INVASION OF PRIVACY LIABILITY IN THE ELECTRONIC WORKPLACE: A LAWYER'S PERSPECTIVE

Christine E. Howard[*]

INTRODUCTION

Electronic technology in the workplace is changing rapidly, and those changes are generating new and distinct challenges for employers seeking to increase productivity and minimize disruptions to employees. Some of the issues facing employers are defensive in nature: protecting the company's systems against intruders, preventing excessive use of electronic resources for non-business purposes, and stemming improper communications by company personnel. Other issues involve decision concerning whether to take action against those who are abusing the company's systems or who are engaging in defamation against the company on outside websites or blogs. Many employers closely monitor employee tardiness, while much more time is likely lost due to employees' personal e-mails, cell phones and access to non-business websites. Employers may be equally or even better served by monitoring employees' use of electronic resources than by monitoring their arrival time.

According to one report involving the most recent electronic avenue to express views, blogs, nearly 80,000 new ones are created every day.[1] There are 14.2 million in existence already, fifty-five percent of which remain active.[2] Some 900,000 new blog postings are

∗ Ms. Howard is a partner with the Atlanta, GA office of Fisher & Phillips LLP. Ms. Howard has been selected as a "Georgia Super Lawyer" for "Labor & Employment" since 2004, and for "Employment Litigation: Defense" in 2007. Ms. Howard received her J.D. from Emory University School of Law with Distinction. The observations expressed are that of the presenter/author and not that of Fisher & Phillips or any of the firm's clients.

1. Dave Sifry, *State of the Blogosphere, Aug. 2005, Part 1: Blog Growth*, TECHNORATI, Aug. 2, 2005, http://www.technorati.com/weblog/2005/08/34.html.

2. *Id.*

added each day.[3] Some of those blogs are highly critical of an individual's employer or former employer, while others are merely a diversion from work.[4] A survey recently found that seven percent of U.S. internet users—more than eight million people—write blogs.[5] Another survey found that three percent of respondents had disciplined or fired employees for their blogging activities in the past year.[6] The number and availability of blogs make them a central concern of employers. This article will first explore the limitations on employers in monitoring their employees' use of electronic resources, and then conclude with precautions employers can take to minimize the risks involved with technology used in the workplace.

I. LEGAL LIMITATIONS IN AN ELECTRONIC WORKPLACE

A. Federal Wiretap Act

The Federal Wiretap Act[7] generally prohibits the interception, disclosure or intentional use of wire, oral or electronic communications, including those that occur in the workplace.[8] A "wire communication" is defined as one that carries a person's oral communication over a wire, such as a phone call, and includes the "electronic storage of such communication."[9] An "oral communication" occurs when the individual uttering the communication expected it would be a private conversation.[10] An "electronic communication" is the transfer of information (writing, images, signals, sounds, data, etc.) transmitted by electronic means including radio waves, but is not an oral or wire communication.[11] E-mail, pagers, and cell phone usage are examples of

3. Dave Sifry, *State of the Blogosphere, August 2005, Part 2: Posting Volume*, TECHNORATI, Aug. 2, 2005, http://www.technorati.com/weblog/2005/08/34.html.

4. *See, e.g.*, Wal*Mart Sucks' Journal, http://community.livejournal.com/walmartsucks (last visited Apr. 4, 2006); Wasting Time Blog, http://msquare2.blogspot.com (last visited Apr. 4, 2006); *see also* Sifry, *supra* note 3 (discussing trends in blog activity, with the greatest activity being during the week, especially in the few hours after work begins).

5. LEE RAINIE, PEW RESEARCH CTR., THE STATE OF BLOGGING 1 (2005), http://www.pewinternet.org/pdfs/PIP_blogging_data.pdf.

6. Nancy Flynn, *Blog Rules*, LEADER'S EDGE (Am. Mgmt. Ass'n), May 2006, http://www.amanet.org/LeadersEdge/editorial.cfm?Ed=269.

7.18 U.S.C. §§ 2510-2522 (2000).

8. *See* 18 U.S.C. §§ 2510-12.

9. 18 U.S.C. § 2510(1).

10. 18 U.S.C. § 2510(2).

11. 18 U.S.C. § 2510(12).

"electronic communications."

