The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?

Nathan Watson*

* B.S., Indiana State University, 1999; Candidate for J.D., Indiana University School of Law—Bloomington, 2002.

I. INTRODUCTION

On July 20, 2000, an interesting mix of federal legislators proposed legislation that would affect monitoring of employee communications and computer usage in the workplace. Representatives Charles Canady (R.-Fla.) and Bob Barr (R.-Ga.) introduced the Notice of Electronic Monitoring Act (NEMA) in the House of Representatives, and Senator Charles E. Schumer (D.-N.Y.) introduced it in the Senate.[1] Had it passed, NEMA would have required employers to notify their employees if they wished to conduct surveillance of their employees' electronic mail ("e-mail") or other electronic communications.[2] The bill would have required the prior notice to include the form of communication that would have been monitored, the means by which monitoring would have taken place, the type of information that would have been obtained, the frequency of monitoring, and the intended use of the obtained information.[3]

Unfortunately, employer groups succeeded in getting the Judiciary Committee to pull the bill from further consideration.[4] They cited a potential increase in litigation and more work for human resources professionals in complying with NEMA.[5] The bill also languished in the Senate.[6] It is possible, however, that the bill will be reintroduced in both houses of Congress in the near future.[7]

Hopefully the bill will be reintroduced, because the monitoring of workplace e-mail is an issue that needs to be addressed. Union and employee advocacy groups have complained about electronic monitoring, contending that such practices are an invasion of privacy, cause work-related stress and low morale, and can be used in an unfair manner.[8] And while public employees may be protected to some degree under the Constitution from such invasions of privacy, private employees can not rely

1. *Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987 and H.R. 4908 Before the House Subcomm. on the Const. of the Comm. on the Judiciary*, 106th Cong. (2000) [hereinafter *Hearings*].

2. H.R. 4908, 106th Cong. § 2711 (2000).

3. *Id.*

4. *See* Jeff Moad, *Should You Really Be Reading This On Company Time?*, EWEEK, Sept. 22, 2000, *available at* 2000 WL 18178994.

5. *Id.*

6. *See id.*

7. Loretta W. Prencipe, *Federal Law on Employee Privacy Will Likely Open the Litigation Floodgates*, INFOWORLD, Mar. 26, 2001, at 64.

8. Bobby C. Vaught et al., *The Attitudes of Managers Regarding the Electronic Monitoring of Employee Behavior: Procedural and Ethical Considerations*, AM. BUS. REV., Jan. 1, 2000, at 107.

on such protection.[9] Private employees must look elsewhere to find protection, such as state law or even the federal wiretapping statute. The effect of these alternatives on electronic monitoring is ambiguous. This ambiguity needs to be addressed now through a clear standard, so employers are able to install policies without fear of litigation. This will also allow employees to know their rights and what is expected of them at the workplace. NEMA, through its notice requirement, sets a clear standard and marks a fine compromise between employer and employee interests.

This Note argues that NEMA should be adopted, since it would improve the current state of affairs relating to electronic surveillance in the workplace. The Note asserts that NEMA will positively benefit both employers and employees by establishing a "bright line" that takes into consideration both parties' interests. Part II addresses the current state of the law regarding electronic monitoring, with a focus on e-mail. Part III discusses NEMA and addresses the arguments for and against it. Finally, Part IV argues that the current version of NEMA is satisfactory and should be enacted into law.

II. DEVELOPMENT OF THE LAW RELATING TO ELECTRONIC MONITORING

The advent of the Internet has revolutionized the workplace. In particular, the ability to send e-mail has benefited companies and employees alike. In a poll of more than 1,000 employees conducted by Vault.com, "80 percent said e-mail has replaced 'snail mail' [regular mail] for the majority of their business correspondence, 72.5 percent said it has replaced faxing, and 45 percent said it has replaced phone calls."[10] Vault.com estimates that forty million users will send sixty billion e-mail messages per year.[11]

E-mail is generally speedy and easy to use for those who have access to it. These positive attributes are not without negative side effects, however. Since e-mail is readily available in most workplaces, some employees may use it for matters unrelated to their jobs, such as for sending personal messages. Employers may have several concerns about personal use of their computer resources, including potential liability to other employees or third parties, disclosure of sensitive information, and

9. Alexander I. Rodriguez, Comment, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L.J. 1439, 1439 (2000).

10. Terence Chea, *Workplace is Being Altered by E-Mail*, WASH. POST, June 29, 2000, at E7.

11. Barbara Kate Repa, *Computers and E-mail on the Job: They're Watching You*, *at* http://www.vault.com/nr/main_article_detail.jsp?article_id=18716&ht_type=5 (Nov. 18, 2000).

waste of time and resources. A recent example of this problem is the case of "Brad," an attorney at a prestigious London law firm who gained unwanted Internet notoriety after forwarding an e-mail he had received from his friend Claire which complimented his "sexual prowess."[12] The e-mail, initially sent to four male friends of Brad, ended up being forwarded to computer users around the world.[13]

Due to incidents such as these, many employers are interested in how employees are using their computers on company time. According to a survey from the American Management Association, forty-five percent of U.S. firms monitor their workers' electronic communications, including e-mail, voice mail, and Internet use.[14] Monitoring software has become more advanced, allowing employers to record every word of an e-mail message or to monitor Internet surfing.[15]

Of course, monitoring comes at the expense of an employee's privacy. Critics of electronic monitoring claim that it leads to "increased levels of stress, decreased job satisfaction and quality of work life, decreased levels of customer service and poor quality."[16] These criticisms have led to a national debate over whether employer computer surveillance is proper. The current state of the law favors the employer side of the debate. For example, the federal statute regulating wiretapping has been interpreted to cover e-mail, but it is riddled with exceptions that allow electronic monitoring in the private workplace.[17] Most courts have not been sympathetic to employees' claims for invasion of privacy, holding that there is not enough of a privacy interest to justify such claims. Why the federal wiretapping statute and the invasion of privacy claims do not provide protection for employees are discussed below.

