Virtual Performance: Employment Issues in the Electronic Age

by Tanya E. Milligan

Communication technology is advancing at a much faster rate than the laws governing the employer-employee relationship. This article addresses the risks associated with electronic communications in the workplace and laws protecting employee electronic activities.

In the electronic age, employers rely heavily on instant communication with clients and employees. It is commonplace, if not necessary, in today's business world for employers to allow employees to access the Internet through employer-owned computers and smartphones. In 2007, 54 percent of in-house counsel responding to a survey stated that their company allows employees to use instant messaging at work, requiring an Internet or intranet connection.[1] Additionally, 74 percent of companies allow employees to access the corporate network from their home computers on the Internet.[2] These new modes of communication present challenges for employers and employees.

This article discusses the risks associated with employee use of electronic communications and the reasons employers monitor their employees' electronic activities, including e-mails, instant messages, text messages, blogs, and moblogs. The article also explores various causes of action available to employees in connection with their use of electronic communications, including the bases for employee privacy rights, how current federal employment laws protect employee electronic activities, and the possible bases for employee wrongful discharge claims. Attorneys should be aware of these risks and causes of action when counseling employees regarding their electronic activities and counseling employers regarding policies, procedures, and disciplinary actions.

Monitoring Employee Cyber Activities

Employers choose to monitor employee electronic activities for a variety of reasons, from a desire to protect the company's confidential and proprietary information, to improving employee productivity. As explained more fully below, monitoring can lead to an increased risk of litigation. Therefore, the decision to monitor and the manner of doing so should be made with the advice of counsel.

Confidentiality

Most employers invest substantial financial resources in developing their products, services, processes, systems, and methods. The resulting confidential information often is extremely valuable to the business, and it can be financially devastating if the information is revealed to a competitor or the public. Many thefts and inadvertent disclosures of confidential information are committed by company employees, and monitoring employee communications on the Internet can protect confidential information.

Google evidently monitors its employees' electronic activities—it fired an employee after just eleven days of employment for allegedly blogging on the employee's personal website about, in the blogger's words, "vague financial-related things."[3] Eli Lilly & Co. recently learned that a mistaken mouse click can be devastating.[4] The company was in confidential settlement talks with a government agency concerning its most profitable drug, Zyprexa, when one of Eli Lilly's outside counsel accidentally sent an e-mail containing confidential and comprehensive settlement negotiations to *The New York Times*. The outside counsel had intended to send an e-mail to her co-counsel; instead, a *New York Times* reporter with the same last name popped up in the attorney's e-mail contact list.[5]

Trade Disparagement and Defamation

The Internet, an easily accessible and extremely wide-reaching medium of communication, democratized the nature of public speech. Freedom of the press, as one court noted, "is [no longer]

Coordinating Editor

John M. Husband, Denver, of Holland & Hart LLP—(303) 295-8228, jhusband@hollandhart.com

About the Author

Tanya E. Milligan is Of Counsel in the Denver office of Holland & Hart LLP.

Labor and Employment Law articles are sponsored by the CBA Labor and Employment Law Section to present current issues and topics of interest to attorneys, judges, and legal and judicial administrators on all aspects of labor and employment law in Colorado.

limited to those who own one."[6] Anyone with access to the Internet can "become a town crier with a voice that resonates farther than it could from any soapbox."[7]

A company's reputation in the community—for example, for quality of work, timeliness, or goodwill—can be as valuable an asset as any of its confidential information. Goodwill adds tremendous value to a company. Therefore, an employer has a substantial interest in knowing what its employees are saying about the company on the Internet that may affect how its products or services are viewed.

For example, Ellen Simonetti, a Delta Air Lines flight attendant, maintained a blog, "Queen of the Sky: Diary of a Flight Attendant." Simonetti alleged she was fired by Delta for posting photos of herself in uniform on an airplane and for comments posted on her blog that her employer deemed inappropriate.[8] Simonetti sued Delta for wrongful termination, discrimination, and defamation.

