ELECTRONIC SNOOPS, SPIES, AND SUPERVISORY SURVEILLANCE IN THE WORKPLACE[+]

DONALD E. SANDERS*
JOHN K. ROSS**
PATRICIA PATTISON***

I. INTRODUCTION

Employees are spending an ever-increasing amount of time using computers, cell phones, tablets and other communication devices as part of their work-related activities. Unfortunately, the use of advanced communications systems, the proliferation of on-line shopping sites, and the explosion of interest in social media outlets has also resulted in employees spending an ever- increasing amount of time connected to the Internet pursuing personal interest rather than company business.

A recent survey of over 4,600 human resource managers and over 4,000 employees indicates that approximately 65% of employees spend at least some work time on non-work related Internet activity.[1] Of those employees using social networks sites, some 56% check their profiles during their typical workdays and 15% of this group spends at least one hour a day browsing. The same survey indicated that 61% of employees sent personal emails, with 19% sending more than five personal emails per day.

Management's response to non-work related Internet activity has been to establish tighter policies regarding Internet usage and electronic means to monitor employees. The most prevalent method of controlling employees Internet behavior, according to surveyed employers is by blocking sites (54%), monitoring Internet usage and email (50%), and firing employees for policy violations (22%).[2]

[+] Received the 2012 "Best Paper Award" from the Southern Academy of Legal Studies in Business and *Cengage*-Southwest Publishing.
*J.D., Professor, Texas State University-San Marcos, Texas.
**Ph.D., Associate Professor, Texas State University-San Marcos, Texas.
***J.D., Professor, Texas State University-San Marcos, Texas.
[1] *Half of American Workers Will Shop Online at Work this Holiday Season, According to CareerBuilder "Cyber Monday" Internet Usage Survey*, CAREERBUILDER.COM (Nov. 27, 2011), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr670&sd=11%2f28%2f2011&ed=12%2f31%2f2011&siteid=cbpr&sc_cmp1=cb_pr670.
[2] *Id*.

> The trends in employee potential misuse of technology, and employer reactions to this changing environment, is further evidenced by two earlier surveys conducted by the American Management Association (AMA) and The ePolicy Institute in 2001[3] and again in 2007.[4] These surveys indicated a dramatic rise in the use of electronic monitoring, primarily as a tool to avoid potential lawsuits. According to the 2001 AMA survey over 60% of responding companies monitored employees' Internet connections, 46% e-mail, and 36% storage and retrieval of company files.[5] By 2007 the figures had risen to 66 percent monitoring Internet connections. It is highly likely that this trend in electronic monitoring will continue as the technology (hardware and software) continue to improve and becomes less resource intensive to install and use.[6]
>
> In 2007 employers seemed to be highly concerned with inappropriate web surfing and cyberloafing; 65% of the companies monitoring employees used software to block inappropriate websites, up 27% from 2001. Inappropriate sites that are blocked by companies include those sites with adult content (96%), games (61%), social networking (50%), entertainment (40%), shopping (27%) and sports (21%). Software is also extensively used to monitor email. Approximately 43% of the companies surveyed monitor email, with 73% using technology, and 40% using individuals to manually read and review email. Additionally, 45% monitor telephone use, with 16% recording phone conversations. Another 48% (up from 33% in 2001) use video surveillance for security. Of those that use video, 7% also monitor employees' performance.[7]

In addition to monitoring employee communications, technology now enables the employer to monitor virtually all aspects of an employee's behavior while at the workplace. Employee behavioral monitoring is not only

---

[3] American Management Association, *2001 AMA Survey, Workplace Monitoring & surveillance: policies and Practices* (2001) [hereinafter 2001 AMA Survey]. *See also*, *2001 AMA, US News, ePolicy Institute Survey, Electronic Policies and Practices Summary of Key Findings,* AM. MGMT. ASS'N, http://www.epolicyinstitute.com/survey2001Summary.pdf (last visited Mar. 31, 2012).

[4] *2007 Electronic Monitoring & Surveillance Survey: Over Half of All Employers Combined Fire Workers For Email & Internet Abuse*, AM. MGMT. ASS'N (FEB. 28, 2008), http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/ [hereinafter 2007 Electronic Monitoring and Surveillance Survey].

[5] 2001 AMA Survey, *supra* note 3.

[6] 2007 Electronic Monitoring & Surveillance Survey, *supra* note 4.

[7] *Id*.

conducted on the lower level employee such as the clerical, data entry or telephone employee, but on the intellectual and managerial employee as well. And the monitoring can be done openly or secretively. The concept of privacy at the workplace is clearly in a state of flux as management and employees continue to adapt to the rapid changes brought by the advances in technology.

This article is intended to present a brief review of constitutional issues and federal and state legislation regulating electronic monitoring of employees. Representative cases will illustrate the application of the statutes. The article will discuss the hazards of monitoring email and texting by employees and urge caution when employer monitoring moves to activities outside the workplace. This article is not intended as a comprehensive review of all the permutations relating to legal difficulties of workplace monitoring.

II. CONSTITUTIONAL CONSIDERATIONS

The law as it pertains to privacy, and therefore the invasion of an employee "rights" due to employer monitoring, is anything but new. In their foundational work on privacy, Samuel Warren and Louis D. Brandeis observed:

> Later there came recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life—the right to be let alone, the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.[8]

Because of constitutional considerations public employers have a greater burden to protect employee privacy. The Fourth Amendment's protection against unreasonable search and seizure may include employee privacy of messages sent electronically on the employer's equipment. The Fourth Amendment, as applied to the states and municipalities through the Fourteenth Amendment, protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." Employees have Fourth Amendment rights only when they have "an expectation of privacy that society is prepared to consider

[8] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

reasonable."[9] The Supreme Court recently decided in favor of the employer when it was sued for the invasion of privacy of public employees.[10] To its credit the employer, the Ontario, California police department, had a policy, "Computer Usage, Internet and E-Mail Policy."[11] All employees were required to review and sign that they had read the policy. Three provisions are most relevant:

> C. Access to all sites on the Internet is recorded and will be periodically reviewed by the City. The City reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.
>
> D. Access to the Internet and e-mail system is not confidential. All information produced is considered city property. As such, these systems should not be used for personal or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system.
>
> E. The use of inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the e-mail system will not be tolerated.[12]

The city entered into a contract with Arch Wireless to purchase 20 alphanumeric text-messaging pagers for its SWAT police officers. As part of the contract the city paid Arch a monthly subscription rate keyed to each pager; each one was allotted 25,000 characters. The purpose of issuing the pagers to the SWAT team was to enable better communication and more rapid and effective response to emergencies. When the pagers were given to the SWAT team the administrative officials reminded the officers that the pagers would be considered email messages.[13] In addition a memo with the same message was sent to all supervisory personnel.[14]

Almost immediately after issuance of the pagers several members of the SWAT team exceeded the allotted 25,000 character limit. A police lieutenant, the official in charge of the pagers, took the position that if each officer paid for the overuse charges he would not audit the messages on the

---

[9] O'Connor v. Ortega, 480 U.S. 709, 715 (1987).
[10] City of Ontario v. Quon, 130 S.Ct. 2619 (2010).
[11] Quon v. Arch Wireless Operating Comp., Inc., 445 F. Supp.2d 1116, 1123 (C.D. Cal. 2006).
[12] *Id*. at 1123-24.
[13] *Id*. at 1124.
[14] *Id*.

pager.[15] Only if the user disputed the overage charges would he then audit the content to see if it was work related. There was no apparent problem with the practice; all the officers who incurred overuse charges promptly paid for the overages without dispute.

