William Mitchell Law Review

Volume 29 | Issue 3 Article 1

2003

Competing Interests in the Post 9-11 Workplace: The New Line between Privacy and Safety

Elise M. Bloom

Madeleine Schachter

Elliot H. Steelman

COMPETING INTERESTS IN THE POST 9-11 WORKPLACE: THE NEW LINE BETWEEN PRIVACY AND SAFETY

Elise M. Bloom[†]

Madeleine Schachter[††]

Elliot H. Steelman[†††]

I. INTRODUCTION

An increasing number of employers are focusing their primary

† Elise M. Bloom is a senior partner in the New York City office of Jackson Lewis LLP. The views expressed here do not constitute legal advice.

†† Madeleine Schachter is Associate General Counsel at AOL Time Warner Book Group Inc., which is part of AOL Time Warner Inc. The views expressed here do not necessarily express the views of AOL Time Warner.

††† Elliot H. Steelman is a law clerk in the New York City office of Jackson Lewis LLP.

concerns on security and safety in the workplace due to the events of September 11, 2001. Both employees and managers are increasingly willing to sacrifice accustomed niceties for this enhanced protection.[1] Since September 11, sales of Internet and e-mail monitoring software have risen dramatically. Many employers, who did not do so in the past, now require employees to carry identification badges. Fire and evacuation drills are conducted more frequently. Employers are focusing on learning as much information about employees as possible in the name of safety. These new concerns, while warranted by the events of September 11, raise many issues under applicable employment laws.

The influx in the need for information begs the question: how much is too much before the employer's need for security infringes on the employee's privacy? Employee monitoring has positive and negative consequences. Although monitoring can lead to greater efficiency and better quality control, and possibly decrease the employer's liability for employee misconduct, it can trigger employee backlash and decrease morale. Further, it may lead to union organizing.[2] This article explores emerging questions relating to the needs of employers and employees by examining the current and future state of privacy in the private workplace.

II. HOW FAR CAN AN EMPLOYER GO TO VERIFY CONDUCT AT WORK?

Employee monitoring is not a new concept. Employers have always monitored their employees for reasons of efficiency, security, or legal obligation.[3] Title VII of the Civil Rights Act of 1964,[4] as amended, as well as a myriad of other state and federal laws, impose an obligation on employers to monitor the workplace to ensure the workplace is harassment-free. An employer's communication systems are generally considered part of the workplace since employees use them during working time on working premises.

Improved technology enables employers to dramatically increase the extent and ability to monitor employee activities. As

1. Security is not solely limited to physical safety but also includes safeguarding employees' private information. An employer's security interest is in the protection of its proprietary information as well as the privacy of its employees.

2. John B. Lewis, *I Know What You E-Mailed Last Summer*, SECURITY MGMT, Jan. 2002, at 93.

3. 42 U.S.C. § 2000e-2 to -3 (2002).

4. *Id.* § 2000e.

businesses rely more and more on electronic mail ("e-mail") and other electronic communications, such as voicemail and mobile phones, employers have many new outlets to monitor employees.[5] A 2001 report by the Privacy Foundation[6] stated that fourteen million employees, just over one-third of the online workforce in this country, had their e-mail or Internet usage continuously monitored at work.[7] This increase has raised questions as to how far employers can go to check employee communications.

A. What are the Privacy Rights of the Private Employee? Employer?

The United States Constitution has been interpreted to protect privacy rights, but has not been applied to the private workplace. A right to privacy, although not provided for in the explicit language of the Constitution, has been interpreted by the Supreme Court to fall under the Fourth Amendment. The Fourth Amendment protects against unlawful searches and seizures and applies to federal, state and local government employees, where employers conducted the searches.[8] The Supreme Court, in *O'Connor v. Ortega*, held that in an invasion of privacy suit, the public sector employee's privacy interest must be balanced against the "realities of the workplace."[9] However, absent state action, employees of private companies do not receive the Fourth

5. Businesses are not alone in their use and reliance on e-mail. E-mail and its facility to communicate have penetrated the judicial system. The Ninth Circuit recently held that a lawsuit was properly served when it was sent via e-mail. *See* Rio Prop. Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1016 (9th Cir. 2002).

6. The Privacy Foundation is a privacy interest group. For more information on the foundation see its website at http://www.privacyfoundation.org.

7. ARTHUR SCHULMAN, THE EXTENT OF SYSTEMATIC MONITORING OF EMPLOYEE E-MAIL AND INTERNET USE, PRIVACY FOUNDATION REPORT, *at* http://www.privacyfoundation.org/privacywatch/report.asp?id=72&action=0 (July 9, 2001).

8. Not all agree that the extent of coverage of the Fourth Amendment stops at the public sphere. Judge James M. Rosenbaum, the Chief Judge of the U.S. District Court for the District of Minnesota has expressed that the Fourth Amendment "embodies a higher principle," that "an individual retains a certain sphere of privacy that is inviolate." Megan Santosus, *Hard Drives Raise Hard Issues,* DARWIN, Jan. 2002, at 18, *at* http://www.darwinmag.com/read/010102/buzz_privacy.html (quoting James M. Rosenbaum, *In Defense of the Hard Drive,* 4 GREENBAG 169, 170 (2001), *available at* http://www.greenbag.org/rosenbaum_harddrive.pdf). Judge Rosenbaum opined that the private sector should also be covered by the Fourth Amendment's "higher principle." *Id.*

9. 480 U.S. 709, 721 (1987).

Amendment protection granted to their public counterparts.[10]

In the private realm, the employer's interests in, for example, safety, liability for employees' actions, and prevention of theft and intellectual property are weighed against the individual's right to privacy. The lower an employee's expectation of privacy, the greater the likelihood that the employer does not invade the privacy of the employee when conducting searches or monitoring. The trend in workplace privacy before September 11 was shifting toward employees' interests; however, employees have become less resistant to monitoring since September 11. It now seems that an employer is best protected if it announces its policies regarding employee monitoring and workplace privacy. If an employer does not have a policy in place, the employee may still derive protection under common law and federal and state statutes.