Although her claims still are unresolved, her termination by Delta, ostensibly to protect its trade name and goodwill, came with the cost of defending this litigation and the countless articles published about it.[9] Even so, in November 2008, Virgin Atlantic Airways fired thirteen flight attendants after they posted joking messages on Facebook about passengers and faulty airplane engines.[10]

HealthSouth also resorted to litigation to protect its goodwill. A former employee of HealthSouth posted several embarrassing and personal allegations about HealthSouth's CEO and his wife on a Yahoo! Finance message board.[11] The individual posted under the name "I AM DIRK DIGGLER," a reference to the male porn star character in the movie *Boogie Nights*.[12] The postings were quintessential defamatory statements—false statements that harm or tend to harm an individual's reputation or standing in the community.[13] Although HealthSouth was successful in determining the identity of the blogger and ending the defamation, it is not known what damages HealthSouth recovered. As it turns out, the blogger was a food-service worker at Penn State University, who, as a result of the lawsuit, lost his job.[14]

Productivity—"Cyberloafing"

Employees often use employers' online and e-mail services to pay bills, e-mail family and friends, shop for gifts or other personal items, or chat with office colleagues. According to a survey by America Online and salary.com, the average worker admits to wasting more than two hours per eight-hour workday, and 44 percent of respondents cited Web surfing as their top time-waster.[15] Increasing productivity and commitment is a constant concern for employers, because wasted employee hours directly affect the bottom line. Thus, employers have a substantial interest in monitoring employee electronic activities in relation to productivity.

Employee Discrimination and Security

Federal law requires employers to maintain a workplace free of sexual, racial, and other types of harassment. Employees might blog on their personal websites using sexist or sexually explicit comments or racial epithets when discussing their co-workers. Such conduct is even more troubling if the employee is a manager or supervisor, because the employer can be held strictly liable for such discriminatory remarks if they affect the working conditions of other employees.[16] An employee also might use his or her blog to express threats of violence at the workplace or against other employees, or even a third party.

There is legal precedent for requiring an employer to take affirmative action to prevent violent or illegal behavior against a person who is not an employee of the company. In *Doe v. XYC Corp.*,[17] company computer technicians and supervisors discovered that an employee was using the employer's computer system to visit pornographic websites while at work. Because the employer had a policy against monitoring the Internet activities of its employees, the company did not take any action. Later, it was discovered the employee also was taking illicit pictures of his 10-year-old stepdaughter and using his office computer to publish the photos on the Internet.

In a lawsuit initiated by the girl's mother, the New Jersey Superior Court reversed the lower court's summary judgment, holding that the employer was on notice of the employee's activities and was under a duty to investigate further and to take prompt action. The case was returned to the trial court.[18] Thus, an employer may be held liable for an employee's electronic activities—even when those activities affect third parties but no other employees.

Employee Causes of Action Based on Electronic Activities

Given the volume and variety of risk associated with employee electronic activities, more employers are monitoring their employees' electronic activities and taking employment actions based on these activities. In doing so, employers should be mindful that existing laws may protect certain electronic activities. Some of the most common causes of action available to employees are discussed below.

Public Sector: First Amendment Protection

Employee privacy rights can vary widely depending on whether the employee works in the public or private sector. Public sector employers are state actors and must conform their actions to the protections under the U.S. Constitution, specifically the First and Fourth Amendments. Whether a government employee's speech is protected by the First Amendment determines whether the government employer may discipline the employee based on that speech. In other words, if speech is protected, the public employer cannot discipline an employee for exercising his or her First Amendment rights.