However, the lieutenant's policy was in effect for approximately eight months when he tired of being a bill collector and complained to the police chief.[16] The chief then requested that the lieutenant audit the pager transcripts of the two heaviest users to see if the pages were work related or personal. The pager transcripts of one of the audited officers indicated that of his average of twenty-eight texts daily, only three were work related.[17] Many of his texts were sexually explicit. Some of the texts were to and from his wife who was also a police officer. Others were to and from his mistress, a police dispatcher. When this was reported to the police chief, the chief determined that both he and the SWAT officer's immediate supervisor should also read the transcripts. As a result the SWAT officer was disciplined for using too much duty time for personal issues.[18] Then he, his wife (ex-wife by the time of the trial) and his mistress joined to sue the city, bringing a Section 1983 action for breach of privacy.

The Federal District Court held that the government defendants were not liable. Although the city had created and distributed a clear policy, nevertheless the court found that the plaintiffs did have a reasonable expectation of privacy.[19] The "operational reality" was transformed by the lieutenant when he made a conscious decision not to enforce the written policy of the city.[20] The court stressed that the employer's mere ownership of the equipment is not sufficient to defeat an expectation of privacy.[21] Having found that the employees had a reasonable expectation of privacy, the court then considered whether the auditing of the pager was "reasonable under the circumstances."[22] The court determined that the audit would not be justified at its inception if the employer's purpose for conducting the audit was to ferret out misconduct.[23] However, a jury found that the audit's purpose was to determine if there was a need to increase the amount of monthly characters allotted for work-related usage, so the audit was judged reasonable and all defendants were absolved of liability for the search.

---

[15] *Id*.
[16] *Id*.
[17] *Id*. at 1126.
[18] *Id*.
[19] *Id*. at 1140.
[20] *Id*.
[21] *Id*.
[22] *Id*. at 1144.
[23] *Id*.

On appeal, the Ninth Circuit reversed, holding that the search was unreasonable as a matter of law; the intent in authorizing the search was not relevant.[24] The circuit court reiterated that the touchstone of the Fourth Amendment is reasonableness. The totality of the circumstances must be examined to determine if a search is reasonable; there are two assessments to be made, "the degree to which a search intrudes upon an employee's privacy and the degree to which it is needed for the promotion of legitimate governmental interests."[25] The court agreed that the police department's informal policy that the text messages would not be audited if the employee paid the overages made the employee's expectation of privacy reasonable.[26] Also, the search was not reasonable in its scope because less intrusive methods were feasible; the depth of the inquiry exceeded what was necessary for the department's legitimate purpose. The department could have warned the police officer that it was going to audit his pager transcripts in advance so he could have limited his personal use. Or, it could have asked him how many uses were work-related.

The Supreme Court unanimously reversed and remanded the case.[27] Justice Kennedy, writing for the Court, acknowledged that although "the case touches issues of far reaching significance, the Court concludes it can be resolved by settled principles determining when a search is reasonable." [28] When considering the degree to which society will recognize privacy expectations to be reasonable, Kennedy commented,

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own.[29]

Citing an earlier plurality opinion,[30] Justice Kennedy noted that when a search is conducted for a "noninvestigatory, work-related purpose," or when it's purpose is to investigate work-related misconduct, a government employer's warrantless search is reasonable if it was justified at its inception

---

[24] Quon v. Arch Wireless Operating Comp., Inc., 529 F.3d 892, 903 (9th Cir. 2008).
[25] *Id*.
[26] *Id*. at 906.
[27] City of Ontario v. Quon, 130 S.Ct. 2619 (2010).
[28] *Id.* at 2624.
[29] *Id.* at 2630.
[30] O'Connor v. Ortega, 480 U.S. 709, 725-26 (1987).

and if the procedures adopted are reasonably related to the purpose of the search and are not excessively intrusive.[31] The Court clearly disagreed with the District Court that the reason for a search makes a difference.

In this case, both the search and scope were reasonable. The search was justified at its inception because the police chief ordered the search to find whether the character limit was sufficient to meet the department's needs. The scope was reasonable because it was "efficient and expedient" to determine whether the overages were personal or work-related. Two facts were considered to determine that the scope was reasonable: (1) only two months of transcripts were reviewed, and (2) all off duty messages were redacted. These two steps reduced the invasiveness of the search to make it reasonable. The Circuit Court had erred in considering that other, less invasive, measures were available. The Supreme Court has repeatedly refused to declare that only the "least intrusive search practicable can be reasonable under the Fourth Amendment."[32]

In a concurring opinion, Justice Stevens summed up the Court's holding in saying that is clear that:

> [A] law enforcement officer who served on a SWAT team, should have understood that all of his work-related actions – including all of his communications on his official pager – were likely to be subject to public and legal scrutiny. He therefore had only a limited expectation of privacy in relation to this particular audit of his pager messages.[33]

III. STATUTORY CONSIDERATIONS

A. *Federal Forum*

The initial federal legislation dealing with electronic interception was the Omnibus Crime Control and Safe Streets Act of 1968, commonly known as the Wiretap Act. Although containing varied provisions, the Act addressed issues which, to a degree, govern an employer's electronic monitoring.[34] Even though the act has undergone periodic revision, the statute's clarity has suffered criticism, to the extent that one court has scornfully noted:

---

[31] *City of Ontario*, 130 S.Ct. at 2630.
[32] *Id.* at 2631.
[33] *Id.* at 2633-34.
[34] *See* 18 U.S.C. §§ 2510-22 ("Wire and electronic communications interception and interception of oral communications"); 18 U.S.C. §§ 2701-12 ("Stored wire and electronic communications and transactional records access") (West 2012).

