



Every Breath You Take:
Blogging, Texting, E-mails and Social Networking
in the Workplace

Eric L. Barnum and Nora Kersten Walsh

American Bar Association
Section of Labor and Employment

3rd Annual CLE Conference
Washington

November 5, 2009

One Atlantic Center, Suite 2300
1201 West Peachtree Street
Atlanta, Georgia 30309
t 404.437.7000 f 404.437.7100

225 Franklin Street, Suite 2600
Boston, MA 02110
t 617.848.5750 f 617.848.5784

6600 Sears Tower
233 South Wacker Drive
Chicago, IL 60606-6473
t 312.258.5500 f 312.258.5600

One Westminster Place
Lake Forest, IL 60045-1885
t 847.295.9200 f 847.295.7810

900 Third Avenue
New York, NY 10022
t 212.753.5000 f 212.753.5044

One Market
Spear Street Tower
Thirty-Second Floor
San Francisco, CA 94105
t 415.901.8700 f 415.901.8701

1666 K Street NW, Suite 300
Washington, DC 20006
t 202.778.6400 f 202.778.6460

www.schiffhardin.com

Introduction¹

For all its efficiencies and productivity enhancements, technology in this digital age continues to trend well ahead of American jurisprudence. We have found more ways to exchange information about where we are, what we're doing, where we're going and what we'll do when we get there than can possibly be consumed in a rational and thoughtful manner. One can only wonder whether Sting knew the prophecy of his words when he penned the lyrics

Every breath you take and every move you make
Every bond you break
Every step you take, I'll be watching you
Every single day and every word you say
Every game you play
Every night you stay, I'll be watching you²

Electronic mail, internet blogging, cellular phone text messaging, instant messaging, and global positioning satellite systems (GPS) are only some of the tools available to employers and employees to help them communicate with customers, clients and co-workers. Managing these tools has proven to be difficult for employers as more companies try to avoid liability for improper use of company information technology. The "now" phase of communicating has created an even more complex set of rules for workplace interaction.

What appears to be an irreversible cultural phenomenon has created a multitude of employment and labor law issues for management. "Social networking" – whether it be Facebook®, Twitter®, Myspace®, LinkedIn®, Friendster® or any of the other up-and-coming networking sites – is here to stay and employers need to adapt. The statistics regarding the explosion of "social networking" sites tells the story. According to a Deloitte LLP 2009 survey³, 55% of employees admit to visiting social

networking sites at least once a week. Twenty percent admit to visiting social networking sites during work hours. Thirty-one percent of American CEOs are on Facebook, while 30% say they use social networking as part of their business and operational strategies. Another 23% use social networking for recruiting purposes. Still, there seems to be a disconnect between what management does and what they believe is right for their businesses. Seventy-four percent of managers surveyed believe social networking sites put the firms and their brand at risk. Fifteen percent consider the risks of social networking sites at the boardroom level, but only 17% have risk mitigation policies or programs in place.

What about the inherent conflict between what companies want to say about themselves and what employees have to say about the company – or one another? According to the Deloitte study, 60% of managers believe they have the "right to know" what their employees are saying about the company on the employees' personal (and private) social networking web pages. Fifty-three percent of employees say their social networking content is none of the company's business, and 33% of employees never even consider the business implications of their postings.

This clash of perspectives often leaves employers in a no-man's-land of drafting fair and effective employment policies to control the flow of information. Employers feel compelled to do something to protect their employees, and at the same time protect their company brand and company assets. This paper will discuss these issues and offer some practical solutions to avoid liability pitfalls. The first place to start, however, is with a discussion of some of the applicable laws of employee monitoring.

I. Federal Law

The federal Electronic Communications Privacy Act ("ECPA") prohibits the unauthorized interception of wire, oral or electronic communication. 18 USC §§ 2510-2521. An "interception" 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. *Id.* § 2510(4). Criminal penalties for a violation of the ECPA can include a fine or imprisonment up to five years. *Id.* § 2511(4)(a). Further, individuals whose communications were intercepted under this section can bring a civil action against the person or entity who engaged in the violation for damages including preliminary or equitable relief, actual damages, statutory damages amounting to the greater of \$100/day for each day of the violation or \$10,000, punitive damages, and attorney's fees. *Id.* § 2520(a)(c).