The U.S. Supreme Court's opinion in *Garcetti v. Caballos*[19] addressed government employees' First Amendment rights to free speech. The Court stated that public employees do not lose their First Amendment rights to speak on matters of public concern simply because they are public employees. Nevertheless, the Court recognized that freedom of speech is not absolute and government employers need a significant amount of control over their employees' words and actions to efficiently provide public services.[20]

The Court described the appropriate analysis regarding whether the First Amendment protects a public employee's speech. The first step of the analysis has two parts: (1) the employee must speak as a citizen; and (2) the speech must be regarding a matter of public concern. If the employee is speaking as a citizen and the speech is regarding a matter of public concern, the second step is to determine whether the government entity had an adequate justification for treating the employee differently from any other member of the general public.[21]

The First Circuit applied the *Garcetti* analysis in a case involving a corrections officer, Curran, who was terminated for the content of his blog entries posted on a website hosted by the employees' union.[22] In his comments, Curran complained that the sheriff unfairly disciplined and harassed his political rivals and union members. Curran compared the sheriff to Hitler and referenced, with approval, the few German soldiers who plotted against Hitler's life, ending one of his blog entries with the words "death before dishonor."

The First Circuit held that, even though Curran was speaking as a citizen and some of his statements regarded matters of public concern, the sheriff's department was justified in terminating his employment, because his postings contained speech "going far beyond providing information in which there was a legitimate public interest."[23] Defamatory, vulgar, insulting, and defiant speech is entitled to less weight when determining whether the government entity had an adequate justification for treating the employee differently.[24] Moreover, the sheriff's department did not have to show an actual adverse effect to terminate Curran—the risk of disruption to the department from the text was enough.[25]

Garcetti did not alter the general rule that private employees usually are not entitled to First Amendment protection.[26] To the contrary, the Supreme Court emphasized that "[g]overnment employers, like private employers, need a significant degree of control over their employees' words and actions."[27] *Garcetti* affirms the right of every employer to control its employees' official job-related speech, stating that "the First Amendment does not prohibit managerial discipline based on an employee's expressions made pursuant to official responsibilities."[28]

Public Sector: Fourth Amendment Protection

A government employer's attempts to monitor the electronic activities of its employees may be considered a "search" for Fourth Amendment purposes. If a search violates the Fourth Amendment, the results of the search may not be used as the basis for an employment decision.[29]

The analysis for determining whether a government employee has a privacy right in his or her computer files is similar to the analysis regarding privacy rights in an employee's office, desk, or personal papers. Whether a government employer can search its employees' computer depends on the employees' expectations of privacy and the reasonableness of the search. Notice of the right to search, coupled with the consistent and not-infrequent conduct of searches, are critical to a finding that a public employee has no reasonable expectation of privacy.[30]

In 2008, the Ninth Circuit held that the city of Ontario, California violated a police sergeant's privacy rights by reading the text messages he sent and received on his department-issued pager.[31] The city had a policy restricting the use of communications systems to city business. The city also had a practice of requiring employees to pay the overage charge if the employee exceeded his or her allotment of 25,000 characters. Employees were informed that the text messages would not be audited if the employee agreed to pay the overage charge.

Frustrated with the drain on administrative resources to collect overage charges from employees, the city contacted its text message provider, Arch Wireless Operating Co., and requested transcripts of the text messages. The city audited the transcripts to determine whether the overage charges were caused by personal use, or whether the city needed to increase the character amount to cover work-related communications. The investigation revealed that many of the text messages sent and received by plaintiff, John Quon, were personal and sexually explicit.[32]

Quon sued the city, alleging a violation of his Fourth Amendment right to privacy. The Ninth Circuit ruled that the city violated Quon's privacy, holding: (1) Quon had a reasonable expectation of privacy in the messages, given the city's practice of not auditing text messages; and (2) the search was unreasonable, because the city could have used less intrusive means to determine whether it needed to increase the character amount.[33]

Strong policies and practices can go far in helping clarify an employee's expectation of privacy or lack thereof. This case demonstrates, however, that if an employer fails to enforce its computer use policy or does so inconsistently, the policy might be ineffectual in litigation.