"Interception" is the aural or other acquisition of the contents of any oral, wire, or electronic communication, through the use of any electronic or mechanical device.[12] For example, intercepting a call with a tape recorder connected to a switchboard without an employee's knowledge is a violation of the Act. However, merely listening to an allegedly illegally-obtained audiotape of private telephone conversations is not a violation of the Act.

The Act provides an exception for employers who act in the "ordinary course of business."[13] This exception allows an employer to electronically monitor, using a telephone extension, any business-related communication without the employee's knowledge or consent.[14] An employer may not, however, monitor communications of a purely personal nature.[15] An employer does not violate the Act if it terminates electronic monitoring immediately upon discovering that the monitored call is purely personal.[16] The Act also does not apply if the employer has the consent of one party to the communication, unless the communication is intercepted for the purpose of committing a criminal or tortuous act.[17] Consent by one of the parties may be either express or implied.[18] Finally, under the "provider" exemption, telephone companies and other employers that provide wire communication services may monitor calls for service checks.[19]

The Act provides a civil cause of action to anyone whose communications are unlawfully intercepted.[20] Successful plaintiffs may recover actual or statutory damages ($10,000 or $100 a day for each day of violation, whichever is greater), punitive damages, and attorney's fees.[21] The Act also makes the unlawful interception, or the attempted interception, of an oral, wire, or electronic communication a felony punishable by fine and/or imprisonment.[22]

12. 18 U.S.C. § 2510(4).
13. 18 U.S.C. § 2510(5)(a).
14. 18 U.S.C. §§ 2510(5)(a), 2511(1)(b).
15. *See* 18 U.S.C. § 2510(5)(a).
16. *See id.*
17. 18 U.S.C. § 2511(2)(d).
18. *Id.*; *see also* United States v. Faulkner, 439 F.3d 1221, 1225 (10th Cir. 2006) (holding warnings by a correctional facility's staff that calls would be monitored, and continued use by inmate, as sufficient implied consent under § 2511(2)(d)).
19. 18 U.S.C. § 2510(5)(a)(ii).
20. 18 U.S.C. § 2520(a).
21. 18 U.S.C. § 2520(b), (c)(2).
22. 18 U.S.C. § 2511(4)(a), (5)(a).

B. State Laws

Many states have counterparts to the Federal Wiretap Act. Some are similar to federal law, and courts are likely to look to federal law for guidance in interpreting the state law.[23] Other states, however, prohibit surreptitious recording of communications even by one of the parties to the conversation, unless all parties consent.[24] Therefore, employers who wish to monitor oral, wire, or electronic communications need to know whether the state or states in which they operate have any specific laws that might affect such monitoring.

II. ISSUES WITH SPECIFIC TYPES OF ELECTRONIC COMMUNICATIONS

A. Voice Mail

A Ninth Circuit Court of Appeals case, *Payne v. Norwest Corp.*,[25] illustrates the general analysis on voice mail recordings. In that case, an employee sued his former employer for wrongful termination.[26] Part of his evidence consisted of tapes of voice mail messages made with a hand-held tape recorder.[27] The employer counterclaimed against the employee alleging that his making of these recordings violated the Federal Wiretap Act.[28] The court concluded there was no violation because no "interception" had occurred.[29] The former employee's "use of a handheld recorder to record voice mail messages did not occur contemporaneously with the leaving of the messages.[30] Moreover, the persons leaving a message consented to the recording of their message by the fact that they left a message."[31] Therefore, the court concluded that an "interception" did not occur within the meaning of the federal wire tapping statute.[32]

23. *E.g.*, Packer v. State, 800 N.E.2d 574, 578-79 (Ind. Ct. App. 2003).
24. *E.g.*, People v. Windham, 51 Cal. Rptr. 3d 884, 886 (Cal. Ct. App. 2006).
25. 911 F. Supp. 1299 (D. Mont. 1995), *rev'd on other grounds*, 113 F.3d 1079 (9th Cir. 1997).
26. *Id.* at 1301.
27. *Id.* at 1302-03.
28. *Id.* at 1302.
29. *Id.* at 1303.
30. *Id.*
31. *Id.*
32. *Id.*

B. Tape Recording

Under federal law, it is permissible to record otherwise protected communications when the recorder is a party to that communication or consent is obtained from one of the parties to the communication, unless the communication is intercepted for the purpose of committing a criminal or tortious act in violation of federal or state law.[33] This is called the "one party consent" exemption. Under state law, however, *all* parties to the communication *may* be required to consent, depending on the law of the particular state.[34]

Some state laws impose other requirements, such as the recording may not be made for a criminal or tortious purpose. In all cases, employers must be sure that employees do not have an expectation of privacy in making these recordings.