A. Electronic Communications Privacy Act of 1986

Congress first attempted to deal with new privacy issues resulting from advances in technology with the Electronic Communications Privacy

12. T.R. Reid, *Brad the Cad Disciplined But Not Fired*, WASH. POST, Dec. 22, 2000, at C3.

13. *Id*.

14. John Yauckey, *Firms Crack Down on E-Mail: Spreading Off-Color Humor is No Joke*, USA TODAY, June 28, 2000, at 2B.

15. *Id*.

16. Vaught, *supra* note 8. In the Vault.com survey mentioned above, forty-two percent of employees stated that they worried about employers monitoring their e-mail. Chea, *supra* note 10. Seventy-nine percent reported using a separate account (such as Yahoo! or Hotmail) to check their personal correspondence. *Id.*

17. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

Act of 1986 (ECPA).[18] The ECPA, among other things, amended the Omnibus Crime Control and Safe Streets Act of 1968 "to protect against the unauthorized interception of electronic communications."[19] Congress adopted the ECPA to bring the federal criminal law "in line with technological developments and changes in the structure of the telecommunications industry."[20]

The ECPA first amended the Act by proscribing the interception of "electronic communication," as well as wire and oral communications.[21] The term "electronic communication" certainly includes e-mail. Even though e-mail is not mentioned in the text of the ECPA, the Act defines "electronic communication" as "any transfer of . . . data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce . . . ."[22] This definition would definitely include e-mail. Also, the legislative history of the ECPA indicates that e-mail is covered by the statute.[23]

Courts are split, however, on what an "interception" means in regard to electronic communications. Some courts have determined that an interception under this provision means only the interception of e-mail in route to the receiver, which can be a span of milliseconds. For example, in *Steve Jackson Games, Inc. v. United States Secret Service,*[24] the Secret Service seized a computer from the plaintiffs pursuant to a warrant. Plaintiffs used the computer to operate an electronic bulletin board service ("BBS"), from which users could send and receive private e-mail.[25] The court found that, evidently, the Secret Service agents read the private e-mail stored on the BBS.[26] The plaintiffs sued the Secret Service under Title I of the ECPA, claiming that the reading of e-mail sent to a BBS, but not

18. *Id*.

19. S. REP. NO. 99-541, at 1 (1986).

20. *Id.* at 3.

21. 18 U.S.C. § 2511 (1994). The statute states that "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" shall be subject to criminal penalty or civil suit. 18 U.S.C. § 2511(1)(a). This is referred to as part of Title I of the ECPA, or the Wiretap Act. Title II of the ECPA, discussed below, covers the unauthorized assessing of stored communications.

22. 18 USC § 2510(12) (1994).

23. The report detailing the legislative history discusses "electronic mail." *See* S. REP. NO. 99-541 at 3-5 (1986). Subsequent court decisions have also assumed that e-mail is within the purview of the ECPA. *See* Wesley Coll. v. Pitts, 974 F. Supp. 375 (D. Del. 1997).

24. 36 F.3d 457 (5th Cir. 1994).

25. *Id.* at 458.

26. *Id.* at 459.

yet retrieved by the recipient, was an interception under the statute.[27] The court found otherwise, holding that interceptions did not apply to electronic communications in electronic storage.[28] Since the e-mail at issue was in electronic storage, the ECPA did not apply. Other courts have also adopted this narrow view of interception under the ECPA.[29]

In *Konop v. Hawaiian Airlines*,[30] however, the Ninth Circuit rejected *Jackson.* In this case, plaintiff Konop was a pilot for defendant Hawaiian Airlines. Plaintiff maintained a Web site criticizing the defendant, which could only be accessed with a username and password provided by plaintiff himself. After the employer accessed the site using the username and password of another pilot, plaintiff sued under the Wiretap Act. The court first noted that "[i]f interception requires that acquisition and transmission occur contemporaneously, then unauthorized downloading of information stored on a web server cannot be interception."[31] Instead of accepting this rule, however, the court rejected the need for simultaneous acquisition and transmission, and held instead that "the Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit."[32]

Even if e-mail was intercepted under the Wiretap Act, there are several exceptions that might allow an employer to monitor e-mails without authorization. First, section 2511(2)(a)(i) of the ECPA allows a provider of "electronic communication service . . . to intercept . . . [a] 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."[33] For example, employers can use this provision to argue that monitoring is

27. *Id*.

28. *Id.* at 461-62. The court's reasoning was based on United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976), which held that an intercept under the federal wiretapping statute required a "contemporaneous acquisition of the communication." It also based its reasoning on the use of the word "transfer" in the ECPA's definition of "electronic communication" in section 2510(12) and on the omission in the same provision of the phrase "any electronic storage" (as compared to the provision for wire communications, which did include electronic storage of wire communications). Jackson, 36 F.3d at 461-62.

29. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 634-635 (E.D. Pa. 2001) ("The Wiretap Act provides protection for private communication only during the course of transmission."); Eagle Inv. Sys. v. Tamm, 146 F. Supp. 2d 105, 112 (D. Mass. 2001) ("[T]his court concludes that the ECPA did not eliminate the during-transmission requirement from the Wiretap Act.").

30. Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001).

31. *Id.* at 1043.

32. *Id.* at 1046.

33. 18 U.S.C. § 2511(2)(a)(i) (1994).

necessary to prevent excessive personal use of the system.[34]

Second, section 2510(5)(a) allows a network provider to intercept an electronic communication on a device furnished to the user by a provider of "electronic communication service in the ordinary course of its business and being used by the . . . user in the ordinary course of its business."[35] This is the so-called business use exception, and it would seemingly allow employers to monitor employee e-mail as long as there is a legitimate business purpose for doing so.[36] Finally, section 2511(2)(d) allows interception of a communication where a party has consented.[37]

Therefore, whether an employee would have an action under the Wiretap Act for an employer's unauthorized monitoring of e-mail is unclear. If interception under the Act is narrowly defined (as in *Jackson*), this would effectively end such claims, since the only way for an employer to be liable would be to capture the communication *en route* to the recipient. The reading of e-mails in storage would fall outside the scope of the Act. Even if there is an interception, one of the exceptions to the Wiretap Act may allow the employer to monitor e-mails.

There is another possibility for e-mail protection under the ECPA. Section 2701 prohibits the interception of electronic messages in storage.[38] Several courts have interpreted this section to cover e-mail in storage, which encompasses most e-mail.[39] The disadvantage of using this section is that it is less flexible in awarding damages.[40] Furthermore, the ECPA also lists several exceptions to this rule regarding electronic communications.[41] There are two main exceptions in section 2701(c) which state that the

34. *See* Rodriguez, *supra* note 9, at 1452.

35. 18 U.S.C. § 2510(5)(a) (1994).

36. *See* Rodriguez, *supra* note 9, at 1451. This exception has not yet been applied to any recorded cases involving e-mail.

37. 18 U.S.C. § 2511(2)(d) (1994). Consent is discussed below, under the ECPA's provision for accessing stored communications.

38. *Id.* § 2701(a). The statute reads:

> Except as provided in subsection (c) of this section whoever— (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

Id.

39. *See* Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994). *But see* Fraser, 135 F. Supp. 2d. at 635-36 (holding that the Stored Communications Act "provides protection for private communication only during the course of transmission.").

40. *Compare* 18 U.S.C. § 2520(c)(2) (1994) *with* 18 U.S.C. § 2707(c) (Supp. V 1999).

41. *See* Rodriguez, *supra* note 9, at 1450-60.

above rule does not apply to conduct "by the person or entity providing a wire or electronic communications service,"[42] or a "user of that service with respect to a communication of or intended for that user."[43]

Employers who have their own e-mail system *may* fall within the definition of a service provider.[44] The ECPA defines an "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[45] In *Bohach v. City of Reno*,[46] a United States District Court held that a police department was a "provider" of a paging system to its officers, and as a provider, could "do as [it] wished when it comes to accessing communications in electronic storage."[47] Using the rationale of this case, and the literal language of the statute, it seems that the ECPA would allow an employer who supplies an employee with e-mail and Internet access to fall within this exception.[48] It is unclear, however, whether an employer who contracts with a third party to supply e-mail and Internet access to employees would fall under this section.[49]

Section 2701(c) also provides an exception for conduct authorized by a "user of that service with respect to a communication of or intended for that user."[50] Thus, a communication may be accessed if one of the parties to the communication consents.[51] Of course, this provision does not matter when there is no consent among the parties. Whether an employee consents to having his e-mail checked by his employer is the issue, however, as consent may be actual or implied. While there have been no cases addressing this issue under the section 2701(c)(2) exception, there have

42. 18 U.S.C. § 2701(c)(1) (1994).

43. *Id.* § 2701(c)(2). The (c)(3) exception covers governmental conduct. *Id.* § 2701(c)(3).

44. *See id.* The legislative history of the ECPA is silent on whether an employer can fall within the provider exception. *See* Jarrod J. White, Commentary, *E-Mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1089 (1996).

45. 18 U.S.C. § 2510(15) (1994).

46. 932 F. Supp. 1232 (D. Nev. 1996).

47. *Id*. at 1236.

48. *See* Scott A. Sundstrom, Note, *You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2072 (1998).

49. *See* White, *supra* note 44, at 1088-89; *see also* Rodriguez, *supra* note 9, at 1452 (arguing that "the provider exception should not [apply to] employers who furnish networks through public providers.").

50. 18 U.S.C. § 2701(c)(2) (1994).

51. *See In re* DoubleClick Inc. Privacy Litig., No. 00-Civ.0641, 2001 U.S. Dist. LEXIS 3498 (S.D.N.Y. Mar. 28, 2001) (holding that information submitted to web sites could be accessed by the defendant because access was authorized by "user" web sites).

been cases involving a similar provision in the Wiretap Act.[52]

In *Deal v. Spears*,[53] the defendant store owners had asked the plaintiff, their employee, to cut down on her personal use of the store's phone. They also told her that "they might resort to monitoring calls or installing a pay phone in order to curtail the abuse."[54] The defendants recorded twenty-two hours of the plaintiff's conversations with her lover, and eventually fired her for violating a store policy. The plaintiff sued under the ECPA, and the defendants claimed that the plaintiff had consented to the recording based on section 2511(2)(d). The court of appeals held that while "actual consent may be implied from the circumstances," implied consent could not be found in this case, since the defendants "did not inform [the plaintiff] that they were monitoring the phone, but only told her they might do so in order to cut down on personal calls."[55]