Private Sector: Invasion of Privacy

Because private sector employers are not state actors, generally, private sector claims of privacy are based in the common law tort of "intrusion upon seclusion" or "invasion of privacy." The basis for a claim of invasion of privacy is whether the intrusion would be considered highly offensive to a reasonable person.[34] Thus, whether the employee had a reasonable expectation of privacy will guide the analysis of whether the employer can access the employee's information and act on that information.

Courts generally have held that an employee does not have a reasonable expectation of privacy in the employer's computer or e-mail system. In *McLaren v. Microsoft Corp.*,[35] the Texas Court of Appeals concluded that an employee had no reasonable expectation of privacy in the contents of e-mail messages sent and received over the employer's e-mail system and stored on the employee's office computer.

Following termination, the plaintiff-employee brought suit for invasion of privacy, alleging the employer "broke into" some personal e-mail folders that were stored under a private password, separate from the password needed to log on to the computer, and released the e-mail folders to third parties.[36] The employee argued that the additional password gave rise to a legitimate expectation of privacy in those e-mail messages. The employee analogized this situation to a case where an expectation of privacy was found to exist with regard to the contents of an employee locker that was locked with a private padlock brought from home.[37] The court refused to analogize employee e-mail to an employee's assigned locker, because the locker was meant for storage of personal items, whereas e-mail and workplace computers are intended for the employee to perform the functions of the job.[38]

McLaren is illustrative of the direction courts are taking with regard to employee expectation of privacy in the private sector. Clear policies stating that the employee has no expectation of privacy in the employer's computer and equipment, and that the employer will monitor the communications systems, further reduce any employee expectation of privacy and, thus, risk of liability under such a claim.

Federal Omnibus Crime, Control and Safe Street Acts

In 1968, Congress enacted the Omnibus Crime, Control and Safe Street Acts, or "Wiretap Act," which prohibits private individuals and employers from intercepting wire or oral communications, including telephone, computer, or electronic communications.[39] Additionally, most states have laws that prohibit interception of telephone and electronic communications. There are three elements to a violation of the Wiretap Act: (1) intentional or reckless disregard of the law; (2) a wire, oral, or electronic communication; and (3) an interception.[40]

> The "interception" element has proven to be the most interpreted aspect of the statute. Courts have held that an interception must occur contemporaneously with transmission.[41] Accordingly, the Wiretap Act does not apply to communications in electronic storage—either before or after being sent—because opening and reading such communications would not occur at the time of transmission. Therefore, where an e-mail has been sent but remains unread in the recipient's inbox, a third party may open the e-mail and read the stored communication without violating the Wiretap Act.
>
> In one case, where the Secret Service seized a computer used to operate an electronic bulletin board system that contained private, unopened e-mails, the Fifth Circuit held there was no violation of the Wiretap Act.[42] Due to the courts' interpretation of "interception," the Wiretap Act has only very narrow applicability to employee monitoring contexts because, technologically, it

is almost impossible for an employer to "intercept" an e-mail as that term is interpreted.[43]

Federal Electronic Communications Act and Stored Communications Act

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to expand the protections of the Wiretap Act. The ECPA prohibits the interception of e-mail transmissions by: (1) unauthorized individuals; or (2) individuals working for a government entity acting without a proper search warrant.[44] Although the ECPA generally is concerned with the unauthorized interception of electronic communications by business competitors, it does not specifically exempt employers monitoring the e-mail of its employees.[45]

However, the ECPA has several exceptions to the prohibition on intercepting e-mails. The three most relevant to the workplace are: (1) where one party consents; (2) where the provider of the communication service can monitor communications; and (3) where the monitoring is done in the ordinary course of business.[46] Employers have fit fairly easily into the consent exception to the ECPA by instituting policies and procedures in their employee handbooks indicating that they will monitor electronic and e-mail communications, and by requiring employees to sign an acknowledgment indicating their consent to abide by the policies and procedures in the employee handbook or stating that continued employment indicates consent.[47]

The Stored Communications Act is part of the ECPA and generally provides privacy protection for facilities through which electronic communications are stored.[48] Some of the exceptions to the protection are: (1) access authorized by the person or entity providing a wire or electronic communication service; or (2) access authorized by a user of that service with respect to a communication of or intended for that user.

