iBRIEF / eCommerce **Cite as 2001 Duke L. & Tech. Rev. 0026**

7/25/2001

MONITORING EMPLOYEE E-MAIL: EFFICIENT WORKPLACES VS. EMPLOYEE PRIVACY

Employer monitoring of electronic mail constitutes an emerging area of the law that is clearly unsettled at this point in time. This iBrief demonstrates that the privacy rights of non public-sector employees are relatively unprotected by the federal and state constitutions, broad judicial interpretations of enacted privacy legislation favor legitimate employer-monitoring practices, and many of the elements of common law claims are difficult for employees to prove.

INTRODUCTION

¶ 1 Employee use of electronic mail (e-mail) during business hours is a common characteristic of the 21st century American workplace. According to a recent study, over 130 million workers are currently flooding recipients with 2.8 billion e-mail messages each day.[1] Employers provide e-mail services to their employees as an efficient means of facilitating both intra-company communication and communication with the outside client base.[2] E-mail serves to increase the efficiency of today's workplace because it is inexpensive to provide, simple to install and easy to use.[3] E-mail usage also dramatically decreases the use of office-related, paper-based correspondence. However, despite these efficiencies, this technological advancement is also creating collateral problems concerning issues of employee privacy that today's legal environment appears unprepared to solve. This inadequacy in the law is primarily based on the fact that many employees do not know the extent of their privacy rights regarding their company-provided e-mail accounts. In fact, many employees operate under the false assumption that personal e-mail messages sent from work are protected from their employer's scrutiny.

¶ 2 It is interesting to note that employee privacy issues frequently arise in many areas of the work environment other than e-mail monitoring. Employers often monitor employee telephone calls and some companies also record the time each employee spends on bathroom breaks. One employer even "places a device in employees' chairs to measure worker 'wiggling,' presumably because more wiggling means less working."[4] These attempts at monitoring employee behavior, as silly as some may appear, represent aspects of a legitimate struggle

between the employer's ability to conduct its business operations and the employees' privacy rights, between worker efficiency and worker sanity and between technological advancement and current laws operating behind the technological curve.

¶ 3 This struggle is serious and its boundaries are rapidly moving into the arena of workplace e-mail. The problem with this advancement is that neither the United States Constitution, the respective state constitutions nor any federal or state statutes provide a clear concept defining the extent of employee privacy rights as they relate to work-related e-mail accounts. The common law, primarily via the tort of interference with seclusion, provides the most common means by which employees are attempting to define their privacy rights. However, it is often difficult for employees to meet all four of its elements. This iBrief examines the current legal framework encompassing this area and concludes with suggestions both employers and employees can use to protect themselves until the laws dealing with e-mail monitoring become more settled.

THE CURRENT STATE OF E-MAIL MONITORING

¶ 4 In the "pre-Internet world, companies tolerated use of office telephones and radios as ways to satisfy employee needs. The standard for when these resources were being abused and cutting into productivity, in what amounts to employee theft of wages, was intentionally left fuzzy."[5] However, with today's businesses constantly attempting to increase employee efficiency, employers are becoming more concerned with improving their employees' hourly productivity and are using the most current technology to achieve these goals.[6] In fact, employers have many legitimate reasons for desiring to monitor their employees' e-mail usage, such as:

1. Maintaining the company's professional reputation and image;
2. Maintaining employee productivity;
3. Preventing and discouraging sexual or other illegal workplace harassment;
4. Preventing "cyberstalking"[7] by employees;
5. Preventing possible defamation liability;
6. Preventing employee disclosure of trade secrets and other confidential information; and
7. Avoiding copyright and other intellectual property infringement from employees illegally downloading software, etc.[8]

¶ 5 These business justifications are compelling, but so are the reasons for protecting an individual's privacy. The breakeven point, the point at which a company's monitoring program achieves necessary business objectives while also adequately protecting employee privacy, depends primarily on the types of computer programs employers use to monitor their employees' e-mail. The following section discusses a few common surveillance programs that demonstrate different means by which information can be gathered.