C. E-mail

The Electronic Communications Privacy Act of 1986[35] ("ECPA") amended the Federal Wiretap Act to limit the interception and disclosure of e-mail.[36] The ECPA prohibits the intentional interception, use, and disclosure of an "electronic communication."[37] Under the ECPA's narrow definition of "interception," employers rarely violate the statute when reviewing employee e-mails in the workplace.[38] Most courts limit the definition of "interception" to situations where a third party obtains a copy of the e-mail *at the time it is sent.*[39] An "interception" does *not* take place if an individual gets a copy of the e-mail once it is stored in the network computer.[40] This is true even if the person to whom it was addressed has not yet read it.

The ECPA and Federal Wiretap Act are not violated where one of the parties to the communication (e.g., the employer) has given prior

33. 18 U.S.C. § 2511(2)(d) (2000).

34. *E.g.*, CAL. PENAL CODE § 631 (West 2005); People v. Conklin, 522 P.2d 1049, 1056 (Cal. 1974).

35. Pub. L. No. 99-508, 100 Stat. 1848.

36. § 101(a)(3), 100 Stat. at 1848.

37. § 101(a)(5)(C), 100 Stat. at 1848.

38. § 101(a)(3), 100 Stat. at 1848.

39. Payne v. Norwest Corp., 911 F. Supp. 1299, 1303 (D. Mont. 1995), *rev'd on other grounds*, 113 F.3d 1079 (9th Cir. 1997).

40. Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004) (citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)).

consent to the interception by a third party.[41] Therefore, an employer may notify employees that e-mails sent over the company system may be disclosed with the lawful consent of the originator or of any addressee or intended recipient. Consent may be express, as by signed, written acknowledgment, or implied, as by inclusion in a handbook or policy on the use of e-mails. As noted above, however, some more restrictive state laws may require the consent of all parties to a communication.[42]

The ECPA is also not violated where the employer is monitoring communications made through its service "while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or the property of the provider of that service . . . ."[43]

The Federal Stored Communications Act[44] ("SCA"), which applies to stored e-mails, contains an even broader exception.[45] The SCA does not apply to the monitoring of e-mails where such monitoring is authorized by the person or entity providing the e-mail service, as long as the service is not provided to the general public.[46]

D. Blogs

Blogs are "web logs" that may be established by a company for its employees' use, by individual employees, or by other outside organizations or individuals. Blogs have gained attention among human resources professionals recently because of several high-profile cases in which employees were fired because of their journal entries about the workplace.[47]

Some high tech companies, however, have helped their employees gain access to software to create blogs. The companies believe that grass-roots communication with their prospective clients makes the company appear more accessible and responsive. A software company reportedly has more than 1200 bloggers who write such topics as product development and programming strategies, and company

41. 18 U.S.C. § 2511(2)(d) (2000).

42. See *supra* text accompanying footnotes 24, 34.

43. 18 U.S.C. § 2511(2)(a)(i).

44. 18 U.S.C. §§ 2701-2711.

45. 18 U.S.C. § 2701(c).

46. 18 U.S.C. § 2701(c)(1); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1226 (2004).

47. Stephanie Armour, *Warning: Your Clever Little Blog Could Get You Fired*, USA TODAY, June 15, 2005, at B1; Tom Zeller, Jr., *When the Blogger Blogs, Can the Employer Intervene?*, N.Y. TIMES, Apr. 18, 2005, at C1.

executives say they appreciate the "real-time feedback" from customers who respond to the bloggers.[48]

If the employee can show that the online journal was used to promote common goals of a group of employees relating to wages, hours, or working conditions, the blogging might constitute protected concerted activity under the National Labor Relations Act.[49] In addition, several states have enacted laws which limit an employer's ability to discipline employees for lawful conduct outside the workplace.[50] A prudent blogging policy should be reviewed for compliance with state law and compatibility with company goals and objectives.

Thus, the increasing use of blogs, sometimes used to vent about company policies and workplace issues, means that more employers will need policies governing what is essentially away-from-work conduct.