In *Konop v. Hawaiian Airlines*,[49] the Ninth Circuit applied the Stored Communications Act to a case involving an employer who accessed an employee's blog without authorization. The plaintiff, a pilot and employee of Hawaiian Airlines, maintained a website that contained commentary critical of the Airlines' management practices. The website required users to have an assigned username and password to access the site, and most registered users were other Hawaiian Airlines employees. The users also were required to abide by the terms and conditions of the website, which included a prohibition on allowing management to view the website and a prohibition on disclosing the website's contents to any other person.[50]

A senior manager used the usernames and passwords of other employees, with their permission, to access the website and view the pilot's blog entries. The Ninth Circuit held that the senior manager violated the Stored Communications Act because, although the employees who authorized the manager's access had usernames and passwords, those employees had never accessed the website and, thus, they were not users within the plain meaning of that term.[51] Because the Stored Communications Act allows only a user or provider to give authorization, the senior manager's access of the blog violated the Stored Communications Act.

The case was remanded to the trial court for an assessment of damages allowable under the Stored Communications Act.[52] *Konop* is illustrative of the pitfalls an employer may encounter by

being overzealous in its attempts to monitor and control its employees' Internet activities.

National Labor Relations Act

The National Labor Relations Act is a federal act that protects the rights of employees to form unions, engage in collective bargaining, organize strikes, and engage in concerted activities.[53] If an employer monitors employee electronic activities, it should take care to avoid improper interference with employee attempts to unionize, in violation of the Act.

In 2007, the National Labor Relations Board (NLRB), the entity charged with enforcing the Act, considered whether a policy that prohibited the use of e-mail for all non-job-related solicitations interfered or restrained employees in the exercise of their right to form unions.[54] The union president sent three e-mails to other employees using the company e-mail system. Two of the e-mails were found to be solicitations to support union activity, and the union president was disciplined as a result of the violation of the Communication Systems Policy.[55]

In finding that the employer did not violate the Act, the NLRB reaffirmed that an employer has a "basic property right" to "regulate and restrict employee use of company property."[56] The opinion stated that the Act provides "no statutory right to use employer-owned property, such as bulletin boards, telephones, televisions, and now email, as long as the employer's restrictions are nondiscriminatory."[57] The NLRB held that employees are not entitled to the most convenient or most effective means of communication for unionizing purposes, and they have no additional right to use an employer's equipment for those purposes regardless of whether the employees are authorized to use that equipment for work purposes.[58]

Employers that permit employees to use electronic communication systems, including e-mail, smartphones, instant messaging systems, or other means to communicate with one another (perhaps even blogging during work hours) must be careful to implement policies that prevent abuses and prohibit excess personal use, but do not unreasonably interfere with protected activity.

Sarbanes-Oxley Act and State Whistleblower Laws

In 2002, the U.S. Congress passed the Sarbanes-Oxley Act (SOX).[59] SOX contains important protections for employees of publicly traded companies who are discriminated against in retaliation for reporting corporate fraud or accounting abuses.[60] SOX protects internal whistleblowers who provide information regarding mail fraud, wire fraud, bank fraud, or securities fraud to a person of supervisory authority or a person who has the authority to investigate such conduct.[61] Employers are prohibited from taking actions against such employees that are likely to stifle the behavior Congress intended to encourage.[62]

Additionally, the legislatures of seventeen states have enacted statutes designed to protect employees in the private sector who participate in whistleblowing.[63] Many of these states have substantially similar provisions defining the types of activities protected. The most common protected activities are: (1) disclosing certain information to employers and/or public entities; (2) appearing before public bodies or courts of hearings or inquires; and (3) refusing to obey directives.[64]

It is not uncommon for employees to use e-mail or blogs to voice concerns or complaints about their employment conditions. If such e-mails or blog postings raise issues related to company fraud, accounting abuses, or matters of public policy, the employee's e-activity may be protected by state or federal laws related to whistleblowers. In such situations, the employer should be careful about making employment decisions based solely on the content of the employee's e-mails or blog postings.