B. Common Law Tort Actions

Employers who access their employee's workplace e-mail without a clear electronic communication policy may be inviting claims under state common law for invasion of privacy. Most states have a common law tort claim for privacy, but not all states recognize all types of claims. There are four common law theories to bring a claim for invasion of privacy: (1) "intrusion upon the seclusion of another," (2) "appropriation of the other's name or likeness," (3) public disclosure of "private life" facts, and (4) "publicity that unreasonably places the other in a false light."[11] As a general matter, an employer can avoid liability under the first three theories if it does not disclose the information reaped from the monitoring of its employees, and does not continue listening in when the conversation turns personal.

In New York, for example, courts have declined to recognize a common law right of privacy.[12] The New York Court of Appeals stated, "[w]e have in the past recognized that, in this State, there is no common law right of privacy and the only available remedy is that created by Civil Rights Law §§ 50 and 51."[13] In its place, some

10. *See* Katz v. United States, 389 U.S. 347, 352 (1967) (holding that individuals are protected against unauthorized interception of their telephone communications by the government).

11. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

12. Hurwitz v. United States, 884 F.2d 684, 685 (2d Cir. 1989) (stating "[n]o so-called common law right of privacy exists in New York").

13. Freihofer v. Hearst Corp., 480 N.E.2d 349, 353 (N.Y. 1985). Civil Rights

employees turn to the tort theory of defamation to bring claims against employers.[14] However, this theory is concerned with publication rather than with the monitoring or recording of telephone or electronic communication.

With the exception of New York, the most prevalent privacy theory an employee invokes when their e-mail or voicemail was monitored is intrusion upon seclusion.[15] When deciding an intrusion upon seclusion claim, courts will consider: (1) whether the intrusion was intentional, (2) whether the act in question would have been highly offensive to the average reasonable person, (3) whether the plaintiff's activity was subjectively and objectively private, and (4) whether the intruder had a legitimate purpose justifying the invasion.[16] The courts, interested in protecting employers' ability to conduct their business, have set a "highly offensive standard," a high bar for employees to meet.

In *McLaren v. Microsoft*, the Texas Court of Appeals held that the employer's "breaking into" personal folders maintained on the employee's office computer which were protected by a password, did not amount to a "highly offensive" invasion of privacy.[17] The court further held that the employee's use of a personal password did not create a reasonable expectation of privacy, which would prohibit the employer from reviewing the message as part of an investigation into workplace harassment.[18]

Employees may also seek redress under a claim for wrongful

Law § 50 protects an employee's right to privacy if the employer uses for advertising purposes or for trade, the "name, portrait, or picture of any living person without having first obtained written consent of such person." N.Y. CIV. RIGHTS L. § 50 (2002). Civil Rights Law § 51 states that the violation of § 50 is a misdemeanor and further grants the employee a cause of action for injunction and damages. N.Y. CIV. RIGHTS L. § 51 (2002).

14. An employee may bring a claim of defamation if the employer has, without an applicable privilege, communicated something false and defamatory about the employee. If the statement communicated is true, the employer has an absolute defense to defamation claims, but may be held accountable on other invasion of privacy based claims. *See* Lewis, *supra* note 2 (citing Lian v. Sedgwick James, 992 F. Supp. 644 (S.D.N.Y. 1998) (providing more information on claims of defamation, emotional distress, and intentional infliction of emotional distress)); *see also* Sarah DiLuzio, *Workplace E-Mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741, 750 (2000).

15. *See* Amanda Richman, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337, 1352 (2001); *see also* Lewis, *supra* note 2, at 93.

16. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

17. No. 05-97-00824-CV, 1999 WL 339015, at *5 (Tex. App. May 28, 1999).

18. *Id.* at *12-*13.

termination under tort law. In *Smyth v. Pillsbury Co.*,[19] an at-will employee claimed he was wrongfully discharged. The employee allegedly sent inappropriate e-mails to his supervisors over the company's e-mail system.[20] The employee argued that the employer's interception of these e-mails was an invasion of his privacy since the employer repeatedly told its employees that the communications over the e-mail system would be confidential.[21] The court concluded that there was no privacy interest implicated in the employee's message to his supervisor and that the employer's interest in maintaining professional and appropriate e-mail protocols outweighed the employee's privacy interest.[22] The court also noted that to establish a violation of public policy, the employee must show that the employer's actions were a "substantial and highly offensive invasion of" the employee's privacy.[23]

However, in *Restuccia v. Burk Technology, Inc.*,[24] the court, in partially denying the employer's motion for summary judgment, reached a different conclusion. In that case, the employer did *not* have in place a policy regarding use of its e-mail system for personal use, but did prohibit "excessive chatting."[25] Moreover, the plaintiffs, as employees, were not specifically informed that their supervisors had access to computer files and e-mail messages, and that this information was automatically saved on backup files which the supervisors could access. The plaintiffs' supervisor read their e-mail files after hearing that the employees were spending a large amount of time on the e-mail. Among these e-mails were personal correspondence and messages sent back and forth between the two employees regarding one of the plaintiffs' extra-marital affairs with another employee.[26] The employees were discharged. The employer claimed that they were dismissed for excessive use of e-mail and not for its content. The employees brought claims for wrongful termination, invasion of privacy, unlawful interception of wire communications, intentional and negligent infliction of emotional distress, loss of consortium and interference with

19. 914 F. Supp. 97, 98 (E.D. Pa. 1996).
20. *Id.* at 98-99.
21. *Id.*
22. *Id.* at 101.
23. *Id.* In *Smyth*, the court held that a reasonable person would not find that the employer's actions met this standard. *Id.* at 101.
24. No. CA 95-2125, 1996 WL 1329386, at *1 (Mass. Supp. Aug. 13, 1996).
25. *Id.*
26. *Id.* at *3.

contractual relations.[27] The court granted summary judgment for the employer on the intentional infliction of emotional distress and tortious interference with contract claims, but denied summary judgment on the employees' wrongful termination claim. The court held that there was still a genuine issue of material fact on the issue of "whether [the employees] had a reasonable expectation of privacy in their e-mail messages and whether [the employer's] reading of the e-mail messages constituted an unreasonable, substantial or serious interference with plaintiff's privacy."[28]

C. Federal Statutes and Judicial Interpretation

Common law tort actions only grant private sector employees and employers one mode of protection. The groundwork for electronic privacy law comes from federal statutes. There are a variety of federal statutes that apply to workplace monitoring and protection of privacy in the private sector with the purpose of curbing employers' powers to delve into employee communications. Nevertheless, most courts are sensitive to employers when interpreting the statutes and find that there is not enough of an employee privacy interest to warrant protection when balanced against the employer's business interests. Relevant statutes include the Federal Omnibus Crime Control and Safe Streets Act of 1968,[29] the Electronic Communication Privacy Act of 1986 ("ECPA")[30] and the Stored Wire and Electronic Communications and Transactional Records Access.[31] Although not specifically targeting workplace monitoring, these Acts have been applied to this area.[32] The Uniting and Strengthening

27. *Id.*

28. *Id.*

29. 18 U.S.C. §§ 2510-2520 (2000) (*amended by* Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135).