E-MAIL MONITORING SERVICES AND PROGRAMS

¶ 6 There are many companies that are currently marketing e-mail monitoring services. The scope of these services range from a full e-mail monitoring application to a program that only records the time at which employees pick up their e-mail.[9] The full e-mail application program will record all of the following information:

1. The e-mail recipient;
2. The e-mail sender;
3. The number of words in the e-mail;
4. The time the employee spent reading e-mail;
5. The time the employee spent composing e-mail;
6. The number of attachments; and
7. The type of e-mail - business-related or non-business related.[10]

¶ 7 The less-intrusive "e-mail pick-up" program will monitor only the following information:

1. The employee name;
2. The date; and
3. The time the e-mail was picked up by the employee.[11]

¶ 8 Some of these services obviously cross the line between employers' legitimate business justifications and intrude into employees' privacy. For instance, a program entitled "Back Orifice 2000" is described as "a very powerful piece of software...[allowing] unlimited data access."[12] The current state of e-mail monitoring and the powerful nature of some of these monitoring programs create a need for up-to-date legal rules and concepts that employers and employees can turn to in an attempt to defend their business practices or to remedy an invasion of their privacy.

CONSTITUTIONAL PROTECTIONS

¶ 9 Simply put, "the extent of employees' privacy rights in the workplace depends on whether they work in the public sector or private sector. Because constitutional rights operate primarily to protect citizens from the government[13] 'state action' is required before a citizen can invoke a constitutional right."[14] Therefore, since most Americans work in the private sector, the United States Constitution and its corresponding Fourth Amendment privacy protection[15] provides little guidance in private sector e-mail monitoring situations.

¶ 10 The constitutions of eight states[16] explicitly protect privacy and offer greater protection of the rights of public employees than does the United States Constitution. However, as with the Constitution, these documents protect public employees and the protection does not extend to the private sector. "The one and only notable exception to this rule is the state of California, that has extended its state constitution's protection of privacy to private as well as public employees."[17]

¶ 11 Therefore, both employers and employees must look to current federal or state statutes, or to the common law, in order to gain any clarity concerning the legal issues surrounding the monitoring of employee e-mail.

FEDERAL STATUTORY PROTECTIONS

¶ 12 Congress responded to the lack of protection provided by the United States Constitution and the respective state constitutions by enacting the Electronic Communications Privacy Act of 1986 (the ECPA or the Act). The Act "prohibits the intentional or willful interception, accession, disclosure, or use of one's electronic communication."[18] "The ECPA defines [the term] 'electronic communication' as 'any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectric, or photocell system that affects interstate commerce."[19] Although e-mail is not specifically mentioned here, "the legislative history clearly shows Congress' intent to include it within the definition of 'electronic communications.'"[20]

¶ 13 The ECPA has three exceptions that serve to limit is applicability to employer monitoring:

1. The provider exception;[21]

2. The ordinary course of business exception;[22] and
3. The consent exception.[23]

¶ 14 The fact that the courts broadly interpret these three exceptions makes the ECPA's privacy protections illusory at best. An analysis of these exceptions will better illustrate this idea.

The Provider Exception

¶ 15 The provider exception is proving to be a strong ally to employers desiring to monitor their employees' e-mail. Concerning this exception, "commentators have predicted that most private employers will be exempt from the ECPA under this exemption if they provide their employees with e-mail service through a company-owned system."[24] In fact, a few courts have already applied this exception to employer e-mail monitoring. In one of the most interesting of these cases, the provider exception allowed United Airlines to monitor the online reservation system that it provided to employees in an attempt to discover falsifications by a travel agent.[25] However, there is confusion as to whether private employers will be protected under the ECPA if they merely use a third-party service provider.[26] In these cases, employers are not truly providing the e-mail services to their employees and would likely have to use one of the other two broad exceptions that the ECPA provides.

The Ordinary Course of Business Exception

¶ 16 The ordinary course of business exception is "actually an exclusion from the definition of an 'electronic device'" under the ECPA.[27] This exception has not been applied to workplace e-mail, "but based on its application in analogous contexts, such as telephone communications, it may well provide another shield for employers who engage in routine monitoring of their employees' e-mail.[28] Courts have taken two approaches when applying the ordinary course of business exception to telephone communications:

1. The content approach - which permits an employer to monitor "business-related" communications but does not allow monitoring of personal communications; and
2. The context approach - this approach looks to the employer's reason for monitoring its employees' communications to determine whether they had a legitimate business justification for the monitoring.[29]

¶ 17 It is likely that many courts will soon be willing to use these approaches when applying the ordinary course of business exception to employee e-mail communications. It is important that both employers and employees become aware of the method their state follows in telephone monitoring situations in order to determine which approach will likely apply to e-mail monitoring cases.