III. INTERNET AND E-MAIL HARASSMENT/DISCRIMINATION ISSUES

As case law has made clear, an employer can be held responsible for the content of electronic communications under both the National Labor Relations Act ("NLRA") and Title VII of the Civil Rights Act ("Title VII").[51] Further, both the NLRA and Title VII require employers to protect employees against illegal harassment. Under Title VII, an employer can be held liable for the harassing actions of its employees if it knew or should have known of the offensive behavior but failed to act to remedy the situation.[52] The EEOC and the courts have made it clear that employers are expected to stop harassment *before* it rises to the level of a violation of federal law.[53] An employer who learns of, but fails to take effective measures to stop retaliation against employees who have made concerted complaints about harassment would also be liable for violating the NLRA.[54] Therefore, some form of monitoring is essential

48. John Gapper, *A Blog Reveals the Mind of Sun*, FIN. TIMES, Apr. 22, 2005, at 13; *see* Sun Microsystems Communities, Sun Guidelines on Pubic Discourse, http://www.sun.com/communities/guidelines.jsp (last visited Sept. 12, 2008).

49. *See* 29 U.S.C. § 157 (2000).

50. *E.g.*, MINN. STAT. § 181.938 (2005); MONT. CODE ANN. § 39-2-313 (2005); NEV. REV. STAT. § 613.333 (2005); N.C. GEN. STAT. § 95-28.2(b) (2005); TENN. CODE ANN. § 50-1-304(e) (2005).

51. *See, e.g.*, Duane Reade, Inc. v. Local 338 Retail Union, UFCW, AFL-CIO, 777 N.Y.S.2d 231, 235 (N.Y. Sup. Ct. 2003); Davis v. Globalphone Corp., No. 1:05CV187(JCC), 2005 WL 2708921, at *4 (E.D. Va. Oct. 19, 2005).

52. *See, e.g.*, *Duane Reade*, 777 N.Y.S.2d at 235; *Davis*, 2005 WL 2708921 at *4.

53. *See* Minnich v. Cooper Farms, Inc., 29 F. App'x 289, 290-91, 295 (6th Cir. 2002); Debbie Schiltz Jones, E.E.O.C. Dec. 01894050, at *7 (1990), 1990 WL 711422, at *7 (Mar. 8, 1990).

54. *See* U.S. Auto. Ass'n v. NLRB, 387 F.3d 908, 917 (D.C. Cir. 2004).

for legal reasons.

These types of claims have taken many forms. In a recent New York case, the plaintiff brought a claim of age-based harassment relying on the contents of four e-mails.[55] The e-mails referred to the plaintiff as a "wrinkled-up, hairy upper-lipped neighbor and co-worker," a "grave-lady," "the wrinkled but aged babe," and stated that she "look[ed] like Mickey Mantle just before the time he received his liver transplant."[56] The plaintiff reported these e-mails and the company disciplined the offenders.[57] Nevertheless, plaintiff brought suit against the company. The suit was ultimately dismissed on the grounds that the few e-mails, while inappropriate, did not rise to the level of a hostile environment.[58]

A lawsuit was filed in Maryland by an individual who worked as a personal assistant for an executive.[59] The executive had occasionally received e-mails containing jokes with sexual content, and the assistant claimed these e-mails were offensive.[60] Other employees have supported their harassment claims on the basis of offensive screen savers or other images on computer screens at work.[61]

Because e-mails do not "disappear" and provide solid evidence of harassing or discriminatory behavior, employers have more trouble defending these than in past "he said, she said" cases. Conversely, courts routinely have dismissed suits against employers when an employee's harassing or discriminatory e-mails violated the company's electronic communications policy.[62] Courts hold that a violation of an employer's policy is a legitimate non-discriminatory reason for termination.[63]

IV. INTERNET AND E-MAIL CONCERTED PROTECTED ACTIVITY ISSUES

Generally, employees may engage in oral union solicitation during non-working time even in work areas; but, employees may not distribute

55. Irvine v. Video Monitoring Servs. Am., L.P., No. 98 Civ. 8725(NRB), 2000 WL 502863, at *1 (S.D.N.Y. Apr. 27, 2000).

56. *Id.*

57. *Id.*

58. *Id.* at *4.

59. Hoffman v. Lincoln Life Annuity & Distrib., Inc., 174 F. Supp. 2d 367, 371 (D. Md. 2001).

60. *Id.*

61. *See, e.g.*, Steck v. Francis, 265 F. Supp. 2d 951, 966 (N.D. Iowa 2005).