As the surrounding circumstances must indicate that the employees "*knowingly agreed* to the surveillance,"[56] an employer would have to have a set, announced policy about monitoring e-mail in order to meet section 2511(2)(d) or 2701(c)(2). An employee's use of company e-mail could then be seen as implied consent to monitoring. Cases like *Deal* would allow the consent provision to apply as long as the policy stated that the employer *would* be monitoring e-mail, and not that they *might* monitor. The employer should carefully adhere to the policy, however, in order to avoid reaching outside the boundaries of consent.[57]

While the ECPA clearly covers electronic mail, it does not adequately define what an employer may and may not do in monitoring employee e-mail. It does not mesh well with the current technological realities of e-mail; as a result, ambiguity reigns. For example, can an employer be a service provider under the statute? What is required for consent? Until now, the employer has won suits involving e-mail and the ECPA; yet,

52. 18 U.S.C. § 2511(d) (1994). This provision states:

> 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 . . . .

Id.

53. 980 F.2d 1153 (8th Cir. 1992).

54. *Id.* at 1155-56.

55. *Id*. at 1157 (citing *Griggs-Ryan v. Smith*, 904 F.2d 112 (1st Cir. 1990), which held that recorded conversations were exempted under the consent provision because the plaintiff told the defendant that she would be recording all incoming calls).

56. Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993) (emphasis in original).

57. *See* Sarah DiLuzio, Comment, *Workplace E-Mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741, 748 n.47 (2000).

given the current public debate over e-mail surveillance, it is possible that a court could sympathize with an employee and hold his employer liable under the Act.[58]

B. Privacy Torts

In addition to options provided by the ECPA and similar state provisions, employees have the option of filing invasion of privacy claims against employers who engage in the unwanted monitoring of electronic communications. There are four basic torts for invasion of privacy under the common law: (1) unreasonable intrusion upon the seclusion of another; (2) commercial exploitation of a person's name or likeness; (3) public disclosure of private facts; and (4) depiction of a person in a false light.[59] The few reported cases dealing with employer monitoring of employee e-mail have concerned the first tort: intrusion upon seclusion.

Unfortunately, as with the ECPA, the few cases that deal with this issue do not give a clear answer as to whether employees have any protection from unwanted monitoring. While two courts have found that employees do not have a valid intrusion upon seclusion claim against their employers, one court has found there may be such a claim. These cases are discussed below.

In *Smyth v. Pillsbury*,[60] the U.S. District Court for the Eastern District of Pennsylvania dealt with a wrongful discharge claim brought by an employee who had been fired for "transmitting what [the employer] deemed to be inappropriate and unprofessional comments over [the employer's] e-mail system."[61] The defendant employer had repeatedly assured its employees that all e-mail communications would be "confidential and privileged," and that "e-mail communications could not be intercepted and used by defendant against its employees as grounds for termination or reprimand."[62] The plaintiff received e-mails from his supervisor through the defendant's system on his home computer, and had exchanged e-mails with the advisor. The defendant intercepted these messages, which he later alleged to contain threats to "kill the backstabbing bastards" and a reference to an office party as the "Jim Jones Koolaid

58. 18 U.S.C. § 2701 (1994 & Supp. V 1999). For example, there could be liability by finding that the employer intercepted a stored communication under section 2701 and that the employer did not fall within the service provider exception. *Id*.

59. Rodriguez, *supra* note 9, at 1462. These privacy torts are based on Prosser's four proposed privacy actions, which were subsequently adopted into the Restatement (Second) of Torts. *See also* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

60. Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996).

61. *Id*. at 98-99.

62. *Id*. at 98.

affair."[63]

The federal court dismissed the complaint. It began by stating that, under Pennsylvania law, a wrongful discharge claim was not valid unless the discharge "threatens or violates a clear mandate of public policy."[64] The plaintiff had argued that his termination "was in violation of 'public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law.'"[65] He argued that this right to privacy was manifested in Pennsylvania's recognition of the tort of intrusion upon seclusion.

The court cited the Restatement (Second) of Torts definition of this tort: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."[66] The court then held that the plaintiff had failed to state a claim because there was not a "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."[67] In other words, since the employee communicated over the employer's system, he had lost any expectation of privacy in his messages. Furthermore, the court stated that even if there were a reasonable expectation of privacy, the interception of these messages would not be "a substantial and highly offensive invasion of his privacy."[68] The court also cited the employer's interest in monitoring employee activity over its e-mail system and the fact that the employee did not have to disclose personal information or subject himself to an invasion of his person.[69]

In *McLaren v. Microsoft*,[70] the Texas Court of Appeals reached a similar conclusion. The defendant employer suspended the plaintiff based on accusations of sexual harassment. The plaintiff requested that "no one tamper with his Microsoft office workstation or his e-mail."[71] After being terminated, the plaintiff sued based on invasion of privacy, alleging that the defendant broke into the personal folders on his office computer. He argued

63. *Id.* at 98, n.1.
64. *Id.* at 99.
65. *Id.* at 100.
66. *Smyth*, 914 F. Supp. at 100.
67. *Id.* at 101.
68. *Id.*
69. *Id.*
70. McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 at *1 (Tex. App. 1999).
71. *Id*.

that there was an expectation of privacy because the personal folders were only accessible with a personal password. The court disagreed with this argument because the defendant had provided the workstation for use related to his employment and not personal use. The court also found that the invasion was not highly offensive, as in *Smyth*.[72]