There are two exceptions to the ECPA relevant to this analysis: the consent exception and the business extension

¹ Eric L. Barnum is partner in the Labor and Employment Law practice group at Schiff Hardin LLP, resident in the Atlanta, Georgia office. Mr. Barnum received his law degree from Pacific McGeorge School of Law and his Bachelor of Arts from the University of California, Los Angeles. Nora Kersten Walsh is a senior associate on the Labor and Employment Law practice group at Schiff Hardin LLP, resident in the Chicago, Illinois office. Ms. Walsh received her law degree from the University of Wisconsin Law School and her Bachelor of Arts from College of the Holy Cross.

² Taken from "Every Breath You Take", from the 1983 album *Synchronicity*, written by Sting and performed by The Police.

³ "Social Networking and reputation risk in the workplace" Deloitte LLP 2009 Ethics & Workplace Survey. http://www.deloitte.com/dtt/cda/doc/content/us_2009_ethics-workplace_survey_150509.pdf.

exception. Courts view the applicability of these exceptions as fact-specific.

A. Consent Exception

The “consent” exception is the most significant exception to the ECPA. Theodora R. Lee, Wrongful Termination Claims: What Plaintiffs and Defendants Have to Know, 651 PLI/LIT 477, 547 (2001). Under the “consent” exception, a party to a communication can “consent” to an otherwise impermissible monitoring of the communication:

It shall not be unlawful under this chapter for a person. . .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 such communication is intercepted for the purpose of committing any criminal or tortious act. . .

18 U.S.C. § 2511(2)(d). Thus, employers will not face liability under the ECPA as long as it obtains consent from at least *one* of the parties to the communication. Consent under the ECPA can be either express or implied. One author noted that because the determination of whether there is implied consent is highly fact-specific, employers should attempt to obtain express consent in writing. Lee, Wrongful Termination Claims: What Plaintiffs and Defendants Have to Know, 651 PLI/Lit at 545.

Implied consent is inferred from the surrounding circumstances indicating that the party knowingly agreed to the surveillance. Laughlin v. Maust, 1997 WL 436224 at *5 (N.D.Ill. Aug. 1, 1997) (Reinhard) (restaurant employee who was notified that its main business line would be monitored had impliedly consented to the recording, but employees who had not been notified had not impliedly consented). Cases addressing implied consent seem to indicate that as long as an employer notifies its employees that *all* calls or *both work* and *personal* calls at certain phones or workstations might be subject to monitoring, an employer will probably not face liability if it picks up an occasional personal call on a telephone earmarked for quality control monitoring.

Consent, however, is not to be “cavalierly implied.” Abbott v. Village of Winthrop Harbor, 953 F. Supp. 931 (N.D.Ill. 1996) (fact that plaintiffs heard beep tones indicative of the “tapped phones” when using the line was insufficient to create “consent”); Deal v. Spears, 980 F. 2d 1153, 1157 (8th Cir. 1992) (informing employee that he “might” monitor was not sufficient to obtain “consent”); Watkins v. Berry, 704 F. 2d 577, 579-81 (11th Cir. 1983) (where employer told employees that personal calls would not be monitored except to the extent necessary to determine whether a call

was personal or business related, monitoring of a personal call might violate ECPA).

Given that the ECPA requires the consent of only *one party*, employers should not face liability under the ECPA for monitoring calls with the consent of its employees. The fact that both incoming and outgoing calls are monitored should not effect the analysis.

B. The Business Extension Exception

The business extension exception provides an alternative, although less clear-cut, defense for employers who face liability for monitoring communications under the ECPA. 18 USC § 2510(5)(a)(i). Unlike the consent exception, this exception is not explicitly provided as an exception in the statute. Rather, courts have anchored it within the definition of the phrase “electronic, mechanical, or other device” (an “intercept” requires the use of a “mechanical, electronic, or other device”). The phrase is defined as:

Any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than –any telephone or telegraph instrument, equipment or facility, or any component thereof, i) furnished to the subscriber or user by a provider . . . in the ordinary course of its business and being used by the subscriber 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. . . .