> [W]e are once again faced with the troublesome task of an interstitial interpretation of an amorphous Congressional enactment. Even a clear bright beam of statutory language can be obscured by the mirror of Congressional intent. Here, we must divine the will of Congress when all recorded signs point to less than full reflection. But, alas, we lack any sophisticated sensor of Congressional whispers, and are remitted to our more primitive tools. With them, we can only hope to measure Congress' general clime. So we engage our wind vane and barometer and seek to measure the direction of the Congressional vapors and the pressures fomenting them. Our search for lightning bolts of comprehension traverses a fog of inclusions and exclusions which obscures both the parties' burdens and the ultimate goal.[35]

Generally it is a violation for a person, directly or through another, to intentionally intercept or attempt to intercept a wire, oral, or electronic communication; or, to disclose the contents of any wire, oral, or electronic communication when one knows or has reason to know of its interception a violation of federal law.[36] A "wire communication" is one made by means of an "aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection . . . ."[37] Thus wire communication would anticipate the interception of aural methods such as telephone conversations. An "oral communication," on the other hand, would involve an oral communication uttered by a person "exhibiting an expectation that such communication is not subject to interception,"[38] but specifically does not include any "electronic communication." Otherwise stated, interception of an oral communication ordinarily would involve microphone usage to intercept a spoken conversation.

The Electronic Communications Privacy Act of 1986 (ECPA*)* added the concept of electronic communication to the federal interception statutes. An "electronic communication" generally "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[39] Electronic communication would therefore include the newer methods of digital communication such as email, texting, and fax communications,

---

[35] Briggs v. Am. Air Filter Co., Inc., 630 F.2d. 414 at 415 (5th Cir. 1980).
[36] 18 U.S.C. § 2511(1) (West 2012).
[37] 18 U.S.C. § 2510(1) (West 2012).
[38] 18 U.S.C. § 2510(2) (West 2012).
[39] 18 U.S.C. § 2510(12) (West 2012).

supplementing the restriction on interception of aural communications identified as a wire communication. Note, however, that the ECPA would not prohibit video only surveillance; it only prohibits the interception of video. This is not to say that video surveillance or monitoring is without its risks. The common law concept of invasion of privacy poses the possibility of liability for unauthorized video, especially if made in sensitive areas. Additionally, many states have enacted statutes prohibiting "voyeuristic" taping, such as in restrooms, bedrooms, or other areas where there is an expectation of privacy.[40]

Penalties for violation of the federal prohibitions are both criminal and civil. Criminal violation provides for punishment for interception violations from a fine, to a fine and imprisonment of up to five years, depending upon the type of interception or disclosure, and whether an original or a subsequent violation.[41] Civil damages due to an improperly intercepted communication range from equitable relief, to statutory damages, punitive damages, attorney's fees and costs. For those issues which would likely involve employer interception, the statutory damages would be the greater of: 1) the actual damages incurred and any profits made by the violator; or 2) the greater of $100 per day for each day of the violation or $10,000.[42]

As is common with legal issues, the devil of the details is not so much in the statement of the rule itself, but rather in the exceptions. As applied to the federal statutes noted above, there are two exceptions under which employers commonly seek to find solace: the business extension exception and the consent exception.

1. The Business Extension Exception

The business extension rule of the Wiretap Act exempts, as a violation, interception by certain devises that are:

> [F]urnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business . . . .[43]

---

[40] *See, e.g.*, CONN. PENAL CODE § 53a-189a; ARIZ. REV. STAT. § 13-3019; TEX. PENAL CODE ANN. § 21.15 (2011).
[41] 18 U.S.C. § 2511(4)-2511(5) (West 2012).
[42] 18 U.S.C. § 2520(c)(2) (West 2012).
[43] 18 U.S.C. § 2510(5)(a)(i) (West 2012).

At issue is what devices may be intercepted under the business extension rule, and when. The cases involving employer interception rather universally involve allegations that the interception was required, or at least allowed, under the concept of business necessity. Most of these cases involve the interception of telephone conversations. Fewer cases have involved other more recent technological methods, such as email or texting, logically because the primary communication system in place during the life of the acts has been the telephone and because of the question of what is an interception.[44]

An initial leading case in the application of the Omnibus Crime Control and Safe Streets Act of 1968 to the employment area is *United States v. Harpel*.[45] Although involving a police agency, the issue was not that of a police wiretap, but rather disclosure of a conversation believed to be taped at a police station. Briefly, the conversation of a police corporal with the Colorado Bureau of Narcotics and Dangerous Drugs was in some fashion recorded, presumably by placing a recording device on an extension telephone within the police department. Subsequently, defendant Harpel, a police employee, played the recording on at least two occasions in a local bar. Harpel was prosecuted and convicted at the district court level for disclosing an illegally intercepted wire communication. On appeal, the issue was that of whether or not there was, pursuant to the definition, an "interception." The crux of Harpel's argument was that the telephone extension was the intercepting instrument, and since it was provided by the service provider, falls outside of the definition of "electronic, mechanical, or other device" as required within the meaning of "intercept." Although the court found that the recorder was not the intercepting instrument, it provided further clarification of the exception under § 2510((5)(a) by holding that even though the telephone extension was the acquiring instrument, the exception applies only when the device is used in the ordinary course of business. Specifically, the court stated, "[we] hold as a matter of law that a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business."[46]

Building on the *Harpel* decision, *Briggs v. American Air Filter Co., Inc.*[47] more closely dealt with the issue of business necessity, or ordinary

---

[44] Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F.Supp.2d 548 (S.D. N.Y 2008) (access to emails previously sent not interception of electronic communication, but recognizing application of the Stored Communication Act); United States v. Ropp, 347 F.Supp.2d 831(C.C. Cal. 2004) (keystroke interception between keyboard and computer processing unit was not interception of electronic communication).

[45] United States v. Harpel, 493 F.2d 346 (10th Cir. 1974).

[46] *Id.* at 351.

[47] Briggs v. Am. Air Filter Co., Inc., 630 F.2d 414 (5th Cir. 1980).

course of business. A manager at American Air Filter suspected a current employee of providing company information to a former employee who was now working in competition with Air Filter. After cautioning the current employee the manager became aware of a telephone conversation between the current and former employees. The manager, in order to determine if confidential information was being shared, listened to the employee's conversation on a telephone extension and recorded by portable dictating machine part of the conversation. In ruling for Air Filter, the court gave weight to the admission of the plaintiffs that their conversation was business related. Since the call was not personal, and given the expressed concerns of Air Filter, the court found the conversation fell within the business extension exception.