In the 1996 Massachusetts case of *Restuccia v. Burk Technology*,[73] however, the complaining employees were more successful. In this case, a fellow employee advised the defendant supervisor that one of the plaintiff employees was spending a lot of time using the company's e-mail system. That evening, the supervisor used a supervisory password to access the backup files containing employee e-mail messages, and he read the messages for approximately eight hours. The e-mail messages between the two plaintiffs (the other was also an employee) included nicknames for the advisor and references to his extramarital affair. The plaintiffs were terminated, and the defendant stated that the reason for the termination was the excessive quantity of e-mails, not their content.[74]

Accordingly, the plaintiffs alleged several causes of action, including wrongful termination, invasion of privacy, and unlawful interception of wire communications. With respect to the last claim, the Massachusetts court held that the interception was allowable under the state wiretapping law, which contained an exception for those who possessed "an office intercommunication system which is used in the ordinary course of their business."[75]

The court refused to grant summary judgment on the invasion of privacy and wrongful termination claims, however. The court held that there was a genuine issue of material fact as to whether the plaintiffs had a reasonable expectation of privacy in their e-mails. Also, since there was the possibility of a reasonable expectation of privacy, and since the plaintiffs' wrongful termination claims were based on the alleged public policies found in state statutes prohibiting wiretapping and invasion of privacy, the court denied summary judgment on the wrongful discharge count.[76]

72. *Id*. at *13.

73. Restuccia v. Burke Tech., Inc., No. 95-2125, 1996 Mass. Super. LEXIS 367 at *1 (Mass. Super. Ct. 1996).

74. *Id*. at *3.

75. *Id*. at *5.

76. *Id*. at *9-10.

C. State Laws Regarding Electronic Monitoring

Another source of potential protection for employees is state constitutional provisions. For example, California explicitly recognizes a right to privacy in its state constitution and has applied that right to private sector searches.[77] Courts in that state have held that infringement of an individual's "specifically-identified" privacy rights is only justified when the rights are outweighed by a competing interest.[78] Note that California is an exception to the general rule regarding constitutional protection of privacy. In most states, it is doubtful that their constitutions similarly protect employees.

A related alternative is to pursue a state constitution-based tort claim similar to the claim pursued in *Luedtke v. Nabors Alaska Drilling, Inc.*[79] In *Luedtke*, the Alaska Supreme Court held that even though an employee drug testing program did not violate the state constitutional right to privacy, public policy favors employee privacy which exists, as "evidenced in the common law, statutes and constitution of this state."[80] A violation of this policy amounts to a violation of the implied covenant of good faith and fair dealing, and is a wrongful discharge.[81] Therefore, an employee might argue that public policy prohibits employers from monitoring e-mail. As yet, however, no state has ruled to this effect.[82]

In addition, some states have statutes that are spin-offs of the ECPA. These statutes basically mirror the ECPA, but some provide stricter exceptions than the federal act.[83] Yet no state statutes have been passed that focus primarily on e-mail.[84] California's legislature considered a bill similar to NEMA which would have "prohibited employers from monitoring employees' e-mail or computer files unless the employee had signed an

77. CAL. CONST. art. I, § I. Ten states, including California, explicitly recognize the right of privacy in their constitutions, but only California has applied this right to private actors. Rodriguez, *supra* note 9, at 1446-47.

78. Rodriguez, *supra* note 9, at 1447.

79. Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123 (Alaska 1989). *See also* Rodriguez, *supra* note 9, at 1447-48.

80. *See Luedtke*, 768 P.2d at 1132.

81. *See id.* However, the Alaska Supreme Court held that the discharge in this case did not violate the implied covenant of good faith and fair dealing, based on another public policy supporting health and safety. *Id.* at 1133.

82. *See* White, *supra* note 44.

83. *See id.* at 1089-90.

84. See *id.*

agreement acknowledging the employer's right to monitor."[85] California Governor Gray Davis vetoed the legislation, however.[86] Therefore, employees who seek protection from workplace monitoring and employers who seek certainty do not find an easy answer in state law.

D. Summary

As the above discussion shows, the state of law regarding electronic monitoring of e-mail is uncertain. Employees who are subjected to such monitoring have several possible courses of action, such as suing under the ECPA or state provisions, or pursuing common law privacy claims. However, these courses of action do not guarantee success. Particularly where e-mail is concerned, these options either fail to or refuse to account for new technologies in protecting employees from surveillance. Moreover the success of an employer varies from state to state, depending on the various privacy protections of each state. This lack of uniformity can be dangerous to employer-employee relations, and is precisely why NEMA is needed.

III. THE PROPOSED ACT

NEMA is limited in scope. It does not ban or even limit electronic monitoring in the workplace. In addition, no substantive rights are given to employees that would allow them to refuse to be monitored. Instead, NEMA merely requires that employers give notice to employees that electronic monitoring will take place. This notice must include the form of communication that will be monitored; the means by which monitoring will take place; the kind of information that will be obtained; the frequency of monitoring; and the intended use of the obtained information.[87] While this seems like a modest change, the notice requirement actually marks a good point of compromise for employers and employees alike. Employers may be deterred from more extreme forms of workplace monitoring if they are required to give notice.[88] This, of course, is in employees' interests. Employees given notice may also be deterred from abusing employer-supplied e-mail and Internet access, aiding employer interests as well.

85. Allison R. Michael & Scott M. Lidman, *Monitoring of Employees Still Growing*, NAT'L L. J., Jan. 29, 2001, at B17.

86. *Id*.

