity and profitability, and maintaining employee morale. In addition, management must exercise care to comply with all relevant Federal and State laws.

In dealing with the legal issues, the conclusion reached by the authors hereof is that employees face an uphill battle in bringing actionable complaints against employers regarding electronic workplace surveillance activities, as long as management has taken the care cited above in legal compliance. As an employee, you must almost presume that Big Brother is (legally) watching.

Management analysis

The ethical and managerial issues of what constitutes good management practice with respect to the activities of employers in using electronic surveillance of employee communications, must balance the competing interests of companies with that of their employees.

Clearly, under the law, companies have a legitimate right to protect their trade secrets from disclosure by disgruntled employees. Similarly, companies also have a duty to protect their good names and reputations from unauthorized employee communications with outside parties, and even other employees, that may damage them.

It also is a prime duty of management to ensure, in their direction of their workforces, that the employees execute their legal and ethical responsibilities to work full time on their stated objectives. In this regard, any management that fails to oversee its workforce to ensure that employees are not expending valuable company time, for which they are being compensated, on personal business including unauthorized communications or some other private non-company related purpose, is remiss in its responsibilities.

For example, if employees were using company time to play computer games or to gamble over the internet or to use the internet for non-company purposes such as watching sports programs when they should be working on company-related business, these employees are in effect not meeting their legal and ethical responsibilities to the company. If such employee activities are taking place on company time, it might affect the productivity of the company adversely to the detriment of the company and its shareholders.

However, the question of how management is best able to bring about and maintain expected standards of worker productivity is a very complex issue as it relates to questions of controlling and monitoring employee communications on the job. It seems to be clear, based upon the legal issues discussed above, that management is permitted by law, under a variety of circumstances, to monitor employee communications in the workplace. Such controlling and monitoring of employee communications is a complex managerial policy decision that should take into account certain important criteria and considerations.

Specifically, what type of corporate culture is desirable and appropriate for a particular company is a critical consideration with respect to monitoring

employee communications on the job. If a company places a premium on a relaxed informal culture that strives to encourage creativity and innovation among its employees, then management must be very careful with respect to instituting a policy of electronic surveillance of employee communications. Implementation of such a new company policy could have a very chilling effect in what was formerly a very open and relaxed atmosphere in the workplace of the company. This new policy could have very negative effects upon creativity and innovation.

Under these circumstances, employees may resent management's ''intrusions'' into communications that they consider private and appropriate in the workplace. Employees may then conclude that management does not trust them anymore. If employees under these circumstances begin to resent and/or fear management, then an essential ingredient of creativity, namely, *esprit de corps*, may be lost, resulting in a substantial diminution of creativity.

Presumably, companies that are on the forefront of technological innovation as well as firms in creative fields such as advertising, marketing, and entertainment, would be examples of companies that place very high demands upon the creativity of their employees. From a management perspective, even though electronic surveillance of employee communications would be legal, such surveillance might be quite counterproductive for such companies to institute a policy of monitoring employees' communications without much discussion with the employees.

The more complex issue from a management perspective is whether to institute a policy of monitoring employee communications in companies that do not place a premium on creativity and innovation. One could assert that management should institute such a policy if doing so would improve employee productivity. This requires a judgment call by management, who may be influenced by the past practices of employees regarding their communications practices at work. If management has been lax in this area, resulting in abuse by employees of company communication privileges with respect to their interactions, it might be appropriate for management to institute a policy of surveillance of employee communications at work.

Such managerial decisions should probably not be predicated solely upon an ''abuse test.'' It may be appropriate in some cases for management to institute a policy of surveillance of employee communications in the absence of any evidence that employees have abused company time and property to engage in unauthorized communications of a personal nature. Despite the absence of evidence of such abuses, management may still want to institute a policy of surveillance of employee communications where, in the judgment of management, this policy would make the employees more efficient and, thus, hopefully more productive.

One way for management to introduce such a new policy of surveillance of employee communications would be to begin by conducting open and transparent studies of employee communications practices in their firms, which will demonstrate to employees the necessity of instituting ongoing practices of surveillance of employee communications to increase efficiency.

Specifically, if the result of such a company study by productivity experts clearly demonstrates to the employees that instituting such a policy will improve efficiency and productivity, then it may be much easier for management to convince employees that such a policy of surveillance of employee communications is both ethical and fair to all concerned.

In theory, employees should have a definite interest in improving productivity in their company, because this would hopefully improve profitability. If the company will become more profitable, then wise management will share these increased profits with employees in the form of higher compensation.