The Consent Exception

¶ 18 The consent exception "generally applies when one party to the communication has given prior consent, actual or implied, to the interception or accession of the communication."[30] Gaining employee consent can occur in at least two different ways. First, an employer can publish an e-mail monitoring policy to all employees.[31] Second, an employer can rely on the fact that its employees "are informed of an affirmative monitoring policy with regard to their e-mail, and they still choose to use the e-mail system."[32] In this case, these employees have effectively consented to the e-mail monitoring.[33] This is a powerful exception because of the ease with which an employer can create and provide a monitoring policy.

THE NOTICE OF ELECTRONIC MONITORING ACT

¶ 19 The Notice of Electronic Monitoring Act (the NEMA) is proposed legislation dealing with how often employers must inform their employees about electronic monitoring.[34] Under last year's version of this bill, "employers would be required to tell employees at the time of hire about electronic monitoring policy, notify workers annually, and whenever a material change in electronic monitoring practices occurs. The notice would include monitoring type, frequency, method, and use of the information. Employers would be exempt from giving notice when they reasonably believe that an employee is engaging in "harmful" or "illegal" conduct at work."[35]

¶ 20 This legislation, if enacted, would be a step in the right direction because it would help increase employee awareness regarding the lack of workplace privacy and also clarify to employers when and what type of electronic monitoring policy information they must distribute to employees.

STATE STATUTORY PROTECTIONS

¶ 21 If an employer cannot fit its situation under any of the exceptions listed above, or if an employee's cause of action is vulnerable because of the above-mentioned exceptions, state statutory law is unlikely to come to the rescue. Although some states have passed legislation similar to the ECPA, with the corresponding exceptions also being broadly interpreted by state courts, "no state has passed a law specifically aimed at employee e-mail privacy rights."[36]

COMMON LAW PROTECTIONS

¶ 22 The common law may be the best means to obtain a legal remedy when a person believes an employer has violated his privacy. In fact, studies show that "many employees are turning to traditional state tort law actions."[37] However, because of the difficulty employees often face in attempting to meet all of the required elements of the requisite causes of action, employers acting reasonably under the circumstances have little to fear from these common law causes of action.

¶ 23 The four most frequently invoked common law torts invoked by plaintiffs arguing that excessive e-mail monitoring violates their right of privacy are:

1. Unreasonable intrusion into the seclusion of another;
2. Appropriation of the other's name or likeness;
3. Unreasonable publicity given to the other's private life; and
4. Publicity that unreasonably places the other in a false light before the public.[38]

¶ 24 Of these four torts, "the tort of intrusion of seclusion is the most often cited as a basis for a claim by an employee against her employer for monitoring e-mail."[39] This tort provides that "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be offensive to a reasonable person."[40] Because this tort applies to invasions of privacy, "physical or otherwise," it could be extended to protect against e-mail monitoring.[41]

¶ 25 The hardest elements for an employee to meet, of the four comprising this tort, are the "highly offensive conduct" element and the "expectation of privacy" element. First, it will be difficult for an employee to show that her employer's conduct was highly offensive as long as the employer places employees on notice that it might monitor their e-mail. Second,

it is often difficult for an employee to show that his expectation of privacy in the workplace was reasonable because the employer is paying the employee to work during business hours and because the employer is providing all of the equipment used for e-mail purposes. Due to these difficulties, and those mentioned above, employers face few serious legal worries when monitoring employee e-mail.

CONCLUSION: HOW TO PROTECT YOURSELF AS AN EMPLOYER OR AS AN EMPLOYEE

¶ 26 With the law in this area unsettled and riddled with exceptions not fully tested by the courts, both employers and employees would be wise to undertake certain steps to protect themselves from potential problems this legal uncertainty creates.