87. H.R. 4908, 106th Cong. § 2711(b) (2000).

88. *See Hearings*, *supra* note 1, at 49-91 (statement of James X. Dempsey). Dempsey stated in his testimony: "The bill merely requires employers to tell their employees in advance what types of monitoring they will be subject to. Yet this alone will go a long way to restoring to workers their sense of dignity, which is a large part of the concept of privacy." *Id.* at 56.

Part A examines the specific provisions of the Act that were proposed and shelved in 2000. Part B examines some of the criticisms of NEMA from both employer and employee groups, and then addresses potential answers to these criticisms. The next section discusses why NEMA is a good idea, notwithstanding the criticisms.

A. Provisions

NEMA would create a new § 2711 in Title 18 of the United States Code.[89] Section 2711(a)(1) reads:

> Except as provided in subsection (c), an employer who intentionally, by any electronic means, reads, listens to, or otherwise monitors any wire communication, oral communication, or electronic communication of an employee of the employer, or otherwise monitors the computer usage of an employee of the employer, without first having provided the employee notice meeting the requirements of subsection (b) shall be liable to the employee for relief as provided in subsection (d).[90]

NEMA's language does not prohibit monitoring, but merely requires an employer to give notice before electronic monitoring occurs. The language also does not require notice before each instance of monitoring.[91] Instead, the employer must give notice when an employee begins working and must continue to give notice once a year after that.[92]

NEMA then requires an employer to provide annual notice of electronic monitoring.[93] Thus, an employer is required to give notice when an employee is hired, based on § 2711(a)(1), and annually thereafter.[94] NEMA further requires an employer to give notice of a "material change" in an electronic monitoring practice that falls within § 2711(a)(1).[95]

While § 2711(a) requires an employer to give notice, § 2711(b) defines the notice an employer is required to give an employee under NEMA. The Act begins by requiring the notice to be "clear and conspicuous" and given "in a manner reasonably calculated to provide actual notice."[96] Yet it does not require the employer to give notice in a certain manner, such as in writing. As one expert testified: "Arguably, even verbal notification of a company's monitoring practices passes muster

89. H.R. 4908 § 2711.
90. *Id.* § 2711(a)(1).
91. *See id.*
92. H.R. 4908, 106th Cong., § 2711(a)(2) (2000).
93. *Id*.
94. *See Hearings*, *supra* note 1, at 56 (statement of James X. Dempsey).
95. H.R. 4908 § 2711(a)(3).
96. *Id*. § 2711(b).

under the Act, provided that such notice encapsulates the remaining requirements of section (3)(b)."[97]

NEMA then states that the notice must describe five things. First, the notice must describe what form of communication or computer usage is to be monitored.[98] Second, it must state how such monitoring will be accomplished.[99] Third, it must describe the kinds of information that will be obtained, and "whether communications or computer usage not related to the employer's business are likely to be monitored . . . ."[100] Fourth, the notice must describe how often monitoring will take place.[101] Fifth, it must state how the information gathered by monitoring will be used.[102]

Section 2711(c) sets forth an exception to the notice requirement of 2711(a). It allows an employer to conduct electronic monitoring without notice if he has reasonable grounds to believe that: (1) an employee is engaged in conduct that "violates the legal rights of the employer or another person;"[103] (2) the conduct "involves significant harm to the employer or such other person;"[104] and (3) the monitoring may "produce evidence of such conduct."[105]

Finally, § 2711(d) sets forth the conditions for bringing a civil action under NEMA. In a claim under the Act, a court may award punitive damages, attorney's fees, and other equitable relief it determines appropriate.[106] However, NEMA caps the amount of damages that can be leveled against an employer at $500,000.[107] This means that if the employer had engaged in an act violating NEMA, and the act had involved many employees, damages could still only be assessed at an amount at or below $500,000.[108] NEMA sets the statute of limitations for an action under its provisions at two years.[109]

97. *See Hearings*, *supra* note 1, at 94 (statement of Kenneth Segarnick). The expert goes on to state: "[V]erbal notification of monitoring is undesirable, as it is subject to varying interpretations and it cannot be reproduced in the event a dispute arises between employer and employee." *Id.*

98. H.R. 4908 § 2711(b)(1).

99. *Id*. § 2711(b)(2).

100. *Id*.

101. *Id*. § 2711(b)(3).

102. *Id*. § 2711(b)(4).

103. H.R. 4908, 106th Cong., § 2711(c)(1)(A) (2000).

104. *Id*. § 2711(c)(1)(B).

105. *Id*. § 2711(c)(2).

106. *Id*. § 2711(d)(2).

107. *Id*. § 2711(d)(3)(B). The act also caps the award for damages against an employee violating its provisions at $20,000. *Id*. § 2711(d)(3)(A).

108. *See Hearings*, *supra* note 1, at 56-57 (statement of James X. Dempsey).

109. H.R. 4908, 106th Cong., § 2711(d)(4) (2000).

B. Criticisms

Since workplace privacy is a touchy subject for employers and employees alike, it is not surprising that both groups have criticized NEMA on several grounds. In fact, pressure from business and employer groups apparently led the Judiciary Committee to table the bill based on employers' fears of more litigation.[110] Groups advocating employee privacy were generally sympathetic to the bill, but they also had several criticisms, which are listed below.

As explained above, the current state of the law regarding the monitoring of workplace e-mail is unclear. If employers and employees can agree on the implementation of a bright-line rule on this matter, it would reduce potential harmful conflict in the future between the parties. This is the beauty of a notice requirement—it allows for a compromise between employee and employer interests, while setting a fairly clear standard for both parties to follow. For such a rule to be accepted, however, one must deal with the potential criticisms of such a standard.