Therefore, the exception is derived from an inference - telephone equipment used for intercepting communications furnished by a subscriber used in the ordinary course of business is not a “mechanical, electronic, or other device.” If an employer uses such equipment while monitoring a phone call for business purposes, there is no unlawful “intercept.” The applicability of this exception thus depends upon the equipment used for monitoring and the reasons for monitoring. At least one court has held that consent is *not* a component of this exception. Arias v. Mutual Central Alarm Svc., Inc., 202 F.3d 553, 559 (2d Cir. 2000).

The business extension exception is highly fact-intensive and has received diverse treatment. Courts focus first on the kind and source of equipment used to intercept to determine the applicability of the exception. Laughlin v. Maust, 1997 WL 436224 at *3 (recording phone calls through an adapter and recorder attached to a main business line, where the employer merely recorded, but did not “listen in” and where the recording device at issue was not provided by the telephone company, did not satisfy the extension); Watkins v. Berry, 704 F. 2d at 582 (recording device purchased at Radio Shack attached to a phone extension did not qualify for the extension); Amati v. City of

Woodstock, 1997 WL 857493 at * 3 (N.D. Ill. 1997) (“[A] vast majority of the circuit courts of appeals having [addressed this issue] have held that a recorder acquired via a third party and attached to a telephone line does not fall within the exemption of section 2510(5)(a)”).

Courts also address the nature of the calls intercepted and reasons for doing so. Epps v. St. Mary’s Hospital, 802 F.2d 412, 416 (11th Cir. 1986). See also Smith v. Devers, 2002 WL 75803 at *3 (M.D. Ala. Jan. 17, 2002) (“It is quite apparent that the complete interception of personal phone calls of an employee is not and can never be protected behavior under the business-extension exemption. That exemption allows only the interception sufficient to determine the personal nature of the call.”)

It seems clear that training and quality control purposes would qualify to be within the ordinary course of business. But, without knowing exactly how a particular client monitors their employees, or whether personal calls and e-mails are also monitored, it is difficult to predict whether they could seek refuge under the business extension exception. It does appear that in order to meet this exception, they must monitor through equipment provided by their telephone service provider, and must refrain from recording personal calls once they determine that the call is personal.

Congress passed the Stored Communications Act as part of the Electronic Communications Privacy Act. The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address. The Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2711, makes it an offense to “intentionally access a facility through which an electronic communication service is provided . . . and thereby obtain . . . access to a wire or electronic communication while it is in electronic storage in such system.” It is possible, therefore, that an employer could face liability under the SCA for accessing an employee external website where that website is password protected or contains other security measures – and the employer does so without the employee’s authorization.

Like the ECPA, the SCA contains an exception from potential liability if the conduct is, in fact, authorized by the person using the service with respect to any communication intended for the user. 18 U.S.C. § 2701(c)(2).

II. State Law

Various states have also adopted some form of the ECPA or the SCA. This paper will review a small sampling of these states – Illinois, New Jersey, Ohio, Georgia and California. See, e.g., 720 ILCS § 5/14-2; NJ

ST 2A: 156A-3(a); OH ST § 2933.52(A)(1); GA ST § 16-11-65; CA PENAL § 632(a). Each statute contains a consent exception in some form, although two states – Illinois and California - require the consent of *both* parties to the communication for the consent exception to apply. A brief overview of the five state wiretap statutes follows.

A. Illinois

The Illinois Eavesdropping Statute prohibits the monitoring of communications without the consent of all parties:

A person commits eavesdropping when he 1) knowingly and intentionally uses an eavesdropping device for the purpose of hearing or recording all or any part of any conversation or intercepts, retains, or transcribes electronic communication unless he does so A) with the consent of all of the parties to such conversation or electronic communication or B) in accordance with Article 108A of Article 108(B) of the Code of Criminal Procedure...

720 ILCS § 5/14-2.

The statute defines “conversation” as an “oral communication between two or more persons regardless of whether one or more of the parties intended their communication to be of a private nature under circumstances justifying that expectation.” Id. § 5/14-1(d). This definition, added by the Illinois legislature in December 1994, was intended to eliminate the confusion caused by two Illinois Supreme Court decisions which disregarded the “all parties” requirement: People v. Beardsley and People v. Herrington. Instead, the relevant analysis under the amended Illinois Eavesdropping Statute is not whether the parties had an expectation of privacy, but rather whether the “eavesdropper” obtained the consent of all parties before recording.