30. 18 U.S.C. §§ 2510-2522 (2000) (*amended by* Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135).

31. 18 U.S.C. §§ 2701-2711 (2000) (*amended by* Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135).

32. Besides these existing Acts, legislation has been proposed to focus more narrowly on the issue of workplace monitoring. In July of 2000, the Notice of Electronic Monitoring Act ("NEMA") was introduced in the House and the Senate. Nathan Watson, *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?*, 54 IND. FED. COMM. L. J. 79, 80 (2001). The Act mandated employers to notify their employees before conducting surveillance of their employees' communications. *Id.* This notification was to include the type

America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, commonly known by its acronym the "USA PATRIOT Act,"[33] may also have an effect on the private sector workplace.

The Federal Omnibus Crime Control and Safe Streets Act of 1968,[34] known as the "Federal Wiretapping Act," provides for a civil cause of action against those who intercept wire, oral or electronic communication without the consent of a party.[35] A party's consent can be expressed or implied,[36] however, and the statute excludes interceptions by employers in the ordinary course of business.[37] The Act also provides for the recovery of compensatory and punitive damages as well as attorneys' fees.[38]

The Electronic Communication Privacy Act of 1986 ("ECPA")[39] amended the Omnibus Crime Control Act.[40] Although noted for its lack of clarity,[41] the Act lays out certain prohibitions and guidelines. Title I of the ECPA, like its predecessor, prohibits an employer from intentionally intercepting its employees' wire, oral or electronic communications.[42] Title II of the ECPA prohibits unauthorized "access" to stored communications.[43] The Acts provide an additional exception for the use of "telephone extensions or monitoring equipment, supplied as part of the

of monitoring to take place, the kind of communication to be monitored, the type of information sought and obtained, the intended use of the information gathered, and the frequency that monitoring would be conducted. *Id.* However, NEMA was not passed and it seems that with the current state of affairs and attitudes, a similar bill will not be proposed for some time. For more information on NEMA, *see id.* at 79 (discussing NEMA and arguing why the proposed legislation should be reintroduced).

33. Pub. L. No. 107-56, 115 Stat. 272 (2001).

34. 18 U.S.C. §§ 2510-2520 (2000).

35. *Id.* § 2520(a).

36. For example, consent may be implied where a party knows that telephone calls will be intercepted. Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990).

37. 18 U.S.C. §§ 2510-20 (2000).

38. *Id.* §§ 2520(b)(1), (2) (2000).

39. *Id.* § 2510 (2000).

40. *Id.*; *see also* S. REP. NO. 99-541, at 1 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

41. *See* United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (citing Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (stating that the Wiretap Act "is famous (if not infamous) for its lack of clarity")).

42. *See* 18 U.S.C. § 2511(1)(a) (2000). The ECPA amended the Omnibus Crime Control and Safe Streets Act of 1968 to prevent against unlawful interception of electronic communications. *See* S. REP. NO. 99-541, at 1.

43. 18 U.S.C. § 2701 (2000).

original communications system that are used in the ordinary course of business."[44]

In sum, there are three pertinent exceptions under the "Federal Wiretapping Acts."[45] The first exception is for e-mail service providers, the "provider exception." The provider exception authorizes access to those providing wire or electronic communications services.[46] Hence, if a company provides employees with e-mail use from a company-owned system it should be covered by this exception. The second exception is for access accomplished in the "ordinary course of business."[47] Under this exception, if an employer can justify the monitoring of its employees' communications with a business purpose, it should not be liable under the Act. The last exception is the consent exception.[48] Consent from one party is all that is needed, but it must be explicit. Some courts choose not to infer consent, but will find consent when it is apparent.[49] Thus, under this third exception, employers may escape liability under the Act by giving clear *notice* to employees of an employee monitoring policy.

44. *Id.* § 2510(5)(a) (2000).

45. For more analysis, *see* DiLuzio, *supra* note 14.

46. 18 U.S.C. § 2511(2)(a)(i) (2000).

47. The ordinary course of business exception for telephones is set forth in § 2510(5)(a) of the ECPA:

> (5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral or electronic communication other than –
>
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof,
>
> (i) furnished 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; . . . .

Id. § 2510(5)(a).

48. *Id.* § 2511(2)(d).

49. *See* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (holding that implied consent could not be found since the employer did not inform the employee that it was definitely monitoring the phone but only said that it might monitor in an effort to "cut down on personal calls").

1. *Application of Federal Statutes to Reviewing E-mail, Voicemail and the Internet*

As noted above, the ECPA regulates the monitoring of electronic communications, including e-mail and voicemail. The statute includes several exceptions (as noted above). Court decisions involving monitoring employee e-mail have balanced the employer's legitimate business needs against the employee's privacy expectation.[50] Under the exception to the ECPA, it appears that the employer can escape liability under the Act if the employee continues to use the e-mail system after being given adequate notice of an employee monitoring policy.

Courts, including New York state courts,[51] have held that the ECPA applies when the e-mail is intercepted at the point of transmission.[52] The Wiretap Acts thus "provide protection for communication only while it is in the course of transmission. The strong expectation of privacy with respect to communication in the

50. *See* Smith v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding that "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments").

51. *See, e.g.,* Hudson v. Goldman Sachs & Co., 283 A.D.2d 246, 247 (N.Y. App. Div. 2001) (reinstating the plaintiff's cause of action alleging that his employer learned about his affair by intercepting his e-mail, because "although the statute prohibits only intercepts that are contemporaneous with transmission, i.e., the intercepted communication must be in transit, not in storage, an allegation that there was an intercept is sufficient for pleading purposes") (citation omitted).