Common Law Wrongful Discharge

Concurrently with the enactment of whistleblower protection laws by state legislatures, the judiciaries of forty-five jurisdictions in the United States have recognized common law protections for employees who allege their employment was wrongfully terminated in retaliation of conduct in furtherance of public policy.[65] Although the elements necessary to prove a claim for wrongful discharge vary from state to state, generally, public policy prohibits discharge of employees in three circumstances: (1) where an employee was discharged for refusing to commit an illegal act; (2) where an employee was discharged for exercising a statutory right; or (3) where an employee was discharged for carrying out an important civic duty.[66]

Employers should consider the laws in their states regarding wrongful discharge before disciplining or terminating an employee due to the content of an employee's blog or other electronic speech. The content of the speech may be in furtherance of state-recognized public policy and afford the employee protection under state law by asserting a claim for wrongful discharge.

Conclusion

Given the amount and variety of risk of liability to employers associated with employees' electronic activities, employers are becoming more vigilant in monitoring such activities. Also, the technology associated with employee monitoring continues to increase in sophistication at a rate parallel to technology regarding communication systems. The decision to monitor employee e-activities has its own risks. To appropriately advise both employers and employees, attorneys should know and understand the laws governing employee privacy and speech, as well as how these laws are applied to the ever-evolving intersection of the workplace and the Internet.