Similar to the ECPA, consent under the Illinois Eavesdropping Act can be either express or implied. Consent exists where a person’s behavior exhibits “acquiescence or a comparable voluntary diminution of his or her otherwise protected rights.” People v. Ceja, 204 Ill.2d 332, 349 (2003) (inmates who knew their conversations were being monitored had impliedly consented to monitoring). Implied consent is consent in fact, and is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance, and thus, language or acts indicating that a party *knows of* the recording should suffice. Id. at 349-50.

The Illinois Eavesdropping Act also contains Exemption “j” - a more limited exemption to the statute. Although no case law exists interpreting this exemption, Exemption “j” allows businesses engaged in “telephone solicitation” to monitor the phone calls of “telephone solicitors” for quality

control purposes, employee education, and internal research as long as at least one party (presumably the employee) consents to the recording. Id. § 5/14-3(j). “Telephone solicitation” is defined as a “communication through the use of a telephone by live operators (i) soliciting the sale of goods or services; (ii) receiving orders for the sale of goods or services; (iii) assisting in the use of goods or services; or (iv) engaging in the solicitation, administration, or collection of credit accounts. Id.

Under the statute, an employer seeking to record conversations under this exemption cannot use any portion of a recorded conversation in an administrative, judicial or other proceeding, nor can the employer divulge the conversation to any third party. Id. Further, an employer must terminate recording upon learning that the conversation that does not relate to telephone solicitation, and must provide current and prospective employees with notice that the monitoring or recordings may occur, including “prominent signage.” Id. And finally, a business entity using a telephone monitoring system pursuant to this exemption must provide their employees access to a personal-only phone line which is not subject to recording. Id.

A first violation of the Illinois Eavesdropping Act is considered a Class 4 felony, and subsequent offenses are considered a Class 3 felony. Id. at 5/14-4. Further, injured parties are entitled to the following civil remedies: an injunction prohibiting further eavesdropping; actual and punitive damages against the eavesdropper; actual and punitive damages against any landlord, building owner, or common carrier who assists with or permits the eavesdropping. Id. § 5/14-6.

B. New Jersey

Under the New Jersey Wiretapping and Electronic Surveillance Control Act (“New Jersey Act”), any person who “purposely intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication” is guilty of a third degree crime. NJ ST 2A: 156A-3(a). The statute also prohibits the disclosure or use of unlawfully obtained communications. Id. § 156A-3(b)(c). Unfortunately, the New Jersey state courts have not applied this Act in the employment context. New Jersey Practice Series: Privacy in the Workplace, 18 NJPRAC § 13.11. But because the New Jersey Act was modeled after the federal ECPA, New Jersey courts have looked to federal decisions for guidance in interpreting this statute. Id.; Cacciarelli v. Boniface, 325 N.J. Super. 133, 137, 737 A.2d 1170, 1173 (NJ Sup. 1999).

Similar to the ECPA, the New Jersey Act contains a *single-party consent* exception. The statute exempts interception of communications where the person is “a party to the

communication or one of the parties to the communication has given prior consent to such interception unless such communication is intercepted or used for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States.” NJ ST 2A: 156A-4(d). Presumably, because the New Jersey courts look to federal decisions for guidance, consent under the New Jersey Act can be either express or implied.

Further, the New Jersey Act contains a “business extension exception” virtually identical to that of the ECPA, and has been interpreted in the same way. Pascale v. Carolina Freight Carriers Corp., 898 F.Supp. 276, 281-82 (D. N.J. 1995) (“Since New Jersey Courts have looked to constructions of the federal act when interpreting the New Jersey wiretap statute. . . this Court will rely upon the cases interpreting the federal business extension exception”). In Carolina Freight Carriers, an employer investigating an employee’s possible criminal activity connected tape recorders to three extension phones with a Radio Shack wire in order to record all incoming and outgoing calls. The United States District Court of New Jersey held that because the “intercepting devices” were not provided by the phone company, and the recorders were not “telephone or telegraph instruments”, the employer could not meet the business extension exception under either the ECPA or the New Jersey Act. Id.