1. A Notice Requirement Does Not Go Far Enough

In his statement before the House Subcommittee on the Constitution, Marc Rotenberg of the Electronic Privacy Information Center outlined a potential criticism of the notice requirement:

> A notice-only privacy law, absent any of the substantive rights associated with Fair Information Practices, such as access, correction, or use limitation, is problematic. It could in practice reduce the amount of covert surveillance, but it will not limit overt surveillance. It may in fact increase the amount of overt surveillance, as companies under directions from their attorneys, write very broad policies outlining a wide range of possible surveillance activities that may not have previously occurred.[111]

Rotenberg then stated that such a standard would impact employee privacy by undermining an employee's claims under state common law "because employees would be effectively on notice of monitoring practices."[112]

As such, critics argue that a notice requirement may lead to more "snooping" by employers because it provides a legitimate means for monitoring. Since the notice requirement encourages monitoring, employees will have more personal information examined and possibly disclosed. There will be no room for privacy in the workplace.

110. *See Hearings*, *supra* note 1.

111. *Hearings*, *supra* note 1, at 69-70 (statement of Marc Rotenberg).

112. *Id*. at 70.

This is a particularly sensitive argument because in today's culture, the workplace and personal life have become increasingly intertwined. The Internet provides a quick link from the workplace to the home, and vice versa. Many people take care of personal business on company time and, for the most part, many employers do not mind this behavior as long as it is within reason. Because more personal matters are being attended to at work, the presence of electronic monitoring will be seen as a more personal affront to privacy.

Yet this commingling of personal and work lives is why a notice requirement may be beneficial. NEMA's purpose is to put employees on notice that electronic monitoring will take place, in order to deter employee abuse of Internet and e-mail. A notice requirement is beneficial because it helps employees separate personal material from work-related material; employees are warned about what will be monitored, and thus can plan accordingly what can be used for personal use. With notice, employees can make informed decisions about what private information to bring to the workplace and what to leave at home. Therefore, privacy interests are helped.

A notice requirement may also deter employers from engaging in extremely intrusive monitoring.[113] If an employer must inform its employees about what type of monitoring will be used, employers may be more likely to refrain from more personal forms of surveillance, lest they lose employees. Thus, privacy is protected to a certain extent by the notice requirement.

Finally, this argument does not consider employer interests. One does not have the same expectation of privacy in the workplace as in the home. The fact that an employee is using an employer-supplied computer and e-mail account tends to shrink an employee's expectation of privacy. Employers need to be given the chance to regulate the use of their equipment through some electronic monitoring in order to deter employees' abuse of that equipment, just as employers have traditionally supervised employees to deter other forms of abuse.[114]

It is true that a notice requirement will probably not lead to less electronic monitoring. This does not mean, however, that employee privacy will not be aided enough by such a requirement. Given notice, employees may make informed decisions about whether intimate personal matters should ever be introduced into the workplace. A notice requirement may deter employers from engaging in severely intrusive forms of monitoring,

113. *See id.* at 49-91 (statement of James X. Dempsey).

114. One example is abusing company time by napping during one's shift.

thus aiding privacy interests. Finally, the notice requirement accurately reflects the fact that the workplace is not as private as the home.

2. A Notice Requirement Impedes Employer Interests

As stated above, employer groups also had several criticisms of NEMA's notice requirement. They feared NEMA's notice provisions could lead to more litigation for several reasons. First, the groups feared that the bill did not adequately address what type of notice was required.[115] Also, by having to give notice of the frequency of observations, the bill may lead to a heightened duty of care for the employers.[116] Finally, there is the potential argument that an employer should not have to give notice before engaging in monitoring.

The first criticism is that NEMA does not require a certain method of giving notice to employees.[117] Instead, it requires "clear and conspicuous notice" given "in a manner reasonably calculated to provide actual notice."[118] The bill does not define "clear and conspicuous." The fear is that the employer may give the employee some type of notice that is not clear and conspicuous, allowing an employee to sue on the basis that he was not given adequate notice under the statute.

One suggested solution is to require written notice or a "click-wrap agreement" where the notice appears on the employee's computer.[119] These methods would be desirable, as having such a requirement would be of minimal inconvenience to employers and would force them to be more up front in their dealings with employees. But this concern should not scuttle the whole bill. Given the nature of the law, most employers would probably prefer to set out notice in writing, anyway, so they would not have to prove in court that they made an oral statement to avoid liability under NEMA.

The second criticism is that requiring an employer to provide notice would raise the duty of care owed to its employees. In other words, employees might be able to sue their employer based on its failure to monitor transmissions at the level described in its notice.[120] For example, if an employee sends harassing e-mails to another employee, the harassed employee could argue that the employer should have caught the harassing

115. *Hearings*, *supra* note 1, at 90 (statement of Kenneth Segarnick).

116. *Id*.

117. *See* H.R. 4908, 106th Cong., § 2711(b) (2000).

118. *Id*.

119. *Hearings*, *supra* note 1, at 94 (statement of Kenneth Segarnick).

120. David McGuire, *Advocates Decry Business Opposition to Privacy Bill*, NEWSBYTES, Sep. 18, 2000, *at* http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=155364.

employee by monitoring his messages.[121]

While a valid point, this concern should not spoil the notice requirement. The only employers who will face problems under this line of reasoning are those who fail to meet the standard they set forth in their own notice. The purpose of this law is to make employers give information up front to their employees. Therefore, if an employer promises to monitor e-mail, that promise should be kept. If an employer lives up to its promise, then its duty of care is met. In cases where an employer cannot afford to meet this duty of care, it can give notice to its employees under § 2711(a)(3) that a "material change" will be implemented in the monitoring practice.[122] Alternatively, the employer can refrain from monitoring in the first place.