Notes

1. Fulbright and Jaworski, "Fourth Annual Litigation Trends Survey Findings" (this question was asked for the first time in the 2007 survey and was not asked in the 2008 survey), available at www.fulbright.com/images/publications/FourthAnnualLitTrends.pdf.
2. *Id.*
3. *See* 99zeros.blogspot.com/2005_01_01_archive.html. *See also* www.news.com/Google-blogger-I-was-terminated/2100-1038_3-5572936.html (Feb. 11, 2005).
4. *See* www.portfolio.com/news-markets/top-5/2008/02/05/Eli-Lilly-E-Mail-to-New-York-Times. *See also* www.nytimes.com/2006/12/20/business/20lilly.html.
5. *Id.*
6. *American Civil Liberties Union v. Reno*, 31 F.Supp.2d 473, 476 (E.D.Pa. 1999).
7. *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997).
8. "Delta employee fired for blogging sues airline," *USA Today* (Sept. 8, 2005), available at www.usatoday.com/travel/news/2005-09-08-delta-blog_x.htm.
9. *See* queenofsky.journalspace.com/?cmd=displaycomments&dcid=923&entryid=923.
10. *See* www.guardian.co.uk/business/2008/nov/01/virgin-atlantic-facebook.
11. Lidsky, "Silencing John Doe: Defamation & Discourse in Cyberspace," 49 *Duke L.J.* 855, 866-68 (2000).
12. *Id.*
13. Finkin, *Privacy in Employment Law* 91-92 (2d ed., 2003).
14. Lidsky, *supra* note 11 at 868.
15. "Wasted Time at Work Costing Company Billions," available at www.salary.com/careers/layouthtmls/crel_display_nocat_Ser374_Par555.html.
16. *Wyninger v. New Venture Gear, Inc.*, 245 F.Supp.2d 976, 981 (S.D.Ind. 2003) ("[w]here, the alleged harassment was committed by management and culminate in a tangible job detriment, the employer is subject to strict liability"), *citing Burlington Industries v. Ellerth*, 524 U.S. 742 (1998) and *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998).
17. *Doe v. XYC Corp.*, 887 A.2d 1156, 1158-60 (N.J.Super. 2005). *See also Satterfield v. Breeding Insulation Co.*, No. E2006-903 (Tenn. Sept. 9, 2008) (employer owed a duty of care to the daughter of one of its former employees for asbestos exposure).
18. *Doe, supra* note 17 at 1170.
19. *Garcetti v. Caballos*, 547 U.S. 410, 126 S.Ct. 1951 (2006).
20. *Id.* at 1957-58.
21. *Id.* at 1958.
22. *Curran v. Cousins*, 509 F.3d 36 (1st Cir. 2007).
23. *Id.* at 48.
24. *Id.* at 49.
25. *Id.* at 49-50.
26. *German v. Fox*, 2007 WL 1228481 at *6 (W.D.Va. April 25, 2007), *citing Dixon v. Coburg Dairy, Inc.*, 369 F.3d 811, 817 n.5 (4th Cir. 2004) ("First Amendment does not apply to private employers").
27. *Garcetti, supra* note 19 at 1958.
28. *Id.* at 1961.
29. *O'Connor v. Ortega*, 480 U.S. 709, 714-15 (1987).
30. *See U.S. v. Simmons*, 206 F.3d 392 (4th Cir. 2000); Finkin, *supra* note 13 at 245-46.
31. *Quon v. Arch Wireless Operating Co.*, No. 07-55282, slip op. 7000 (9th Cir. June 18, 2008).
32. *Id.* at 7006-07.
33. *Id.* at 7016-27.
34. *Restatement (Second) of Torts* § 652B (1965).
35. *McLaren v. Microsoft Corp.*, 1999 WL 339015 (Tex.App. May 28, 1999).
36. *Id.* at *1-2
37. *Id.* at *4.
38. *Id.*
39. 42 U.S.C. §§ 2510 to 2520.
40. 18 U.S.C. § 2511(1)(a).
41. *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003).
42. *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994).
43. As the Wiretap Act currently is interpreted, an employer with automatic routing software capable of intercepting e-mails after they are sent but before they reach the employee's inbox may run afoul of the Act. *See U.S. v. Councilman*, 418 F.3d 67, 85 (1st Cir. 2005).
44. 28 U.S.C. §§ 2701 *et seq*.
45. *See* "Electronic Privacy Rights: The Workplace," available at www.lectlaw.com/files/emp41.htm.
46. *Id.*
47. *See* White, "E-Mail @ Work.com: Employer Monitoring of Employee E-Mail," 48 *Ala. L.Rev.* 1079, 1083-85 (1997).
48. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 (9th Cir. 2002) *cert. denied*, 537 U.S. 1193 (2003); 28 U.S.C. §§ 2701 *et seq.*
49. *Konop, supra* note 48 at 879.
50. *Id.* at 873.
51. *Id.* at 880.
52. *Id.* at 886.
53. 29 U.S.C. §§ 151 to 169.
54. *The Guard Publishing Company d/b/a The Register-Guard and Eugene Newspaper Guild, CWA Local 37194*, 351 NLRB No. 70 (Dec. 16, 2007).
55. *Id.* at 3.
56. *Id.* at 5, *citing Union Carbide Corp. v. NLRB*, 714 F.2d 657, 663-64 (6th Cir. 1983).
57. *Id., citing In re Mid-Mountain Foods, Inc.*, 332 NLRB 229, 230 (2000).
58. *Id.* at 6.
59. Westman and Modesitt, *Whistleblowing: The Law of Retaliatory Discharge* 156 (2d ed., 2004).
60. *Id.*; 18 U.S.C. § 1514A.
61. Westman and Modesitt, *supra* note 59 at 163.
62. *Id.* at 169.
63. *Id.* at 77 n.1 (the states are Arizona, California, Connecticut, Florida, Hawaii, Louisiana, Maine, Michigan, Minnesota, Montana, New Hampshire, New Jersey, New York, North Dakota, Ohio, Rhode Island, and Tennessee).
64. *Id.* at 79.
65. *Id.* at 95.
66. *Id.* ■