52. *See* Eagle Inv. Sys. Corp. v. Einar Tamm, 146 F. Supp. 2d 105, 112 (D. Mass. 2001) (holding that the ECPA did not eliminate the "during-transmission requirement" from the Wiretap Act and noting that if Congress had intended the definition of "electronic communication" to include both transfer and storage, it easily could have included the word "storage" in the definition); Steve Jackson Games Inc. v. United States Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994) (stating that "Congress' use of the word 'transfer' in the definition of 'electronic communication' and its omission in that definition of the phrase 'any electronic storage of such communication' (part of the definition of 'wire communication')" reflects that Congress did not intend for "intercept" to apply to communications in "electronic storage"). However, in *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035, 1044 (9th Cir. 2001), *opinion withdrawn*, 262 F.3d 972 (9th Cir. 2001), the Ninth Circuit rejected the Fifth Circuit's limitation to in "transit" e-mails. The court stated, "[a]n electronic communication in storage is no more or less private than an electronic communication in transmission. Distinguishing between the two for purposes of protection from interception is 'irrational' and 'an insupportable result given Congress' emphasis of individual privacy rights during passage of the ECPA.'" *Id.* at 1045 (citations omitted). Nevertheless, the court withdrew its opinion and changed its mind in holding that interception must be done during "transmissions," and "not while it is in electronic storage." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002).

course of transmission significantly diminishes once transmission is complete."[53] Thus, these Acts do not expressly prohibit employers from retrieving stored e-mail and recording video without audio.[54] In *Fraser v. Nationwide Mutual Insurance Co.*,[55] the court analyzed the workings of e-mail and held that review of an employee's e-mail from a file server may be "ethically 'questionable'" but "not legally actionable under" federal statutes.[56]

However, federal protection still exists for employees regarding the distribution of information gathered from storage and file servers. Once the employer has accessed recorded messages, the law limits their disclosure and prohibits certain unauthorized disclosures. However, the employer may disclose a message to an addressee, an intended recipient, or to an agent of that person. The employer may also disclose the contents of stored messages with the lawful consent of the originator, addressee, or intended recipient.

The USA PATRIOT Act[57] gives law enforcement more power to facilitate the investigation of suspected terrorists. It is unclear how this will affect private sector employment. It is expected that the Act will further curtail the private rights of private sector employees because it gives the government increased power to surreptitiously obtain information. The Act makes it easier for the government to check individual's voicemail and e-mail. Whereas before the USA PATRIOT Act the government needed a wiretap warrant that was often difficult to obtain, now a simple search warrant may do.[58]

53. Fraser v. Nationwide Mutual Ins., 135 F. Supp. 2d 623, 637-38 (E.D. Pa. 2001) (holding that the employer did not violate the ECPA by accessing stored e-mail on its system after the e-mail was received by the named recipients). Moreover, the Ninth Circuit in Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (2002), stated in dicta that since Congress amended the Wiretap Act, see USA PATRIOT Act §209, 115 Stat. at 283, "to eliminate storage from the definition of wire communication," that once transmission is complete there is no longer an issue for protection. *Id.* at 879.

54. In an analogous criminal case, United States v. Simons, 29 F. Supp. 2d 324, 329 (E.D. Va. 1998), the court found that there was no violation of the ECPA since the e-mail in question was copied from storage and not while it was being transferred. In Thompson v. Johnson County Cmty. Coll., 930 F. Supp. 501, 501-06 (D. Kan. 1996), the court held that the employer had not violated the ECPA when it installed a video only surveillance camera in the school's security personnel changing room after reported thefts had transpired.

55. 135 F. Supp. 2d 623 (E.D. Pa. 2001).

56. *Id.* at 637-38.

57. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

58. *See* USA PATRIOT Act § 213 (providing for delays of notice of warrants).

The Act allows companies to alert and involve government agencies if an employee is using electronic communications for "unauthorized use."[59] The government, and possibly employers who comply with proper government requests under the Act, can bypass some security safeguards to view a myriad of personal information about employees. Thus, with a new interest in detecting threats not only to the company in question but also to the general public, employers may have even more flexibility in reviewing office communications. As Attorney General John Ashcroft heralded, "prevention is predicated on information."[60] Much public sentiment supports the Attorney General, and many welcome increased security in exchange for the loss of some aspects of privacy.[61] Further, Congress is contemplating giving employers in some industries access to FBI databases of arrests, convictions and other suspect lists.[62]

In addition to concerns regarding office e-mail and voicemail, employers are concerned about employee abuse of the Internet. Inappropriate use of the Internet is an important issue for many companies. In certain circumstances, if employees misuse the Internet, employers may be found liable. Moreover, misuse of the Internet may create a hostile work environment, divert the attention of a company's workforce, and diminish productivity and morale. Misuse by employees of the "Web" has caused a surge in the field of employee Internet management ("EIM"). At a recent conference, one research firm estimated that the market for EIM will approach $750 million by the year 2005.[63] Use of the Internet in the workplace also raises issues regarding employee privacy rights.[64] Most of the concerns about privacy and the Internet focus

59. *Id.* §§ 210, 212 (expanding government access to records which can be sought without a court order); *see also* James Heaphey, *Privacy Not Priority where Workplace Security is Concerned*, DAILY PRESS, Nov. 19, 2001, at C6.

60. Ann Davis, *How September 11 Changed America: Are We Safer Now Than Before Terror Attacks*, MSNBC, *available at* http://www.msnbc.comm/news/721031.asp?pne=msn (March 8, 2002).

61. However, many do not agree with the Attorney General. Some privacy advocates argue that increased security measures and methods directly infringe upon citizens' civil liberties. *See* ACLU, *at* http://www.aclu.org/privacy/privacymain.cfm; *see also* Privacy Foundation, *at* http://www.privacyfoundation.org.

62. Davis, *supra* note 60.

63. *Emerging Web Content and Employee Internet Misuse Continue to Drive Market for EIM Software*, BUSINESS WIRE, Feb. 20, 2002 at 1.