C. Ohio

Similarly, Ohio’s wiretap statute prohibits any person from intercepting, attempting to intercept, or procuring another person to intercept a wire, oral or electronic communication. R.C. § 2933.52(A)(1). Violation of this statute is considered a fourth degree felony. Id. § 2933.51(I). And persons whose communications are unlawfully intercepted may bring a civil action against the person or entity that engaged in the violation for damages including equitable relief; either liquidated damages at a rate of \$200/day for each day of violation or damages of \$10,000, whichever is greater; actual damages; punitive damages; and reasonable attorneys fees. Id. § 2933.65(A).

The Ohio statute contains a *single-party consent* exception, stating that the prohibition does not apply to:

A person who is not a law enforcement officer and who intercepts a wire, oral or electronic communication or if one of the parties to the communication has given the person prior consent to the interception, and if the communication is not intercepted for the purpose of committing a criminal offense or tortious act...

Id. § 2933.52(B)(4). Use of a phone with knowledge of a monitoring practice constitutes consent. State v. Smith, 117 Ohio App. 3d 656, 662, 691 N.E. 2d 324, 328 (Oh. Ct. App. 1997).

The Ohio wiretap statute also contains a business extension exception similar to that of the ECPA. Id. § 2933.51(D)(1)(c); First v. Stark County Board of Commissioners, 234 F.3d 1268, (6th Cir. 2000) (*unpublished decision*) (noting the exceptions in both the ECPA and the Ohio wiretap statute).

D. Georgia

Georgia has adopted a similar wiretap statute which provides that the following activities are unlawful:

(1) Any person in a clandestine manner intentionally to overhear, transmit, or record or attempt to overhear, transmit or record the private conversation of another which shall originate in any private place;

(2) Any person, through the use of any device, without the consent of all persons observed, to observe, photograph, or record the activities of another which occur in any private place and out of public view...

GA ST § 16-11-65. A violation of the Georgia wiretap act is a felony and punishable by imprisonment up to five years or a fine up to \$10,000, or both. Id. § 16-11-69.

The statute contains a *single-party consent* provision which states that “nothing in Code Section 16-11-62 shall prohibit a person from intercepting a wire, oral or electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.” Id. § 16-11-69. It further contains a form of the business extension exception, providing that a “device” used for recording does not include a “telephone or telegraph instrument, equipment, or facility or any component thereof: furnished to the subscriber or user by a provider or wire or electronic communication service in the ordinary course of business and being used by the subscriber or user in the ordinary course or 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...” Id. § 16-11-60.

The Fifth Circuit Court of Appeals did apply the federal ECPA’s business extension exception in finding that a Georgia employer did not violate the ECPA when it “listened in” on an extension telephone to the conversation of an employee whom it believed was disclosing confidential company information. Briggs v. American Air Filter Co., Inc., 630 F.2d 414 (1980).

The Georgia wiretap statute contains an additional relevant exception that permits employers to monitor telephonic communications for “business service improvement.” GA ST § 16-11-65. This section requires, however, that the employer use equipment furnished by a telephone company authorized to do business in Georgia, and that the employer first apply for and obtain a license to install and use the equipment from the Georgia Public Service Commission. Id. Licenses are issued to applicants who demonstrate a “clear, apparent and logically reasonable need” for the use of the equipment in connection with a legitimate business activity and that the equipment will be operated lawfully and by persons “of good moral character.” Id. This section has not been interpreted by any courts of law, however.

E. California

California has adopted the Invasion of Privacy Act (“the Act”) which prohibits, among other conduct, the recording of or eavesdropping upon “confidential” communications without the consent of *all parties* to the communication:

Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), or imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

CA PENAL § 632(a). This provision is distinct from the Act’s “wiretapping” provision at § 631(a). In addition to criminal penalties, the statute provides for a civil action against the person who committed the violation for the greater amounts of \$5000 or three times the amount of actual damages, if any, sustained, as well as an action enjoining the continuing violation. CA PENAL § 637.2(a)(1)(2).