In contrast to *Briggs*, however, *Watkins v. L.M. Berry & Co.*[48] considered the possible liability of an employer for the monitoring of an otherwise personal call by an employee discussing a job interview with another employer. Although the appeal was upon a summary judgment for the employer which was reversed and remanded, the issues again included that of consent and business extension. The defendant employer in *Watkins* relied upon the *Briggs* case for the proposition that a personal call may be classified in the ordinary course of business. In *Watkins*, however, there was no admission by the plaintiff that the call was business, as was the case in *Briggs*. In essence, the defendant's argument was that even though the call was of a personal nature, it included information of interest to the defendant and its enterprise, i.e., the continued performance of plaintiff. In declining the defendant's position the court observed: "The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company…. Her interview [referring to plaintiff] was thus a personal matter, *neither in pursuit nor to the legal detriment of Berry Co.'s business*."[49]

In an exceptional case, the business extension rule may be applied even to continual recording or interception. *Arias v. Mutual Central Alarm Service, Inc.*[50] presented the court with a company whose purpose was the monitoring of alarm calls for emergency services. Recommendations to the defendant, the Mutual Central Alarm Service, from numerous sources, including its underwriter, Underwriters Laboratories, and its trade association all stipulated that all incoming and outgoing calls be recorded as a matter of policy. Although at one time the system had audible beeps during the recording process, the beeps later stopped and the plaintiffs alleged that they were assured that their conversations were not being recorded. The dispute was stimulated due to a domestic quarrel between employees and relatives of

[48] Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).
[49] *Id*. at 582 (emphasis added).
[50] Arias v. Mut. Cent. Alarm Serv., Inc., 202 F.3d 553 (2d Cir. 2000).

employees. At issue was the question of whether the recording itself, even though not listened to, would be an aural acquisition. The court made no determination, but instead found that even if the recording was an aural acquisition, there were legitimate business reasons for such continual recording, thus falling within the business extension exception. Because of the nature of the enterprise and the desirability, if not necessity, of being able to archive the contents of emergency calls and responses, the recording was found to be in the ordinary course of business.

2. The Consent Exception

Unlike the business extension exception, which can be dependent on the type of intercepting device, consent is a specific exception to violation. Under federal law, it is not unlawful "to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception…[unless for the purpose of tort or crime]."[51] Consent, then, is the panacea of monitoring. Note, however, that some individual state laws require the consent of all parties to any intercepted or acquired communication.[52]

Express consent would provide the easiest case, but is noticeably absent from case law. Its absence is not really surprising given that the presence of express consent eliminates a case for wrongful interception under the federal statutes. The issue arises under the umbrella of implied or constructive consent; whether or not the knowledge by an employee of the monitoring of communications, such as by employment policy or beep noise during phone calls, is enough to constitute acknowledgement and permission by the employee.

Even a relatively benign recording policy which provides for business purpose interception or recording, but not that of personal, creates ambiguity which is problematic in practice. The *Watkins v. L.M. Berry*[53] case referenced above also involved the question of consent by the plaintiff due to the defendant's stated policy that only sales calls were monitored, not personal calls. In denying the consent argument made by the defendant, the court determined that the "knowledge of the capability of monitoring alone cannot be considered implied consent."[54] In circumstances where no express

---

[51] 18 U.S.C. § 2511(2)(d) (West 2012).
[52] *See* N.H. REV. STAT. § 570-A:2 (2010); CAL. PENAL § 632 (West 2012).
[53] *Watkins*, 704 F.2d 577.
[54] *Id*. at 581. *See also,* Ali v. Douglas Cable Commc'ns, 929 F. Supp. 1362, 1376 (D. Kan. 1996) (*quoting* Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir.1990)). "The circumstances giving rise to implied consent are case specific, but they 'ordinarily include language or acts

consent has been obtained, the cases are relatively agreed that an employer may monitor only for a sufficient time to identify communications as either business or personal. When identified as personal, then the monitoring must cease.

As the source of communication moves from the telephone to that of digital technology, the issue of consent becomes murky. Although it is common for employers providing access to their computer systems to their employees to have in place a policy restricting use for business purposes, it is widely recognized that personal use will occur. When employers monitor or review such use, including the history of employee websites visited, email recipients, and even the text of email's sent and received, the level of consent, and intrusion into privacy, becomes implicated.

B. *State Treatment*

The states, as is common, have a somewhat disparate treatment of privacy interests. In relation to interception of oral and wire communications, thirty-seven states have passed legislation which generally share the federal approach requiring only one party to a communication agree to its interception.[55] Twelve states require all parties to the communication consent to recording or interception.[56] The following table lists the states based on the general level of consent required for oral or wire communication interception.[57]

Clearly, knowledge of the degree of consent required under state law is necessary to any instance wherein listening to, or recording of, communications. But what of a communication between two differing jurisdictions with opposing requirements?

---

which tend to prove (or disprove) that a party knows of, assents to, encroachments on the routine expectation that conversations are private.'"

[55] *See* Ciocchitti, Corey A., *The Privacy Bailout: State Government Involvement in the Privacy Arena,* 5 ENTREPRENEURIAL BUS. L.J. 597, 610 (2010). *See also*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/electronic-surveillance-laws.aspx (last visited Mar. 3, 2012).

[56] Ciocchitti, *supra* note 55, at 610.

[57] The table is derived from and is substantially the same as found in the sources cited, *supra* note 55. Note that Vermont is not listed due to its having no legislative enactment dealing with communication interception.

Number of Parties to Consent	States
One	Alabama, Alaska, Arizona, Arkansas, Colorado, Delaware, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Missouri, Nebraska, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Texas Utah, Virginia, West Virginia, Wisconsin, Wyoming
All	California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, Washington

In *Kearney v. Salomon Smith Barney, Inc.*,[58] allegations of improper interception of communications were made in a choice-of-law decision. The defendant, Salomon Smith Barney (SSB), is a national brokerage firm with offices in both California and Georgia. As noted in the table above, Georgia requires that only one party consent whereas California requires that all parties consent. In the course of communicating with its California clients, both in calls to and from the clients, telephone calls at SSB's Atlanta, Georgia offices were routinely recorded without knowledge or consent of the California clientele. Upon discovery of the practice, California residents sued SSB in a class action seeking both an injunction and damages. The trial court found in favor of SSB, and the decision was affirmed on appeal to the intermediate appellate court, based on the more generous Georgia consent rule. The California Supreme Court reversed, however, choosing instead to apply the California consent statute, at least insofar as the injunctive relief. Recognizing that SSB was subject to California personal jurisdiction, the court declared that, "California clearly has an interest in protecting the privacy of telephone conversations of California residents while they are in California sufficient to permit this state, as a constitutional matter, to exercise legislative jurisdiction over such activity."[59] After finding that California had a superior interest to that of Georgia and that there was no extraterritorial application (application to communications originating and received outside of California) of a California statue, the California Supreme Court imposed

[58]Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914 (Cal. 2006).
[59] *Id*. at 921.

injunctive relief upon SSB, but declined to assess monetary liability for past conduct. Future conduct was clearly noticed in the court's statement that:

> In light of our decision, of course, out-of-state companies that do business in California now are on notice that, with regard to future conduct, they are subject to California law with regard to the recording of telephone conversations made to or received from California, and that the full range of civil sanctions afforded by California law may be imposed for future violations.[60]

The resulting conclusion to be drawn from *Kearny* is that intercepting or recording a communication within a state in which only one party is required to consent may be subject to sanctions should another party be situated in an all- party consent state. Any such decisions would obviously be complicated with issues of personal jurisdiction, but for multi-state enterprises the question of if they should monitor or record, and the structure for doing so, should be a leading priority.