Instituting a policy of surveillance of employee communications after a careful efficiency study as indicated above, may serve another very important purpose. If a logical rationale can be advanced by management as to the propriety and necessity of employee communication surveillance to improve productivity, then employees may not view such a new policy as either arbitrary or punitive in nature. This is critical, because if employees understand that such a policy is not being instituted to harm them, or because the management does not trust the employees, but instead to benefit all the company's stakeholders, then this may help serve to prevent any potential negative effects, such as a diminution of morale or increase in employee turnover. Perhaps

such a new policy, could be shown to be a win for management in the form of higher productivity and resulting higher profitability and a win for the employees in the form of higher compensation, and possibly greater job security, because the company would be financially healthy and presumably less willing to eliminate jobs to save on costs.

Support of the workforce will help make the policy more effective than, if the advantages of the new policy are not clear to the workforce who might then oppose or obstruct the new policy. This is why, the proposed new change in policy needs to be discussed with employees and their feedback encouraged to make sure that the new policy will be fair to all concerned and will be effective when it is instituted. The policy should also be instituted only after public notice to all concerned.

In developing and implementing a policy of employee communication surveillance, management should be careful to abide by, the dictates of all applicable Federal and State statutes, once the decision is made to implement the new policy so as to be able to defend the company against potential employee litigation in this area.

As cited above, company practices in this area must make a very clear distinction between monitoring employees' communications, which constitute interceptions and in gaining access to communications already in electronic storage, both of which are impermissible under the Electronic Communications Privacy Act of 1988 (ECPA), unless said practices fall under statutory exceptions. The authors recommend that management should make company policy with respect to employee communication surveillance a condition of employment and should require that all employees sign a written waiver to this effect to comply with the dictates of the ECPA, as discussed in the legal section of this paper, if it decides to adopt such a new policy of surveillance of employee communications.

Before a new policy of surveillance of employee communications is instituted by management, it should carefully vet the wording of such a new policy with the company's legal department and/or outside legal counsel to ensure that the policy complies with all of the statutory requirements as discussed in the legal section of this paper above.

Conclusions

In dealing with the managerial and ethical issues set forth in this paper, care must be given by management to balance its objectives of protection of property rights, bolstering productivity and profitability, and maintaining employee morale. In addition to balancing these objectives, management must exercise care to comply with all relevant Federal and State laws regarding surveillance of employee communications.

In dealing with the legal issues involving a policy of surveillance of employee communications, the conclusion reached by the authors of this paper is that employees face an uphill battle in bringing actionable complaints against employers regarding electronic workplace surveillance activities, as long as management has taken the care cited above in legal compliance. Employees must almost presume that Big Brother is (legally) watching.

Notes

[1] 18 U.S.C. § 2510 *et seq*.
[2] 18 U.S.C. § 2511 (1) (a)
[3] 18 U.S.C. § 2510 *et seq*.
[4] Steve Jackson Games Inc. v. U.S. Secret Service, 36 F. 3d. 457 (5th Cir. 1994).
[5] U.S. v. Simons, 29 F. Supp. 2d. 324 (E.D. Va. 1998), *aff*'d in part, remanded in part, 206 F. 3d. 392.
[6] George v. Carusone, 849 F. Supp. 159 (D. Conn. 1994).
[7] Smith v. Wunker, 356 F. Supp. 44 (S.D. Ohio 1972).
[8] Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1977), *aff*'d, 172 F. 3d. 861 (3rd Cir. 1998).
[9] 18 U.S.C. § 2510 (5) (a).
[10] Briggs v. American Air Filter Co. Inc., 455 F. Supp. 179 (N.D. Ga. 1978) *aff*'d, 630 F. 2d. 414 (5th Cir. 1980).
[11] Deal v. Spears, 980 F. 2d 1153 (8th Cir. 1992).
[12] U.S. v. Hodge, 539 F. 2d. 898 (6th Cir. 1976).
[13] Deal v. Spears, *infra*.
[14] 992 F. 2d. 1472 (9th Cir. 1993), *cert. denied*, 510 U.S. 994 (1993).
[15] 352 F. 3d. 107 (3rd Cir. 2003).
[16] Steve Jackson Games, *infra*.

David Halpern
Management,
Iona College, Ph.D., New York University,
New Rochelle, NY, U.S.A.

Patrick J. Reville
Business Law,
Iona College, J.D., Fordham University,
New Rochelle, NY, U.S.A.

Donald Grunewald
Strategic Management,
Iona College, D.B.A., Harvard University,
New Rochelle, NY, U.S.A.
E-mail: Dgrune34@aol.com

Donald Grunewald
5 River Road #307, Wilton, CT, 06897, U.S.A.