As noted, the Act requires the consent of all parties to a conversation before monitoring or recording. See, e.g., Coulter v. Bank of America Nat. Trust and Savings Assoc., 33 Cal. Rptr.2d 4th 766, 28 Cal. App. 4th 923 (Cal. App. 1994) (employee’s recording of private communications with his co-workers without their consent violated the Act). And the Act defines a “confidential” communication as any communication “carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto...” Id. § 632(b). The California Supreme Court interpreted this

provision to mean that a communication is “confidential” if a party to the conversation has an objectively reasonable expectation that it is not being overheard or recorded. Flanagan v. Flanagan, 117 Cal. Rptr. 2d 574, 580, 41 P.3d 575, 581 (2002). The Act protects against intentional, nonconsensual recording of telephone conversations regardless of the content of the conversation. Id. at 581, 41 P.3d at 582.

Interestingly, the Act contains an exception similar to the business extension exception which allows for the “use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility.” Id. § 632(c). For this exception to apply, the equipment must be furnished by the telephone company, and the monitoring or recording activities must comply with the utility’s tariffs – which often require the use of warning devices in monitoring equipment or recorders. Ribas v. Clark, 212 Cal. Rptr. 143, 147-48, 696 P.2d 637, 641-42 (1985) (analyzing the public utility exception under § 631).

The Ninth Circuit decision addressed whether the provisions of California’s more stringent eavesdropping statute or the federal ECPA would apply when a party sought to introduce a recorded conversation into evidence. Feldman v. Allstate Ins. Co., 322 F.3d 660, 666-67 (9th Cir. 2003). The conversation at issue took place with consent of only one party, and thus the recording itself did not violate federal law but did violate California’s eavesdropping statute. Id. at 666. The Ninth Circuit noted that in most instances, evidence obtained in contravention of state law may be admissible in federal court as long as no federal law was violated. Id. However, the court ultimately excluded the evidence, reasoning that the California eavesdropping statute embodied a substantive state interest in protecting privacy, which interest is guaranteed by the California Constitution, and thus California’s substantive law would apply to this issue and would bar admission of the recording into evidence. Id. at 667.

1. California Supreme Court Holds Employees Have Reasonable Expectation of Privacy Against Workplace Surveillance

The California Supreme Court recently issued a ruling with important implications for privacy issues in the workplace, in this case involving the surveillance of employees using hidden cameras. In Hernandez v. Hillsides, Case No. S147552 (August 3, 2009), the Court analyzed the standards for establishing a privacy violation under both the common law and the California Constitution, focusing on (1) whether the employer intentionally intruded into a matter as to which the employee has a reasonable expectation of privacy, and (2) whether the intrusion was highly offensive to a reasonable person.

In Hillsides, the executive director of a non-profit residential facility for abused children discovered evidence that someone was viewing pornographic web sites from a company computer after hours. Concerned for the safety of the children at the center, the employer installed a video surveillance system in plaintiffs’ shared office in order to try to catch the culprit. Plaintiffs themselves were not suspects and were never recorded or videotaped as the recordings only took place overnight when plaintiffs were away from the office. Nonetheless, plaintiffs sued Hillsides for invasion of privacy after discovering the hidden camera.

The Court held that, notwithstanding the diminished expectation of privacy which generally applies in the workplace setting, the plaintiffs here had a reasonable expectation that their actions would not be subject to video surveillance by their employer without their knowledge or consent. See also, Sanders v. American Broadcasting Companies, 20 Cal. 4th 907, 911 (1999) (holding that employees have a “limited, but legitimate” expectation of privacy in the workplace against covert videotaping by a journalist, even though conversations in the workplace were not completely private). However, the Court ultimately decided that, based on the specific facts of this case, the employer’s intrusion was not “highly offensive and sufficiently serious” to constitute a violation of its employees’ privacy interests. [The Court relied on the fact that Hillsides had an especially compelling reason for the surveillance (protecting the children at the center), and that the surveillance was limited to recording on three occasions with the camera pointed only at plaintiffs’ computers, and only after business hours such that plaintiffs were never actually videotaped. Although the Court decided that the employer was not liable for a privacy violation, this decision was based largely on a unique set of facts. This decision is not a green light to conduct broad surveillance, but rather a warning that employers should provide adequate notice and take steps to limit the scope of intrusion of any such surveillance.