IV. EMAIL MONITORING

As discussed above, when the communication acquisition occurs without the necessary consent, the concept of interception is a pivotal concept. Both the ECPA and similar state legislation utilize essentially the same terminology. Oral and telephone communications present the far easier cases, especially in light of the federal case law. Issues relating to email have proven more challenging due to the distinction of an email in transit and one resting in final storage.

The concept of interception has logically been interpreted to anticipate the acquisition of a message or communication in transit from the source to its destination, not access once it has been placed in storage.[61] The common attribute of employer's access to employee email has not involved the intermediate transfer, however, but later access directly to the employee's email account, typically on the employer's server, and therefore not in transit. At a minimum such intrusion by the employer implicates whether there is a reasonable expectation of privacy. If such a reasonable expectation is found to exist, even in the absence of state legislation, common law

---

[60] *Id*. at 938-39.

[61] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) ("[F]or a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage"). *See also*, State v. Brooks, 265 P.3d 1175 (Kan.App. 2011) (although not an employee case, holding emails improperly accessed months after initial transmission is not an interception).

principles of invasion of the right to privacy may be available if the intrusion would be highly offensive to a reasonable person.[62]

Use of employer equipment in itself, however, impacts the expectation of privacy. In a recent California decision email correspondence between an employee and her attorney was determined not to be secure.[63] The *Holmes* case involved a female employee alleging sexual harassment, wrongful termination, violation of the right to privacy, and intentional infliction of emotional distress. Due to a pregnancy the plaintiff requested leave from her newly acquired position as an executive assistant. Following her request the plaintiff felt that confidential information was disseminated by her employer and that there was excessive office commentary about her pregnancy. During the contentious time the plaintiff and her employer exchanged email, some of which the employer forwarded to the company human resources office, the company in-house counsel, and the payroll office. As the conflict escalated, the plaintiff corresponded by email with her attorney using a company laptop computer. Plaintiff was later instructed by her attorney to delete the emails from the laptop. Thereafter, during the trial preparation, the attorney for defendant questioned plaintiff in relation to the email correspondence which took place from the company laptop, thereby making plain that the defendant had retrieved the information. Although the decision is intertwined with a discussion of the attorney-client privilege, the court rejected the privacy claim with reliance on the plaintiff's prior receipt of notice within the company handbook of the defendant's "Internet and Intranet Usage" policy, which clearly warned of a lack of privacy right.[64] Recognizing the California provision which maintains the attorney-client privilege irrespective of the method of communication,[65] the court went on in *Holmes* to determine that:

> (1) when the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions. A communication under these circumstances is not a 'confidential communication between client and lawyer.

---

[62] RESTATEMENT (SECOND) OF TORTS § 652.
[63] Holmes v. Petrovich Dev. Comp., LLC, 119 Cal. Rptr.3d 878 (Cal. Ct. App 2011).
[64] *Id*. at 883. Among other provisions, the policy stated that the "company's technology resources should be used only for company business and that employees are prohibited from sending or receiving personal e-mails. Moreover, the handbook warns that '[e]mployees who use the Company's Technology Resources to create or maintain personal information or messages have no right of privacy with respect to that information or message'." *Id*.
[65] *Id*. at 895 (*citing* WEST'S ANN. CAL. EVID. CODE § 917).

> . . . .
> This is akin to consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by Petrovich would be privileged.[66]

Had there been no prior notice or policy, especially in view of the California constitutional right of privacy, the outcome might have been different. But due to a pleading deficiency the *Holmes* court did not address the constitutional issue.[67]

Contrary to the *Holmes* holding, however, is *Stengart v Loving Care.*[68] *Stengart* also involved employer recovery of attorney-client email for use in litigation with a non-governmental employee. As with *Holmes*, the plaintiff was provided with a laptop computer for her use. Unknown to plaintiff the laptop had spyware installed by the defendant. Using the company computer the plaintiff corresponded with her attorney, through an external Yahoo! email account, regarding a possible lawsuit against defendant. Plaintiff subsequently severed her employment with defendant and instituted her lawsuit. Due to the spyware and in preparation for suit, defendant forensically recovered the files from the laptop computer containing the email communication between plaintiff and her attorney.

In its review, the *Stengart* court looked specifically to the adequacy of notice to the employee as an element to what expectation of privacy the employee may reasonably retain. Unlike the *Holmes* policy, the *Stengart* policy was considered ambiguous. The policy of the defendant referenced company email accounts, but did not expressly implicate personal, external, accounts.[69] Additionally, while the defendant's policy stated that emails "are not to be considered private or personal to any individual employee,"[70] it included the statement that "[o]ccasional personal use [of e-mail] is permitted."[71] In its final analysis the *Stengart* court found that the plaintiff had a reasonable expectation of privacy, contrary to that in *Holmes.* In addition to the considered ambiguity, distinguishing characteristics of the *Stengart* fact pattern which proved instrumental for the court were that:

> Stengart plainly took steps to protect the privacy of those e-mails and shield them from her employer. She used a personal,

---

[66] *Id*. at 895-96.
[67] *Id*. at 900.
[68] Stengart v. Loving Care, 990 A.2d 650 (N.J. 2010).
[69] *Id*. at 658.
[70] *Id.*
[71] *Id*.

> password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer. In other words, she had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit.[72]

V. LABOR LAW IMPLICATIONS

Although privacy discussions predominantly concentrate on methods of interception and the resulting intrusion, the employer is also constrained by elements of labor law. For unionized environments it is imminently clear that monitoring employee organizational or unionization activities is forbidden, particularly when conducted in non-work areas such as break and lunch areas. It is possible, though, those areas not traditionally considered as subject to privacy expectations, and therefore not subject to bargaining, can become involved if treated by employees as gathering areas.[73]

More recently notoriety has come to the general protection of concerted activity[74] afforded in the National Labor Relations Act (NLRA) under its § 7 employee rights, especially in relation to employer monitoring of social media. In January 2012, the Acting General Counsel for the NLRB issued an amended report discussing fourteen NLRB cases occurring during the preceding year which dealt with employer actions and policies relating to social media.[75] The cases detailed had the common element of allegations of concerted activities by employees in pursuit of mutual aid in relation to hours, wages or conditions of employment. Many of the cases involved employer review or monitoring of employee statements made on Facebook or restrictive social media policies, and thus directly concern hazards of employer monitoring or reaction to social media comments. It is important to recognize that for purposes of application of the NLRA, an employer does not need to have any specific size or number of employees. Although some employers are excepted from the statute,[76] including federal and state

---

[72] *Id*. at 663.

[73] Brewers and Maltsters, Local Union No. 6 v. NLRB, 413 F.3d 36 (D.C. Cir, 2005). Anheuser-Busch, a brewing company was held in violation, due to a failure to bargain, of the National Labor Relations Act for having installed covert video cameras, without audio, in a rooftop elevator motor room after learning the room and roof were being used by employees for breaks, including the apparent presence of illegal substances. Note also that under the posting requirement of the NRLB as of April 2012, a specific example, included in the poster, of prohibited employer activity is to "spy on or videotape peaceful union activities."