62. *See, e.g.*, Goldstein v. PFPC, Inc., 17 Mass. L. Rptr. 333, 2004 WL 389107, at *2, *4 (Mass. Super. Ct. Feb. 19, 2004).

63. Rizzo v. PPL Serv. Corp., No. Civ. 03-5779, 2005 WL 913091, at *10-11 (E.D. Pa. Apr. 19, 2005).

written materials in work areas at any time.[64] Unions argue that workers physically separated from each other may have no other effective means of communication than with employer-owned computers and e-mail systems. Employers disagree, noting that there have been dramatic increases in new forms of private communications among employees and between them and labor unions, such as personal cell phones, pagers, PDAs, home and personal laptops, not to mention sophisticated union websites.

Since, as a practical matter, it is difficult to completely prohibit employees' personal use of e-mails during work time, a more realistic approach may be to attempt to manage and limit such uses. In a recent change in NLRB precedent relating to solicitation and distribution, it also appears e-mail usage by employees will only narrowly be protected under the NLRA.[65] An employer may now simply provide a legitimate reason for its actions and show that it was not singling out union activity specifically.[66] Merely excluding a class of activity, such as prohibiting group e-mails to solicit on behalf of entities that aren't charities, the NLRB now says, doesn't single out union activity.[67] Also, some legitimate justifications for placing limits on personal e-mails are: the size of the employer's server cannot sustain an unlimited number of e-mails; there have been past system problems based on the volume of traffic, such as slow time or down time; there have been problems with distractions during work time (e.g., pictures of current news events); employees have been disciplined in the past for inappropriate or excessive use of e-mails or the internet, unrelated to union activity; and employees' personal use has increased risks of exposure to damaging computer viruses or to system "crashes."

V. SECURING EMPLOYEE INFORMATION STORED ELECTRONICALLY

Another issue receiving media scrutiny in the past year is the compromise of personal data via the internet, internal servers, and other computer systems.[68] Consumers and employees have been disturbed to

64. 29 U.S.C. §§ 157, 158(a)(1) (2000); Nancy J. King, *Labor Law for Managers of Non-Union Employees in Traditional and Cyber Workplaces*, 40 AM. BUS. L.J. 827, 859-60 (2003).

65. Guard Publ'g Co. *(Register Guard*), 351 N.L.R.B. No. 70, 183 L.R.R.M. (BNA) 113 (Dec. 16, 2007) (overruling past NLRB precedent to now only protect against employer e-mail policies that strictly discriminate on a union versus non-union subject matter basis).

66. *Id.*

67. *Id.*

68. M. Daniel Gibbard, *ID Theft Toll is Growing in U.S.*, CHI. TRIB., March 11, 2005, at 1;

find that their personal information was stolen and, in many cases, used to open credit cards, rent apartments, buy vehicles, or establish cell phone accounts. The Federal Trade Commission has estimated that more than half of all identity theft results from compromised business records.[69] A study by a credit reporting agency found that the top cause of identity fraud is the theft of information by employees.[70]

The Fair and Accurate Credit Transactions Act of 2003[71] ("FACTA"), has a new records disposal rule aimed at reducing the possibilities for identity theft.[72] The Rule, which went into effect in June of 2005, requires employers to "properly dispose of" consumer reports.[73]

Not all employment records are covered by the Rule. A "consumer report," as defined in the Fair Credit Reporting Act, consists of information provided by a "consumer reporting agency."[74] The information involves an individual's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.[75]

Employers must take reasonable steps to secure this information. Many employers engage third parties to collect this kind of information, particularly for employees whose jobs involve financial transactions, responsibility for children, or work of a similarly sensitive nature. The Rule does not require employers to dispose of this information.[76] But if they do, they must "take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[77] Some states likewise have statutes that govern the destruction of personal information.[78]

Additionally, possible common law actions for negligence arise in these situations. Even in the absence of a specific statute, employees can sue under a common law theory of negligence if the employer has been

Tom Zeller Jr., *Some Colleges Falling Short in Data Security*, N.Y. TIMES, Apr. 4, 2005, at C1.

69. Eric Gillin, *Protecting Yourself Against Identity Theft*, THE STREET, Feb. 27, 2002, http://www.thestreet.com/markets/ericgillin/10010609.html.