III. Other Types Of Claims To Consider In The Electronic Age

As stated earlier, the electronic age, and the explosion of social networking has brought about its own set of unique problems for employers today. Blurring of lines between “work” and “personal” lives makes managing employees within the bounds of the law increasingly difficult. Natural questions arise. Should employers filter all electronic communications coming in and out of the workplace on company-owned equipment and networks? Answering this question is not an easy task when considering that cyber-communication and social networking can be very beneficial to an employer trying to reach a vast audience. The benefits of immediate public viewing are clear for many employers trying to “brand” their corporate image or

persona. With social networking, access to information is quicker, but also less formal. Users of all types tend to be less guarded and careless with what they say and the messages (intended and unintended) they send.

The very structure of social networking poses risks for employers. Some risks include increased complaints of harassment or discrimination, disclosure of confidential information, loss of trade secret protection and, increased exposure to tort lawsuits. It is only a matter of time before "cybersmearing," "cyberstalking" and "cyberharassment" cases arise in the employment setting. Employers should be aware of the possibility that employees (including managers and supervisors) might post offensive language or pictures on social networking sites that can be viewed by co-workers and clients. Employees often comment upon information or pictures on a co-workers social networking site. Those comments can bleed over into direct communication between co-workers about personal social networking pages and information and pictures presented there. These comments can be most "unwelcome".

The truth is, "textual harassment" is nothing to LOL about. Text messaging in the workplace is rapidly becoming a source of employer liability. More and more employers are finding themselves in court over inappropriate and offensive texts that are popping up on employee cell phones, Blackberries and PDAs. The biggest culprits typically tend to be male supervisors who are sending salacious text messages to female subordinates, asking them out on dates or promising promotions in exchange for sexual favors. These text messages can be explosive evidence in litigation and are often hard to dispute or challenge on grounds of authenticity.

In the past year, texts have been key in several cases. In a pending federal sexual harassment suit in Connecticut against World Wrestling Entertainment Inc., a former licensing coordinator says the married, senior director of the company's consumer products division made sexual advances via late-night texts and phone calls.⁴ In another case, four waitresses at Famous Dave's restaurant in Kanawha County, W. Va., also pointed to text messages in pursuing sexual harassment claims against a supervisor last year, alleging, among other things, that he sent text messages asking for sexual favors.⁵ In January, texts helped two women in Ohio secure a \$495,000 settlement in a sex scandal that led to the resignation of state Attorney General Marc Dann. The women used texts to help show

that they were placed in situations that made the AG's office a hostile work environment. In one case, one of the women produced a text message that said she was "in a weird situation" and needed a ride home from Dann's apartment one night.⁶

The phenomenon of "textual harassment" is, perhaps, more prevalent in the public and private education sector. In April 2009, text messages helped two female soccer players who accused their coach of sexual harassment secure \$450,000 in settlement from Central Michigan University. The players accused their coach of sexual harassment, alleging that he manipulated them into having secret sexual relationships with him and lied to his players and to school officials to avoid getting caught. The coach, Tony DiTucci, maintained he was innocent, claiming the two students had made suggestive romantic advances toward him, and that he reported it to his supervisors. The coach also sent the players inappropriate text messages, which were used to help bolster their claims and settle the claims before filing in federal court.⁷

IV. Practical Considerations And Best Practices

The questions for many employers is to what extent should it regulate use of its information technology software and hardware to protect itself from liability? A few simple measures can include:

- Adopt written policies to address social networking as it pertains to your business activities, employees, and information. Policies should be consistent with organization's policies and procedures on confidentiality and trade secrets; protection of the organization's property; harassment and discrimination; privacy of employee/customer information; computer, internet, e-mail systems; and employee privacy
- Publish and notify employees of policies' existence
- Train employees on these policies consistent with training on other key policies
- Enforce all policies consistent and uniformly
- Maintain "professional" accounts separate from personal accounts
- Prohibit employees from speaking on "behalf" of the organization without express authorization or approval

⁴ *D'Angelo v. World Wrestling Entertainment, Inc.*, Case No. 3:08-CV-01548, U.S.D.C., (D. Conn. 2008).