[74] National Labor Relations Act, 29 U.S.C. § 157 (West 2012).

[75] Report of the Acting General Counsel Concerning Social Media Cases, Nat. Lab. Rel. Bd., Memorandum 12-31 (Jan. 24, 2012).

[76] 29 U.S.C. § 152 (West 2012).

governments and their subdivisions, the act applies generally to all employers who are acting in interstate commerce.[77]

Even though the concerted activities language of § 7 of the NLRA would seemingly anticipate two or more employees actively discussing unionization, the interpretation has been far broader. Concerted activities include "those 'engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself.' However, the activities of a single employee in enlisting the support of fellow employees in mutual aid and protection are as much concerted activity as is ordinary group activity."[78] Thus commentary such as the following Facebook exchange was found to be concerted activity even though not directly addressing a change in working conditions or discussing management:

- "a coworker feels that we don't help our clients enough . . . I about had it! My fellow coworkers how do u feel?
- What the f... Try doing my job I have 5 programs
- What the Hell, we don't have a life as is, What else can we do???"[79]

The use of derogatory or explicit language as noted above will not in itself remove employee comments from protection by virtue of being misconduct. Although it is possible for the employee's action to rise to the level of misconduct, a balancing test is applied involving, "(1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee's outburst; and (4) whether the outburst was, in any way, provoked by an employer's unfair labor practice."[80] Given the reasonably non-public, non-work environment nature of social media posts, a spirited discourse is very likely to be protected.[81]

If utilizing social media in review or monitoring of employees, employer policies are crucial. Language used in social media policies and employee handbooks have been the subject of multiple cases finding violation of the NRLA § 7 rights, or § 8(a)(1), wherein the employer action "interfere[s] with, restrain[s], or coerce[s] employees in the exercise of the

---

[77] *See Frequently Asked Questions*, NAT'L LABOR RELATIONS BD., http://www.nlrb.gov/faq/poster#t245n1702 (last visited Nov. 11, 2012). The NLRB does not regulate businesses that it determines have minimal impact on interstate commerce. NLRB guidelines establish monetary thresholds for determination of NLRB jurisdiction, dependent on the business. Examples of the threshold range from $50,000 in inflow or outflow of interstate goods for a non-retail business, to $500,000 in gross sales for a retail business.

[78] Hispanics United of Buffalo, Inc., 2011 WL 3894520 at 4 (N.L.R.B. Div. of Judges, 2011) (*citing* Myers Industries, 281 N.L.R.B. 882, 885 (1986)).

[79] *Id*.

[80] Atl. Steel Co., 245 N.L.R.B. 814, 816 (1979).

[81] *See* Hispanics United of Buffalo, Inc. *supra* note 78 at 5-6.

rights guaranteed in section 7."[82] Examples of policies that have recently been held to be violations in the NLRA include:

1. DirectTV U.S. policies were determined to unreasonably inhibit protected concerted activity including wages, hours, and working conditions. Employees were prohibited from: [83]

    - contacting the media;
    - discussing details about the job, company business or work projects with anyone outside the company, . . . via online posting or information-sharing forums, such as mailing lists, websites, blogs, and chat rooms;
    - blogging, entering chat rooms, posting messages on public websites or otherwise disclosing company information that is not already disclosed as a public record.

2. G4s Secure Solutions (USA) Inc. did not permit employees to:[84]

    - engage in unnecessary conversations at work (determined to be restrictive in application of discussions of unionization);[85]
    - give interviews or make public statements about the activities or policies of the company or clients without written permission from the company (overly broad – considered to be restrictive of discussing conditions of employment);[86]
    - to comment on work-related legal matters without express permission of the company legal department (undefined "legal matters" which employees could interpret to include discussing conditions of employment)

3. Hills and Dales General Hospital restricted employees from:[87]

    - making negative comments about our fellow employees and encouraged them to take every opportunity to speak well of

[82] National Labor Relations Act, 29 U.S.C. § 158(a)(1) (West 2012).
[83] DirectTV U.S. DirectTV Holdings, LLC., 2011 WL 6190411 at 12 (N.L.R.B. Div. of Judges, 2011).
[84] G4s Secure Solutions (USA) Inc., 2012 WL 1065721 (N.L.R.B. Div. of Judges, 2012).
[85] *Id*. at 15-16.
[86] *Id*. at 16.
[87] Hills and Dales General Hospital, 2012 WL 542765 (N.L.R.B. Div. of Judges, 2012).

other employees (implicitly prohibits negative comments about managers)[88]

- engaging in or listening to negativity or gossip ("ambiguous, imprecise and overbroad that a reasonable employee would construe it as prohibiting protected discussions about working conditions and the terms and conditions of employment.")[89]

4. Karl Knauz Motors, Inc. struck down employer policies :[90]

- that "[no] one should be disrespectful or use profanity or any other language which injures the image or reputation of the [employer]" (violated § 8(a)(1) by chilling § 7 rights to discussion of working conditions)[91]
- that any interviews not authorized by the employer and a requirement that information on any unauthorized interviews be reported (restricts rights to discuss working conditions)[92]
- that restricted information concerning employees from being disseminated to outside sources and all such requests should be referred to the employer (restricts rights to discuss working conditions)[93]

In the event an employer chooses to review social networking comments, any actions predicated on the review may come under scrutiny for NLRA violation. Unless employee comments are so extreme or threatening so as to lose protection, or a clear violation of an allowable policy, the employer is at risk of liability for an unfair labor practice. Employee manuals and guidelines can be helpful, but overly restrictive language, particularly that which would restrain open discussion of conditions of employment, or language which is vague or subjective such as negativity or legal, present enforcement problems. Employee comments complaining of employment or managerial conflicts, especially when inviting responses and when co-employees join the conversation, are a blatant danger for an employer if they respond.

---

[88] *Id*. at 4. *See also*, Salon/Spa at Boro, Inc. 356 N.L.R.B. No. 69 (2010)
[89] *Id*. at 6.
[90] Karl Knauz Motors, Inc., 358 N.L.R.B No. 164 (2012)
[91] *Id*. at 3.
[92] *Id*. at 4.
[93] *Id*. at 4.

VI. MANAGERIAL CONSIDERATIONS

A. *Employee Monitoring*

There is extensive academic literature on electronic monitoring which can be subdivided into the non-legal issues of the effects of electronic monitoring on employee behavior (performance), the effects of electronic monitoring on employee perceptions about the workplace and the ethics of electronic monitoring.