64. For more information regarding the Internet and privacy rights, *see* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L.

on the use of data collection and information stored or used without an individual's consent.[65] This concern is not limited to the workplace but is at the forefront of litigation on this matter.[66]

In *In re DoubleClick, Inc. Privacy Litigation*, the court held that the use of "cookies"[67] to access communications between an Internet user and Web sites visited while on-line did not violate the ECPA or the Wiretap Act.[68] The class action was filed by users of the World Wide Web, alleging that DoubleClick and its affiliated web sites collected personal information (names, e-mail addresses, telephone numbers, home and business addresses, previous web sites visited and previous searches on Internet), which users would not ordinarily expect advertisers to be able to collect without authorized access, in violation of several federal privacy acts.[69] The court held that DoubleClick's actions fell under an exception to the ECPA[70] or outside of the statute's purview since Defendant

288 (2001) (discussing anonymity and the Internet); *see also* Rachel K. Zimmerman, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century,* 4 N.Y.U. J. LEGIS. & PUB. POL'Y 439 (2000-2001); Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy; Cyberspace Filters, Privacy-Control, and Fair Information Practices,* 2000 WIS. L. REV. 743 (2000).

65. For a striking view into just how much information can be gathered about a user when surfing the Internet, visit http://www.privacy.net.

66. *See, e.g.,* Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585, 597 (S.D.N.Y. 2001) (holding that Internet user who downloaded supplier's software from website maintained by an unrelated site operator did not assent to licensing agreement not mentioned on unrelated site); *see also* Supnick v. Amazon.com, Inc., No. C00-0221P, 2000 WL 1603820, at *1 (W.D. Wash. May 18, 2000) (allowing for class action suit against software users for software that enables them to intercept and access Internet users' personal information).

67. "Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner." *In re* Doubleclick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001).

68. *Id.* at 514, 519 (citing 18 U.S.C. §§ 2701(c)(2), 2511(2)(d) (1994)).

69. 154 F. Supp. 2d at 503. Defendant was able to reap this personal information by using "cookies" placed or already in existence on Plaintiffs' computers. *Id.*

70. The statute states that it is not an offense to intentionally access without authorization, a facility through which an electronic information service is provided or to intentionally exceed an authorization to access that facility, and thereby obtain access to a wire or electronic communication while it is in electronic storage in a system if the conduct is authorized "by a user of that [wire or electronic communication] service with respect to a communication of or intended for that user." *Id.* at 507 (quoting 18 U.S.C. §§ 2701 (a), (c) (1994)). Congress subsequently the statute amended by the USA PATRIOT Act §209, 115 Stat. at 283, and eliminated storage from the definition of wire communication.

provided the service and the users freely used its service.[71] Further, the court held that Defendant's actions did not violate the Wiretap Act because they fell under the consent exception: the Plaintiffs freely used Defendant's service, Defendant's affiliates consented to the use of this information and Plaintiffs could not show that the Defendant's acts were done for criminal or tortious purposes.[72]

2. *Application of Federal Statutes to Telephone and Cellular Phone Surveillance*

Employers who have traditionally relied on supervisors to monitor employee performance are increasingly using technology, such as telephone monitoring, to track employee workplace operations and communications. In some industries, such as catalogue sales and telemarketing, listening to an employee's telephone conversations enables the employer to accurately assess the employee's contact with clients and the public. In these industries, employees understand that they may be monitored. However, in other industries an unstated presumption of employee privacy exists. Many employers, especially following September 11, surreptitiously monitor telephone calls under the "ordinary course of business" exception to the Federal Wiretapping Act.[73] A general policy authorizing monitoring does not necessarily establish that the monitoring of any particular call occurred in the ordinary course of business. Nor does "the fact that the technology is not eavesdrop-proof . . . in itself defeat any expectation of privacy."[74] Rather, each particular monitoring activity must be considered separately to determine whether it occurred in the ordinary course of business.

For example, in *Arias v. Mutual Central Alarm Services, Inc.*,[75] the court analyzed whether a central station alarm services company

71. 154 F. Supp. 2d at 513-14.

72. *Id.* at 519.

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a[n] . . . 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 in violation of the Constitution or laws of the United States or any State.

18 U.S.C. § 2511(2)(d) (1994).

73. *See supra* note 47.

74. Syposs v. United States, 181 F.R.D. 224, 228 (W.D.N.Y. 1998).

75. 182 F.R.D 407 (S.D.N.Y. 1998), *aff'd* 202 F.3d 553 (2d Cir. 2000).

illegally eavesdropped on employees' private telephone conversations. The court stated that the employer could avail itself of the ordinary course of its business exception.

> Here, the defendants' actions in recording—as distinguished from listening to—the telephone traffic into and out of their premises was amply justified by their legitimate interests in timely provision of emergency services, ensuring employee fidelity and protecting themselves against unfounded claims. Given the fact that alarm signals may be received at any time of the day or night, those interests could be served adequately only by the constant recording that was done. Accordingly, this Court holds that the interceptions—assuming the interceptions consisted of the recording—were made in the ordinary course of defendants' business.[76]

Further, in *Briggs v. American Air Filter Co.*,[77] the ordinary course of business exception applied where a supervisor reasonably suspected that an employee was disclosing confidential information to a competitor and had warned the employee of his suspicions. The court held that the supervisor acted in the ordinary course of business by listening in while the parties discussed business matters.[78]

The exception also applied in *Epps v. St. Mary's Hospital*.[79] An employer overheard a phone conversation in which an employee berated supervisors. The employer turned on a taping system to record the remainder of the conversation. The court held the exception applied because the conversation occurred during office hours, between co-employees, and concerned scurrilous remarks about supervisors.[80] The court stated, "[c]ertainly the potential contamination of a working environment is a matter in which the employer has a legal interest."[81]

Likewise, in *Ali v. Douglas Cable Communications*, the employer monitored calls made by its customer service representatives in order to supervise employee training and service.[82] Although the court found the employer had a legitimate purpose to monitor

76. 182 F.R.D. at 417.
77. 630 F.2d 414 (5th Cir. 1980).
78. *Id.* at 420.
79. 802 F.2d 412 (11th Cir. 1986).
80. *Id.* at 417.
81. *Id.*
82. Ali v. Douglas Cable Communications, 929 F. Supp. 1362, 1373 (D. Kan. 1996).