¶ 27 Employers desiring to avoid liability for monitoring employee e-mail usage should "take all necessary steps to eliminate any reasonable expectation of privacy that employees may have concerning their use of company e-mail...systems."[42] This can be done through a detailed and clearly written electronic communications policy that is distributed regularly to as many employees as practicable before any monitoring begins.[43] This policy should inform employees of several things (including, but not limited to):

1. The absence of any private right by employees while using the company's e-mail. This could be accomplished by including a statement in the policy declaring that the employer's e-mail system is employer property, to be used for the purpose of furthering employer business. The policy should state whether personal e-mails are permitted, and define any limitations on personal use of the system.
2. An explanation of the rules governing the use of the e-mail system; and
3. The employer's ability and right to monitor, intercept, record and review all communications sent by employees over the company's e-mail system. This statement should contain language dealing with the employer's business reasons behind the monitoring and the circumstances under which such monitoring will take place. This statement should also contain a sentence stating that the employee has no expectation to privacy regarding any e-mails sent, received, or stored at the workplace.[44]

¶ 28 Employees, on the other hand, need to understand that current laws governing workplace e-mail will not protect them from excessive personal use. Most employers seem willing to tolerate some personal e-mail use and will police violations by looking more at

employee work product and ability to meet deadlines. In fact, employees will be safer using a personal e-mail account from work, as opposed to an employer-provided account, although employees must remember that excessive personal e-mail may still raise employer scrutiny as it will likely translate into a lower overall performance. However, employees should feel secure that excessive monitoring or other employer abuses of their monitoring privileges will almost certainly violate federal and state statutes and also create tort liability.

¶ 29 Employer monitoring of electronic mail constitutes an emerging area of the law that is clearly unsettled at this point in time. This iBrief demonstrates that privacy rights of non public-sector employees are relatively unprotected by the federal and state constitutions, broad judicial interpretations of enacted privacy legislation favor legitimate employer-monitoring practices, and many of the elements of common law claims are difficult for employees to prove. This current legal situation lies on technological frontier of the struggle between an employer's desire for an efficient workplace and an employee's right to privacy. As the 21st century workplace encounters new technological advances that both increase employee efficiency and create non-work-related distractions, it will be interesting to watch the legal system, through constitutional interpretation, new legislation, and changes in the common law, adapt to meet these new challenges.

By: Corey A. Ciocchetti

Footnotes

1. D. Hawkins, Office Politics in the Electronic Age Workplace, *U.S. News & World Report*, Mar. 22, 1999.

2. Sarah DiLuzio, Comment, Workplace E-Mail: It's Not as Private as You Might Think, 25 Del. J. Corp. L. 741, 741 (2000).

3. In only a few "mouse-clicks" any e-mail based document can be sent to a virtually unlimited number of recipients.

4. S. Elizabeth Wilborn, Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace, 32 Ga. L. Rev. 825, 825 (1998) (citing Robert G. Boehmer, Artificial Monitoring and Surveillance of Employees: The Fine Line dividing the Prudently Managed Enterprise from the Modern Sweatshop, 41 DePaul L. Rev. 739, 751 (1992)).

5. Matt Carolan, Whose e-mail is it, anyway? (visited July 21, 2001) http://www.zdnet.com/zdnn/stories/comment/0,5859,2556098,00.html>.

6. According to data from the American Management Association, in the first quarter of 1999, nearly 30 percent of major U.S. companies monitored employee e-mails, up from 20 percent in 1998 and 15 percent in 1996. Content Technologies, Inc., a company whose software reads incoming and outgoing messages, saw its sales double every year from 1996 through 1998. Mark S. Dichter and Michael S. Burkhardt, Electronic Interaction in the Workplace: Monitoring, Retrieving, and Storing Employee Communications in the Internet Age, Seminar before the American Employment Law Council, Fourth Annual Conference (Oct. 2-5, 1996). Also located on the World Wide Web at http://www.morganlewis.com/art61499.htm> (visited on July 23, 2001).

7. This term is defined as the act of "threatening, harassing, or annoying someone through multiple e-mail messages." Black's Law Dictionary (7th ed. 1999).

8. Terrence Lewis, *Pittsburgh Business Times*, Monitoring Employee E-Mail: Avoid stalking and Illegal Internet Conduct (visited July 21, 2001) http://www.pittsburgh.bcentral.com/pittsburgh/stories/ 2000/05/22/focus6.html>.

9. The Cost Benefits of Using IT Within Companies to Improve Communication (visited July 22, 2001) http://homepage.ntlworld.com/cotwj1/any_res/monitoring.htm>.

10. Id. This service provides a "fully functioning e-mail application that allows users to send and receive internal and external e-mail."