A number of empirical studies have been conducted to study the effect of electronic performance monitoring (EPM) on employee behavior. These studies have generally employed laboratory conditions to experimentally manipulate hypothesized variables effecting subject output.[94]

Results were mixed but may indicate that EPM can alter behavioral outcomes with highly skilled individuals increasing output, and less skilled reducing output, easy tasks being performed quicker but perhaps with more errors, and more difficult tasks with less proficiency. However, as noted by Phipps in 1996,[95] and again a decade later by Alder,[96] numerous confounding variables such as supportive or punitive climate, involvement, and reward structure have not been measured. Additionally, the employee monitoring studied involved repetitive task situations that could easily be counted and manipulated. Current technology for monitoring employees goes far beyond counting keystrokes and may have other, less obvious and longer-term impacts on employee behavior.

---

[94] John R. Aiello & Katherine J. Kolb, *Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress*, 80 J. APPLIED PSYCHOL. 339 (1995); Rick Davidson & Ron Henderson, *Electronic Performance Monitoring: A Laboratory Investigation of the Influence of Monitoring and Difficulty on Task Performance, Mood State, and Self-Reported Stress Levels,* 30 J. APPLIED SOC. PSYCHOL. 906 (2000); Traci L. Galinsky, Lawrence M. Schleifer & Christopher S. Pan*, The Influence of Performance Standards and Feedback on Speed and Accuracy in an Electronically Monitored Data-Entry Task*, 7 INT'L J. HUM.-COMPUTER INTERACTION 25; Ron Henderson, Doug Mahar, Anthony Saliba, Frank Deane & Renee Napier, *Electronic Monitoring Systems: An Examination of Physiological Activity and Task Performance Within a Simulated Keystroke Security and Electronic Performance Monitoring System*, 48 INT'L J. OF HUM.-COMPUTER STUDIES 143 (1998); D. Scott Kiker & Mary Kiker, *A Quantitative Review of Organizational Outcomes Related to Electronic Performance Monitoring*, 11 BUS. REV. 295 (2008) (available at http://search.proquest.com/docview/197297876?accountid=5683); G. Stoney Alder, Marshall Schminke, Terry W. Noel & Maribeth Kuenzi, *Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation*, 80 J. BUS. ETHICS 481 (2008).

[95] Polly A. Phipps, *Electronic Monitoring in the Workplace*, 119 MONTHLY LAB. REV. Vol 119, 33 (1996).

[96] G. Stoney Alder, Marshall Schminke, Terry W. Noel & Maribeth Kuenzi, *Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation*. 80 J. BUS. ETHICS 481 (2008).

Other studies have focused on the perceptions held by employees concerning electronic monitoring.[97] Some of the factors that might mediate the effects of monitoring include procedural justice, invasion of privacy, role conflict and ambiguity, self-esteem, stress, and locus of control. These studies tend to indicate that the implementation and management of the monitoring, rather that the monitoring itself, is a significant contributing agent to the acceptance of electronic monitoring. With "proper implementation" it seems possible that employees will perceive electronic monitoring as "just", non-invasive and producing little stress. However, there are apparently some differences associated with personality factors. Internally controlled individuals seem to be more prone to stress and may suffer some loss of job control and self-esteem. In a comprehensive review of the literature, Stanton[98] combined the traditional literature on all forms of employee monitoring to develop a framework of employee reactions to traditional and electronic monitoring. As noted by Stanton, much of the literature on traditional monitoring has a high degree of relevance to electronic monitoring. Yet electronic monitoring has unique characteristics that separates it from traditional monitoring. The computer can be everywhere; it never sleeps, and has an unfailing memory.

The final aspect of employee monitoring to be discussed concerns the ethics of electronic monitoring. From a legal perspective, illegal electronic monitoring would also be unethical. However, the perceptions of both management and employees' as to what is, or is not, ethical may be somewhat more ambiguous. As part of the ethicist philosophy there are

---

[97] Bradley J. Alge, *Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice*, 86 J. APPLIED PSYCHOL., Special Issue 797 (2001); Carl Botan, *Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects*, 63 COMM. MONOGRAPHS 293 (1996*)*; Pascale Carayon, *Effects of Electronic Performance Monitoring on Job Design and Worker Stress: Results of Two Studies,* 6 INT'L J. OF HUM.-COMPUTER INTERACTION 177 (1994); Pascale Carayon, *Effect of Electronic Performance Monitoring on Job Design and Worker Stress: Review of the Literature and Conceptual Model*, 35 HUM. FACTORS 385 (1993); Kathryn Kolb & John R. Aiello, *The Effects of Electronic Performance Monitoring on Stress: Locus of Control as a Moderator Variable*, 12 COMPUTERS IN HUM. BEHAV. 407 (1996); Jeffery M. Stanton, *Traditional and Electronic Monitoring from an Organizational Justice Perspective*, 15 J. BUS. & PSYCHOL. 129 (2000); Jeffery M. Stanton & Janet L. Barnes-Farrell, *Effects of Electronic Monitoring on Personal Control, Task Satisfaction, and Task Performance,* 18 J. APPLIED PSYCHOL. 738 (1996); Jeffery M. Stanton & E.M. Weiss, *Electronic Monitoring in Their Own Words: An Exploratory Study of Employees' Experiences with New Types of Surveillance,* 16 COMPUTERS IN HUM. BEHAV. 16, 423-440 (2000); G. Stoney Alder, Marshall Schminke, Terry W. Noel & Maribeth Kuenzi, *Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation,* 80 J. OF BUS. ETHICS 481 (2008).

[97] Jerry M. Stanton, *Reactions to Employee Performance Monitoring: Framework, Review, and Research Directions,* 13 HUM. PERFORMANCE 85 (2000).

[98] *Id*.

multiple concepts to consider such as distributive justice, utilitarianism, personal liberty, reciprocity, and the categorical imperative.[99] Each of the philosophical concepts deals with the human condition and individual "rights" in society and in the workplace. It also appears that the methods used, use of information gained from monitoring, and disclosure of employment monitoring are critical to management and employees accepting electronic monitoring as ethical.[100] Up until now, a system of electronic monitoring that is implemented and used "correctly" may well be accepted as ethical by both employees and management.

An additional aspect of electronic monitoring is that of non-performance monitoring, i.e. monitoring the activities of employees while at the workplace, but not working. Technology now enables employers to monitor virtually all aspects of an employee's behavior while at the workplace. They also have the ability to monitor not only the lower level employees such as clerical data entry or telephone employee, but the intellectual and managerial employee as well. And they can do the monitoring openly or secretively.

B. *Suggested Guidelines*

As the use of electronic monitoring has become more prevalent a number of authors have suggested guidelines for the proper implementation and use of such systems.[101] Every organization that uses computers, e-mail and the Internet already has the basic hardware for a monitoring system in place and needs to establish a set of policies and guidelines to ensure legal and proper use and control. An organization, first of all, needs a "good" reason for electronic monitoring. The definition of "good" is, of course,

---

[99] Thomas J. Hodson, Fred Englander & Valerie Englander, *Ethical, Legal and Economic Aspects of Employer Monitoring of Employee Electronic Mail*, 19 J. BUS. ETHICS 99 (1999); Philip Brey, *Worker Autonomy and the Drama of Digital Networks in Organizations,* 22 J. BUS. ETHICS 15 (1999); G. Stoney Alder, *Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives*, 17 J. BUS. ETHICS 729(1998).