telephone calls, the court only recognized the legitimate purpose of monitoring business calls, not all calls.[83]

Case law also reflects the exception's limitations. Notably, in *Deal v. Spears*, the exception did not protect a liquor storeowner who suspected that a recent burglary of the store was an "inside job" involving one of his employees.[84] The employer installed a device to surreptitiously record all calls made or received at the store. The plaintiff employee, who was married, was having an affair with a second plaintiff, who also was married. The employer recorded about twenty-two hours of calls, many of which included sexually provocative conversations. The employer was unable to implicate the plaintiff in the burglary but did learn she sold her lover a keg of beer at cost, for which she was terminated. The employer argued that the monitoring came within the exception. The court disagreed and found the employer had violated the Federal Wiretapping Act by using the recording device.[85]

Similarly, in *Sanders v. Robert Bosch Corp.*,[86] the court held that the exception could not protect an employer when it attached a "voice logger" to record all phone calls. A security guard employed by a subcontractor of the company claimed the taping violated the Federal Wiretapping Act. The court held the taping was not protected by the exception because the logger was not "a telephone or telegraph instrument, equipment or facility," and there was no business justification for "the drastic measure of 24-hour a day, 7-day a week recording of telephone calls."[87]

Business calls generally fall under the exception to the federal wiretapping acts.[88] However, if the employer does not inform the employee that personal calls will be monitored, those calls may not be covered. The Eleventh Circuit has held that when an employer realizes that a call is personal and not business related, the employer must discontinue the monitoring of the call.[89] However, when an employee has been informed to abstain from making personal calls, the employee may then assume the risk that his calls

83. *Id.* at 1380.
84. Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992).
85. *Id.* at 1155-58.
86. 38 F.3d 736 (4th Cir. 1994).
87. *Id.* at 741.
88. Watkins v. L.M. Berry & Co., 704 F.2d 577, 581-83 (11th Cir. 1983) (holding that the employee had only consented to monitoring of business sales calls and not personal calls).
89. *Id.*

may be monitored.[90]

Originally, courts held that cellular telephone users had "no expectation of privacy in their conversations."[91] However, when the ECPA amended the Federal Wiretap Act, cell phones were included in its web of protection. In the wake of this amendment, courts have changed their perception on cell phones, holding that people reasonably expect privacy in their cellular phone conversations.[92]

More recently, courts have continued to apply this rationale. In *Bartnicki v. Vopper*,[93] the Third Circuit analyzed the federal statutes described in the preceding section and deciphered whether the press was liable for broadcasting a cell phone conversation between a teacher's union president and the union's chief negotiator when the conversation had been intercepted by an unknown person. The court found that those who had unlawfully intercepted the conversation violated Title III of the Federal Wiretapping Act.[94]

These federal acts do not preempt state statutes. Individual state statutes may also apply to private sector employees' privacy interests.

D. State Statutes

State legislatures may craft legislation that goes beyond that of the federal statutes. State laws vary; for example, some mandate that all parties must consent before monitoring can take place.

In New York, the statutory grants of the right to privacy to private sector employees are very limited. Under the New York wiretapping statute, the only clear exception applicable is express or implied consent.[95] Certain other statutes eliminate specified

90. *Id.*

91. *See, e.g.,* Tyler v. Berodt, 877 F.2d 705, 706 (8th Cir. 1989).

92. *See, e.g.,* Dunlap v. County of Inyo., 121 F.3d 715 (9th Cir. 1997); United States v. Kim, 803 F. Supp. 352, 362 (D. Haw. 1992). However, this perception does not necessarily apply for criminal cases. *See, e.g.,* United States v. Perez, 177 F. Supp. 2d 342, 348 (E.D. Pa. 2001) (holding that FBI wiretaps of defendant's cellular phone were properly conducted).

93. 200 F.3d 109 (3d Cir. 1999).

94. *Id.* at 125-29. However, the case rose to the Supreme Court, which went on to assume that the interceptor violated Title III of the Act and held that a stranger's illegal conduct does not remove the First Amendment protections for the press. Bartnicki v. Vopper, 532 U.S. 514, 535 (2001).

95. N.Y. PENAL L. § 250.25(1) (1999). *See also* N.Y. CIV. RIGHTS L. §§ 50-51, *supra* note 13.

methods of observation. For example, the General Business Law precludes surveillance equipment from being installed in specific areas of business (i.e. bathrooms, fitting rooms, etc.).[96] New York Penal Law prohibits wiretapping.[97]

Twenty-eight states have passed laws analogous to the ECPA.[98] For example, Connecticut law requires that employers who wish to monitor employees' communications provide written notice of the types of monitoring that they might perform.[99] Prior written notice is not required, however, when an employer has reasonable grounds to believe an employee is engaged in conduct that creates a hostile work environment, violates the law, or infringes on the legal rights of the employer or other employees.[100] Illinois' statute is limited to audible expressions and thus e-mail may not be included.[101] A Maryland statute covers mail surveillance but requires that the communication be intercepted.[102] Furthermore, Maryland law requires prior consent of all parties to the communication.[103] In California, vetoed legislation would have mandated that an employee receive notice of a policy before an employer could view the employee's personal e-mail and computer records.[104] California does extend constitutional privacy protection to private citizens, however.[105] West Virginia enacted a statute in 1999 that bars employers from using any form of electronic surveillance in areas designed for "the health or personal comfort of the employees or for safeguarding of their possessions, such as

96. N.Y. GEN. BUS. L. §395-b (McKinney 2002).

97. N.Y. PENAL L. §§ 250.05, 250.25. However, these statutes are not interpreted to grant a private right of action for their violation. 2 JONATHAN L. SULDS, NEW YORK EMPLOYMENT LAW, ch. 18-5 (2d ed. 2001) (citations omitted).

98. The states that have passed analogous legislation are: California, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, New Hampshire, New Jersey, New Mexico, Ohio, Oregon, Pennsylvania, Rhode Island, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

99. CONN. GEN. STAT. § 31-48d(3)(b)(1) (2001).

100. *Id.* § 31-48d(3)(b)(2).

101. 720 ILL. COMP. STAT. 5/14-2(d) (1993).