70. Stephanie Armour, *Employment Records Prove Ripe Source for Identity Theft*, USA TODAY, Jan. 23, 2003, http://www.usatoday.com/money/workplace/2003-01-23-idtheft-cover_x.htm.

71. 15 U.S.C. § 1681 (Supp. III 2004).

72. 15 U.S.C. § 1681w.

73. 15 U.S.C. § 1681w(a)(1).

74. 15 U.S.C. § 1681a(d)(1).

75. 15 U.S.C. § 1681a(d)(1).

76. 15 U.S.C. § 1681w.

77. 16 C.F.R. § 682.3(a) (2005).

78. *E.g.*, HAW. REV. STAT. § 487R-2 (2005); KY. REV. STAT. ANN. § 365.725 (2005); MONT. CODE ANN. § 30-14-1703 (2005).

careless when storing or disposing of sensitive data.[79] While the FACTA disposal rule covers only "consumer reports," the prudent employer will want to do more to safeguard employee data.

VI. MINIMIZING RISKS OF PRIVACY SUITS

A. Limits On What Employees May Do

It is important to emphasize the implementation of policies before, not after, there is a problem such as union activity or a complaint of harassment. Implementation after a problem arises may lead to charges of disparate treatment or retaliation. Such policies will include search policies, internet and e-mail policies, cell phone usage policies, and blogging policies, among others. Policies and questions to consider might include the following:

1. Reduce or eliminate any expectation of privacy by the employees and explain what employees should and should not do. This applies not only to computers and e-mails but also to searches.

2. Publish policies that reserve the employer's right to monitor, gain access to, or disclose all e-mails on the employer's system. In those policies, state that any messages sent on the system are the sole property of the employer. Among other things, state that security functions such as passwords and message-delete functions do not prevent the employer from retrieving e-mails and that the employer may override any individual passwords or codes.

3. Prohibit the use of cameras, cell phones, recorders, or other devices for taking photographs or making recordings on the premises.

4. Prohibit the use of e-mails for distributing crude, obscene, or offensive material or for other illegal or improper reasons.

5. Prohibit use of company trademarks, logos, and copyrighted materials, without specific authorization.

6. Prohibit disclosure of company materials to competitors or others outside your company.

7. Decide whether there will be a ban on personal use of computers and e-mails or a limitation on such uses. Be realistic. Do not recommend banning personal use unless an employer is prepared to be consistent in applying the ban.

8. Make clear that violations of rules will be punished with

79. *See, e.g.*, Reyes v. Storage & Processors, Inc., 86 S.W.3d 344, 346 (Tex. App. 2001).

discipline up to and including discharge.

9. Train employees in the content and applications of your rules.

10. Monitor compliance with the rules and be consistent in enforcing them.

B. Limits On Employer Representatives

Employers and their officers and managers must also be versed in these topics so as not to overstep their bounds. A few suggestions follow:

1. Limit disclosure of private information about employees to those having a clear need to know.

2. Let managers and supervisors know that improper disclosure of such information can subject both them and the company to liability for invasion of privacy.

3. Ensure that all confidential or private information is stored securely, whether in your computer system or in hard copy.

4. When materials are no longer needed or required to be maintained, ensure that they are destroyed.

5. Restrict access to stored electronic mail transmissions to the systems administrator and management personnel who may have a need for such access. Employers should limit those able to monitor or to review an employee's e-mail or voicemail to reduce the potential for invasion of privacy and other claims. Those able to access the electronic media should be restricted to only those management employees necessary to effectively administer the employer policies and to manage the employee at issue; usually, this will be only the systems administrator and management personnel who may have a need for such access.

6. Because this area of the law is rapidly expanding and new developments, such as statutes and new court decisions, are routine, it is advisable to seek legal counsel before conducting any investigation that may involve access to an employee's e-mail, computer files, or voicemail.

7. Employers will want to adequately train supervisors and other management personnel regarding the policies and their enforcement to ensure consistency.

CONCLUSION

Whether one is advising clients as outside or internal counsel, it is

incumbent to plan in advance of these now common problems associated with technology in the workplace. While an employer might feel comfort in having an isolated policy that may cover some of these issues, that single policy may not save the day if the employer has not carefully considered and periodically revisited these existing policies to ensure they address the myriad of issues that arise not only from traditional forms of communication, but now from electronic mail, cell phone usage, blogging, hackers, and new forms of electronic media to come.