[100] Frances S. Grodzinsky, Andra Gumbus & Stephen Lilley, *Ethical Implications of Internet Monitoring: A Comparative Study*, 12 INFO. SYS. FRONTIERS 433 (2010).

[101] Milton Zall, *Employee Privacy*, 66 J. PROP. MGMT 16 (2001); *E-policy Guidance Where Few Laws Exist*, HR FOCUS Vol 78(7), 7 (2001); Jitendra M. Mishra & Suzanne M. Crampton, *Employee Monitoring: Privacy in the Workplace?*, 63 S.A.M. ADVANCED MGMT J. 4 (1998); Todd Raphael, *Does HR Want to Digital Snoop?,* 80 WORKFORCE Vol. 96 (2001); Joann Greco, *Privacy*, 22 J. BUS. STRATEGY 32 (2001); Miriam Schulman, *Little Brother is Watching You*, 100-101 BUS. & SOCI. REV. 65 (1998); Mark F. Asman & Patricia A. Essex, *Electronic Monitoring of Employees*, 60 OHIO CPA J. 25 (2001); David W. Arnesen & Williamson L. Weis, *Developing an Effective Company Policy for Employee Internet and Email Use*, 11 J. ORG. CULTURE, COMM. AND CONFLICT 53 (2007) (available at http://search.proquest.com/docview/216597269?accountid=5683).

unclear and dependent on the environment in which the organization exist and the perceptions of the employees.

For example, a retail establishment may monitor employees through electronic cash registers, electronic inventory control and video. The justification for this monitoring is security of the goods (loss prevention) as well as performance monitoring (number of scans per hour). Additionally, video monitors the behavior of customers to prevent shoplifting and reduce the company's liability. All of these are legitimate justifications for close monitoring. In addition to having a "good" reason for monitoring, an organization will generally want to adopt a set of policies pertaining to the use of data acquired by monitoring and who has access to that data. Some data electronically stored, such as health records, may be protected by federal statute. Some employee conversations may be protected because of wiretapping or concerted union activity. Some areas may be deemed as unsuitable for monitoring such as break rooms, clean up areas, and restrooms. An organization may already have policies about health records and union activities and probably would not need to be changed. Other items such as the exclusion of specific locations for monitoring could be included in the policy.

For successful implementation of a specific built electronic performance monitoring program, and as a by-product of surveillance, communications may be the key. Once again legitimate reasons for the monitoring should be communicated and the information used in the manner specified. If the purpose is for training, the monitoring should be used to specify training needs and can be used in a positive manner. If, however, the training data is used to discipline or terminate an employee then the policy is not being followed and other employees may view the monitoring as unjust. As with any performance evaluation system you should monitor only important tasks that can be adequately measured and monitor "good" as well as "bad" behavior. To help achieve a sense of justice there should also be mechanisms for employee input, participation, error correction and feedback.

In an organization where the monitoring is done for security purposes, clearly specifying who has access to the data, and for what reasons, should also be included. It may be advisable to limit the surveillance of employees to security personnel, keeping security personnel separate from the other employees, and limiting access to security data.

Recommendations for employers include:

- Obtain express consent of all employees to all forms of communication. For those employees currently employed, it would be advisable to provide some additional consideration to support their consent. Even in an employment at will jurisdiction the

additional consideration would be desirable should the extent of consent be challenged based upon coercion.

- Be familiar with state and local law. Even though the federal act would provide consent with only that of one party, some state laws require all parties to consent. The courts will be justified in using the more restrictive rules and may find violations upon application of choice-of-law criteria. Also be aware that consent of an employee to monitoring or recording will not bind the odd visitor who might use business facilities and find their communications monitored.
- Post notices in all appropriate locations, together with periodic memoranda to all employees. Upon the computer systems, provide a boot screen with periodic reminders notifying employees that the system is the property of the enterprise, is for the sole purpose of business activity, and is therefore subject to monitoring. If telephone systems are to be monitored and employees are to be restricted from making personal calls, provide alternate phones for personal use.
- If monitoring and/or recording, if possible and feasible choose equipment provided by the service provider. Consider utilizing equipment that provides periodic notice of monitoring, such as a beep tone.
- Provide appropriate instruction to those who might monitor. Particularly, school management in the business extension rules which would allow monitoring sufficient to identify the character of the communication, but not beyond if personal.
- Consider the toll on morale that monitoring, especially extensive monitoring, may entail.
- If monitoring is to take place, do so in an even-handed fashion. Have an articulable reason with significant business justification. If personal communications are to be restricted as a policy matter, apply the policy to all levels.
- Be cautious of general monitoring, and particularly recording.
- If cameras are to be utilized, be aware that the addition of sound will bring the activity within the wiretap act. Additionally, recognize that video may entail other hazards within the common law arena, such as invasion of privacy, particularly if used in sensitive areas such as locker rooms or rest rooms, or involving labor law if monitoring in any way involves union activity or chills the concept of concerted activity.
- Be wary of policies, actions, or discipline which could be considered associated with an employee effort for discussion or action in relation to working conditions, wages, or hours.

VII. CONCLUSION

As the use of the Internet has become ubiquitous in the workplace, management has become confronted with the world of email, blogs, instant messages, social networks, global positioning systems and a host of newer technologies that simply did not exist a few years earlier. Has management kept up with these changes and have they reacted appropriately? The answer is probably yes, but slowly. Due to the fear of lawsuits, security issues and lost productivity, many companies have begun to enforce the rules and policies regarding Internet use. Results of the 2007 AMA survey (2007 AMA Survey) indicate that of the 30% of the bosses that have fired employees for inappropriate Internet use, 84% of the employees were fired for viewing, downloading, or uploading inappropriate/offensive content, 48% for violation of any company policy, and 34% for excessive personal use. Are these firings justified and accepted as proper by the remaining employees?

It is likely that the perceptions of employees concerning electronic monitoring have changed, and that the workplace of the future may be substantially different from today. As the legal landscape changes, it will behoove the organization to carefully maintain a watchful eye on current practices and policies. Additionally, future research into the uses of technology to monitor the behavior of employees needs to address the long-term effects of electronic monitoring on employee behavior, and provide additional direction for management decision-making. Although we have monitored employee behavior for developmental, discipline, promotional, and a host of other reasons, the use of computer technology may well have added additional confounding elements. A number of potential factors worthy of research including the pervasiveness and invasiveness of monitoring, stress induced reactions, trusts in management, and perceived fairness. These individual characteristics will also need to be evaluated in light of potential group dynamic interactions like norms, cooperation, boundaries, concerted activity, and cohesiveness.