102. MD. CODE ANN. CTS. & JUD. PROC. § 10-402 (2002).

103. *See* State v. McGhee, 447 A.2d 888, 891 n.7 (Md. Ct. Spec. App. 1982).

104. *See* S. 1016, Reg. Sess. (Cal. 1999).

105. CAL. CONST. art. 1, § 1. The California Court of Appeals, in *TBG Ins. Serv. Corp. v. Superior Court of Los Angeles County*, 117 Cal. Rptr. 2d 155, 163-64 (Cal. Ct. App. 2002), held that when an employee has signed a monitoring policy and was given the use of an office and home computer for work use, and has consented to an employer's monitoring policy, there is no reasonable expectation of privacy under the state's constitution. *Id.* at 164.

rest rooms, shower rooms, locker rooms, dressing rooms, and employee lounges."[106]

After the September 11, 2001 terrorist attacks, state legislatures may follow the utilitarian path of Congress and, under a veil of citizen security, place an entire state's interest in safety above an individual's right to privacy.

III. WHAT COMPANIES ARE IMPLEMENTING AFTER SEPTEMBER 11 AND HOW THE AMERICAN WORKPLACE IS IMPACTED

A. New Safety Inquiries

After September 11, companies are instituting new methods of security. Employers lacking policies regarding office e-mail, Internet and telephone use are enacting such policies. As computer software enabling workplace surveillance drops in price and increases in sophistication, more employers are using electronic means of monitoring.[107] These methods affect not only the workplace as a whole,[108] but also individual employees. Companies that implemented computer monitoring programs to search for trigger words that signal potentially sexually harassing e-mails have now added to the programs words such as "bioterrorism" and "anthrax."[109] Additionally, some companies are extending background checks to all employees. While these methods may create a safer work environment, they must be carefully analyzed in light of federal and state laws because they may affect the employees' rights to privacy.

The multiple requirements of identification badges, fire alarm drills and emergency routes necessitate the need for employers to be advised of their employees' disabilities or impairments.

106. W. VA. CODE § 21-3-20 (2002).

107. Melynda Dovel Wilcox, *You're Being Watched*, KIPLINGER'S PERSONAL FINANCE, Feb. 2002, at 21-22.

108. This article does not directly address the concerns over workplace environments. However, the events of September 11 coupled with the bioterrorism attacks that sent anthrax into American workplaces generate concerns regarding workplace environment and safety. Occupational Safety and Health Administration (OSHA) rules and regulations, 29 U.S.C. § 654 (2002), grant employers a general duty to provide employees with a safe workplace. How far employers must go to prevent anthrax or other bioterrorism attacks in the workplace has not been determined. Employers should reevaluate their security and safety measures to promote a safe workplace under the circumstances.

109. Wilcox, *supra* note 107, at 21-22.

Normally, employers should avoid asking about an individual's disability or impairment as it relates to his job duties. The EEOC ordinarily issues guidance on topics regarding the Americans with Disabilities Act ("ADA"), such as privacy and emergency evacuation procedures.[110] Since September 11, employers must weigh safety concerns against sensitivity towards personal privacy. Therefore, employers are more inclined to ask about impairments in the possibility of an emergency and/or evacuation.[111] With safety as the basis for applying the new requirements, and as long as the level of privacy expected is made clear, the consensus among many is that employees must abide by the employers' policies.[112] Some feel that at a minimum this applies to an employee's age and ethnicity. Because age and race are protected categories under the anti-discrimination laws, amassing a database with this information, even if done under the veil of "safety," may trigger more civil rights litigation if followed by adverse employment actions.

Technology has had a monumental effect upon our ability to store information. Personal information, such as that derived from background checks, which was once filed or stored in cabinets, can now be condensed and easily transferred to a disk or e-mail file or stored on a hard drive or network. Digital storage has also made the process of searching cheaper.[113] The ease with which information can now be sought, gathered, and received was at one time unfathomable.[114]

Post-9/11, employers are using the new technology to determine who exactly is in their workplace.[115] Background check companies state that there is a great influx in the use of such

110. 42 U.S.C. §§ 12112(b)(5)(A), (d) (1990).

111. *See* 16 EMPLOYMENT LITIGATION REPORTER, Dec. 11, 2001, at 10.

112. Carrie Johnson, *Life in Cyberspace; Loss of Privacy Could be Price of Security*, NEWSDAY, Nov. 21, 2001, at C02. One attorney cited in the article stated that if an employee can show that the information required on a mandatory identification badge is "a cover for another kind of information" in a protected category such as age or ethnicity, then the employee may be able to make a discrimination claim. *Id.*

113. *Id.*

114. In the past, many databases were not connected. If an employer based in New York wanted to conduct a search of a potential employee's criminal record, he would have to search each state and county database. Now, some companies have linked databases together to create a more efficient and cost effective search method. *See* Lisa Guernsey, *What Did You Do Before the War?*, N.Y. TIMES, Nov. 22, 2001, at G1.

115. *Id.*

services as they have changed from a luxury to a necessity.[116] One spokesperson for a background check company stated that in October and November 2001, his company had a thirty-three percent increase in business from employers who were re-evaluating security.[117] Background checks that were once used primarily for screening applicant pools are now used to check current employees.[118] Even with this new surge, the question still remains: How far can employers delve into an employee's background before intruding upon an employee's (or potential employee's) right to privacy?

Under amendments to the Fair Credit Reporting Act ("FCRA"),[119] employers who use "consumer reports" must meet stringent standards for disclosure and consent. To fall within the scope of the FCRA, a report must be prepared by a "consumer reporting agency," a business that is regularly paid to gather and report information on consumers for third parties.[120] Before an employer obtains a report on an existing employee or a job applicant, the employer must notify the individual in writing.[121] Further, the employer must obtain written authorization from the employee or applicant before the background check can take place.[122] Moreover, specific requirements govern adverse action by the employer based on information discovered in the report.[123] If the employer is going to use the report in his decision not to hire, the employer must provide the potential employee with a copy of the report accompanied by a statement of the prospective employee's rights.[124] Employers, however, may not use the information revealed in the report as a basis for refusal to hire unless the nature of the offense would create an "unreasonable risk" to property or safety in the work environment.[125]

Some argue an increase in background checks will not create safer work environments. One commentator opined that sophisticated criminals will use the technology to stay ahead of

116. *Id.*
117. *Id.*
118. Christopher A. Weals, *Workplace Privacy, The Tide Has Turned, Opening the Door for Employers to Snoop – and More,* LEGAL TIMES, Feb. 4, 2002, at 27.
119. 15 U.S.C. § 1681 (1997).
120. *See* 15 U.S.C. § 1681a(p).
121. 15 U.S.C. § 1681b(b)(2)(a).
122. *Id.* § 1681b(b)(2)(b).
123. *Id.* § 1681b(b)(3).
124. *Id.*
125. *See* N.Y. CORRECT. L. § 752.

investigators, and pointed out that the hijackers of the planes crashed on September 11 did not buy homes, cars, or apply for loans, which would have created a residual electronic trail.[126] As extensive searches increase and employees assert their privacy rights, the clash between the competing interests will continue.