11. Id.

12. Id.

13. "Even for governmental employees, the Fourth Amendment offers only limited protection from workplace searches...The Fourth Amendment is only violated if public employees have a reasonable expectation of privacy. The standard requires balancing the employer's need for control and supervision of the workplace with the privacy interests of its employees." DiLuzio, supra note 2, at 744. See also O'Connor v. Ortega, 480 U.S. 709 (1987) (finding an government employee's expectation of privacy unreasonable when the

government actor is the employee's supervisor) and Steven B. Winters, Note, Do not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail, 1 S. Cal. Interdisc. L.J. 85, 116 (1992) (arguing that federal courts have so narrowly construed the public employee's work related privacy rights that the right of privacy has almost completely vanished).

14. Wilborn, supra note 4, at 828.

15. "The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizures by government officials. Although the Fourth Amendment does not explicitly mention a right to privacy, the Supreme Court has long interpreted it to include protection of such a right." DiLuzio, supra note 2, at 744.

16. DiLuzio, supra note 2, at 745 (citing Kevin B. Kopp, Comment, Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy, 8 Seton Hall Const. L.J. 861, 867 n. 36 (citing the constitutions of Alaska, California, Florida, Hawaii, Illinois, Louisiana, Montana and Washington).

17. Diluzio, supra note 2, at 745. See also Porten v. University of San Francisco, 134 Cal. Rept. 839, 842 (Cal. Ct. App. 1976) (recognizing a state constitutional violation even when there is no state action).

18. DiLuzio, supra note 2, at 745 (citing 18 U.S.C. §2511 (1994)). See also Kopp, supra note 16, at 868-70 (stating that the ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, and when the ECPA is read with Title III, intentional or willful interception of wire, oral, or electronic communication is prohibited).

19. 18 U.S.C. §2510(12) (1994).

20. DiLuzio, supra note 2, at 760 (citing Kopp, supra note 16, 868 n. 46) (citing Dichter and Burkhardt, supra note 6).

21. 18 U.S.C. §2511(2)(a)(i).

22. 18 U.S.C. §2511(2)(d).

23. 18 U.S.C. §2510(5)(a).

24. DiLuzio, supra note 2, at 746. See also 18 U.S.C. §2511(2)(a)(I) which specifically authorizes:

An officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service...

25. United States v. Mullins, 992 F.2d 14722 (9th Cir. 1992), *cert. denied*, 510 U.S. 994 (1993).

26. Kopp, supra note 16, at 871.

27. DiLuzio, supra note 2, at 74 7 (discussing 18 U.S.C. §2510(5) (1994)).

28. Id at 747.

29. Id at 760 n. 39.

30. 18 U.S.C. §2511(2)(d) (1994). The Act provides:

It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state.

31. Kopp, supra note 16, at 883 (citing Larry O. Gantt, II, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 Harv. J.L. & Tech. 345, 357-58 (1995)). "Many courts imply consent where an employee knew, or should have known, of an employer monitoring policy." DiLuzio, supra note 2, at 748.

32. DiLuzio, supra note 2, at 748.

33. This consent may still be implied even if these employees are "left with no other meaningful choice but to use the e-mail system." DiLuzio, supra note 2, at 748.

34. Last July, during the 106th Congress, Senator Charles Schumer (D-N.Y.) and Rep. Bob Barr (R-Ga.) introduced the original version of NEMA (titled H.R. 4098/S.2898). The full text of the bill is available on the World Wide Web at http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.4908>. *Northern Light* (visited July 23, 2001) http://special.northernlight.com/privacy/floodgate.htm>.

35. Id.

36. DiLuzio, supra note 2, at 749.

37. Diluzio, supra note 2, at 749-50 (citing Kopp, supra note 16, at 884).

38. Restatement, Second, of Torts 652A (1977).

39. DiLuzio, supra note 2, at 750 (citing Kopp, supra note 16, at 884).

40. Restatement, Second, of Torts 652B (1977).

41. DiLuzio, supra note 2, at 750. See also Kopp, supra note 16, at 885.

42. Lewis, supra, note 8.

43. Employees should also be required to sign an acknowledgement that they have "read, received, understood and agree to abide by the rules." Employee E-mails - Employer Considerations (visited July 21, 2001) http://www.nextevel-consulting.com/officemail.html>.

44. Id.