⁵ *Zeigler, et al. v. Famous Dave's, et al.*, 2008 WLNR 4723590.

⁶ Tresa Baldas, *In the Heat of the Moment*, *National Law Journal*, ALM Media, Inc., July 20, 2009.

⁷ *Id.*

- Consider prohibiting supervisors, managers, administrators and professors from “friending” subordinates or students

Employers who may need to conduct surveillance or otherwise monitor employee activity, such as computer or internet use, should consider the following factors:

Prior Notice. When possible without frustrating the objective of the surveillance, employers should provide prior notice to specific employees who may be subject to monitoring. In addition, employers should include the possibility of any monitoring or surveillance in its employee handbooks and policies.

Reasonable time, place, and scope restrictions. Employers who make an effort to minimize the intrusiveness of surveillance or monitoring are less likely to be liable for a privacy violation. Thus, employers should take care to limit the place, time, and scope of surveillance as much as circumstances permit.

- Employee's expectations. An employee's reasonable expectation of privacy varies depending on the workplace environment. Employers should take extra precaution when conducting surveillance on enclosed or partially-enclosed office spaces, as opposed to more public areas such as hallways or lobby areas.

Employer's business needs. Employers should make sure that there is a legitimate business need for taking action that may be construed as an intrusion into employee privacy, such as loss prevention, ensuring the safety of others, or maintaining productivity.

With respect to harassment and discrimination policies, employers should consider adopting policies that prevent employees from “posting material that is abusive, offensive, insulting, humiliating, obscene, profane, or otherwise inappropriate regarding the organization, its employees, vendors, suppliers, business partners and competitors.” Further, internet usage policies should include language preventing employers from “engaging in any conduct that may be construed as harassment based on race, ethnicity, color, national origin, religion, sex, sexual orientation, age, disability, or any other legally protected characteristic.”

Confidentiality and trade secret policies should prohibit employees from disclosing or discussing in social networking activities customers, partners or suppliers by name; organization's confidential information and trade secrets; and information regarding the organization's clients, affiliates, partnerships. Importantly, employers must train employees on the confidential information policy. Disparagement and defamation policies should clearly state that employees engaging in social networking and blogging for either personal or professional reasons must remain respectful of the organization, its employees, and

vendors, suppliers, business partners and competitors. Further, employees should be prohibited from writing about, posting pictures of, or otherwise referring to any other employee without his or her permission. Employers' cyber-policies should limit employees' authority to speak on behalf of the organization. Unless the employee has explicit authorization to do so, he or she may should not use the organization's name in the online identity (e.g. username, “handle,” or screen name), claim or imply that authorized to speak as a representative of organization, or use the organization's intellectual property, logos, trademarks, and copyrights in any manner.

Finally, employers should make clear that its employees have no reasonable expectation of privacy on the organization's computers, email systems, internet, and organization business (also address telecommuting situations). Employers should make sure its employees know that information exchanged on social networking sites can be accessed by the organization.

About the Authors

Eric L. Barnum is an experienced trial lawyer practicing in all areas of employment law and employment litigation, including wrongful discharge, discrimination and hostile environment harassment litigation, labor arbitration and the analysis of personnel practices and procedures

He also has extensive experience in multi-party, complex civil litigation, including class actions, wage and hour claims, unfair competition, and administrative investigations and hearings.

Nora Kersten Walsh concentrates on all areas of labor and employment law, with an emphasis on employment-related litigation and employee counseling.

She also provides input on labor and employment issues implicated in client mergers and acquisitions, and consults on issues faced by institutions of higher education.

About Schiff Hardin LLP

Schiff Hardin LLP is a general practice law firm representing clients across the United States and around the world. We have nearly 400 attorneys in offices located in Atlanta, Boston, Chicago, Lake Forest, New York, San Francisco and Washington



This publication has been prepared for the general information of clients and friends of the firm. It is not intended to provide legal advice with respect to any specific matter. Under rules applicable to the professional conduct of attorneys in various jurisdictions, it may be considered advertising material.

For more information visit our Web site at www.schiffhardin.com.

© 2009 Schiff Hardin LLP