B. What is the Best Way to Inform Your Employees of Your Company's Policy?

To reduce the risk of claims, companies may benefit from having a clear electronic communication policy. An employer may not provide sufficient notice by simply stating that ownership of office property allows the employer unfettered discretion to search electronic communications at any time. A clearly presented policy informs employees: (1) that their modes of electronic communication, such as office computers and phones (including cell phones), cannot be misused for unprofessional and/or inappropriate communications; (2) what constitutes unprofessional or inappropriate misuse; (3) that the electronic devices are the property of the company; and (4) that employees should not have any expectation of privacy in the use of these devices or the communications they exchange. Moreover, the policy should inform employees of the possible legal consequences of electronic communications. A policy that encompasses these specifications has been highly regarded by the judiciary.[127]

Employers should consider many different factors when creating an electronic communication policy. The policy should state who will have access to the information viewed, the purpose of the use, those to whom the information may be disclosed, and that the information may be stored on a separate computer. Unauthorized use by employees may be deterred if they also are placed on notice of the repercussions of misuse. This includes a warning stating that no employee should use e-mail for communications containing racial slurs, sexual harassment, or other inappropriate comments. Knowing that a supervisor could view e-mail correspondence with other employees may deter an employee from discussing inappropriate topics. This would not

126. Guernsey, *supra* note 114.

127. *See* TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 162 (Cal. Ct. App. 2002) (discussing incentives for, and correct inclusions of, employer policies on electronic communications).

only protect the employee, but would also help the employer avoid liability for the employee's acts. When drafting policies, employers should also consider employees' interests; solely considering the employer's business interests may generate policies that fail to address the employee's privacy concerns.[128] In summary, an employer should conceive of appropriate ways to minimize privacy expectations while being sensitive to the potential impact on employee morale.

These suggestions do not necessarily apply to all employers. Nevertheless, employers are encouraged to inform employees that they are under surveillance at work, and each company should have a policy tailored to its needs. Furthermore, there are a variety of ways to notify employees of the company policy. A key requirement is that the employer obtains some form of consent, whether explicit or implicit. While a signature page that affirmatively confirms assent to the company's policy and provides clear evidence of consent would be most beneficial, the consent requirement could be achieved in numerous other ways. Other examples include mandating employee acknowledgment of receipt of e-mail messages concerning the company's policies and notifying employees via the employee handbook that the company adheres to a policy by which it reviews employee e-mail.

It is essential that employers take immediate steps to protect themselves from potential privacy claims. Suggested preventive measures include establishing a privacy checklist. Such a checklist includes the following:

- Awareness of Current Law: Stay apprised of the most current law and its application to your actions;
- Notice: Give applicants and employees notice of intended monitoring and the method of the intended monitoring;
- Purpose of Monitoring: Ensure that monitoring is directly related to the purposes and functions of the employee's job;
- Means of Monitoring: Use reasonable and unobtrusive means to monitor employees when necessary; and
- Confidentiality: Safeguard the confidentiality of private information obtained about employees.

128. Jeremy U. Blackowicz, *E-mail Disclosure to Third Parties in the Private Sector Workplace*, 7 B.U. J. SCI. & TECH. L. 80, 101 (2001). For example, within its business related interest, an employer may justify reviewing an employee's personal e-mail regarding other companies. The employee's concern focuses on disclosure of proprietary information contained in her e-mail. *See id.*

C. *Discovery and the Importance of Data Retention*

Occasionally, e-mails are problematic for employers embroiled in sexual harassment and race discrimination cases.[129] Abuses of company e-mail by employees can lead to the distribution of racially charged[130] or sexually harassing e-mails[131] to the entire company or to a selective group of targeted individuals. In either case, such e-mails could give rise to a claim of discrimination. Once legal action commences, the discovery process can create large obstacles for the employer. The e-mails in question may have been stored on the system and thus subject the employer to grave liability if it is forced to disclose the contents of its networks and databases.

IV. CONCLUSION

The atmosphere of the workplace post-9/11 has changed dramatically. With the passing of the USA PATRIOT Act of 2001, employee privacy rights in the private workplace are declining now more than ever. However, this decline does not indicate that employee privacy rights are not of major concern or a hotly contested issue. For this reason, employers should establish e-mail and voicemail policies to protect themselves and ensure efficient business practices. The implementation of policies can aid in preventing employer liability on multiple fronts, including liability for employees who misuse such communication methods and invasion of privacy claims. In the new workplace, the schism between privacy and safety may coalesce upon the notion that it is better to be safe than sorry.

129. For further analysis on the vast liability that e-mail can create for employers, *see* Gregory I. Rasin & Joseph P. Moan, *Fitting a Square Peg Into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace*, 66 MO. L. REV. 793, 804-07 (2000).

130. *See, e.g.*, Owens v. Morgan Stanley & Co., No. 96 Civ. 9747, 1997 WL 403454, at *1 (S.D.N.Y. July 17, 1997) (granting defendant's motion for summary judgment while granting plaintiffs the opportunity to file an amended complaint in a suit by African American employees premised upon, amongst other things, an allegedly racist e-mail).

131. *See, e.g.*, Strauss v. Microsoft Corp., 856 F. Supp. 821, 821-23 (S.D.N.Y. 1994) (denying defendant's motion for partial summary judgment in a dispute in which a female worker alleged that her supervisor's sexually charged e-mails were offensive).