The third criticism is that a notice requirement would impose too great a burden on employers engaging in the legal practice of monitoring. This concern evidently led to the tabling of the bill.[123] However, as stated by Ari Schwartz of the Center for Democracy and Technology: "If a company is engaged in monitoring, they [sic] should be able to explain how they [sic] do it."[124] If a company has the resources to engage in employee monitoring, it should have the resources to issue notices to each employee.

A positive dimension of NEMA is its solid compromise between employer and employee interests. While each side may be dissatisfied with certain provisions of the bill, NEMA meets both groups in the middle. Employers are allowed to monitor, and employees are shown respect by being informed of monitoring practices. The fact that the introduction of the bill received bipartisan praise and support seems to indicate broad appeal, despite some of the criticisms expressed.[125] The compromise shown in the bill is an advantage. The next section will address some additional advantages that a bill like NEMA provides.

IV. WHY THE CURRENT BILL IS SATISFACTORY

In addition to being a good compromise, the bill is useful for several other reasons. First, there is a need for a monitoring policy, and the bill adequately serves this purpose. Second, giving notice is necessary and will improve employer-employee relations. Finally, the bill allows employers to protect their interests by monitoring employees.

121. *Id.*
122. H.R. 4908 § 2711(a)(3).
123. *See* Moad, *supra* note 4.
124. McGuire, *supra* note 120.
125. *Id.*

A. A Policy is Needed

As the above discussion indicates, the law concerning workplace monitoring of e-mail is unsettled. For the most part, employees have been unsuccessful in their actions against employers. This does not mean, however, that courts will continue to rule for the employer. As stated by one commentator:

> Because of E-mail's relatively short existence, the law concerning how much latitude an employer has in monitoring the use of its company E-mail system remains somewhat unresolved. While future statutory action may remove some of the legal ambiguity, until that time, an employer, unlike the proverbial ostrich, cannot stick its head in the sand and ignore the liability issue.[126]

Because e-mail is a new phenomenon that is being used more and more each day, it makes sense that courts will start to understand that many people see their e-mail as private. Therefore, employers should not take comfort in the ambiguity. An act like NEMA sets forth certain expectations from the employer, which takes away some of the ambiguity. While an employer might be expected to do more, by having to give notice before monitoring, the bill potentially shields from liability employers who follow its provisions.[127] This bill simply forces employers to do something that is good practice anyway and could save them from paying damages arising from a privacy claim.

B. Notice Should Be Given to Employees

In addition to creating a rule just for the sake of having a rule, there are other advantages that favor the passage of a bill like NEMA. A rule addressing electronic monitoring should have a notice requirement for several reasons. First, notice should be given to employees because it is simply the right thing to do. Second, a notice requirement is a simple and cheap solution to this problem. Third, a notice requirement will deter employees from engaging in activity that could be harmful or offensive to others, such as sexual harassment through e-mail. Finally, a notice requirement will give employees needed information to decide if they wish to continue working for the employer. These advantages are discussed below.

First of all, giving employees notice is fair. Since employers cannot

126. White, *supra* note 44, at 1102.

127. Whether the bill preempts state law is unknown. *See Hearings*, *supra* note 1, at 97 (statement of Michael Overly). Also unclear is whether one can maintain a cause of action under this bill along with some other cause of action. "In other words, can an employee maintain a cause of action against an employer under H.R. 4908 and a separate cause of action for damages for invasion of privacy?" *Id.*

reasonably expect employees in today's world to abstain from handling personal matters in the workplace, employees should at least be given warning that employers are watching. If employees desire absolute privacy, they will know that they will not be able to obtain it through their employers' computer systems.[128]

Notice is fair also because it supplies needed communication. As stated above, employers cannot expect employees to abstain from handling personal matters in the workplace. Notice provides the opportunity for employers to state what is acceptable and for employees to give employers feedback regarding what should be acceptable. Therefore, a reasonable policy can be established that will allow employees "to use the Internet for personal matters before or after normal work hours and/or during their lunch hours."[129] Moreover, notice can provide an opportunity for employers to make clear that "[u]se of the Internet in a manner that might create a hostile work environment on the basis of race, sex, age or other protected classifications should be expressly prohibited."[130]

Second, a notice requirement will not burden employers. In fact, most employers who engage in the practice of electronic monitoring do give notice.[131] This may be due to lawyers advising employers to give notice in order to fight off potential state invasion of privacy suits; as with notice, there is no reasonable expectation of privacy. Whatever the motivation, that such practices are developed at all shows that employers do not unduly suffer from having to give notice of electronic monitoring.

Third, a notice requirement will deter employees from engaging in activities that may lead to liability for the employer. Because employers can be held liable for their employees' actions, conduct such as sexual harassment through e-mail or the downloading of offensive pictures from the Internet can lead to legal trouble for employers. An employee who knows he is being monitored will probably not engage in such activity.

Finally, notice gives employees who highly value their privacy needed information to decide if they wish to continue working for the employer. Since NEMA requires an employer to give notice of electronic monitoring before engaging in the activity, the employee can use the notice to decide whether he wishes to continue working for the employer, or whether he should consider other employment.

128. *Id.* at 96.

129. Jeffrey S. Klein & Nicholas J. Pappas, *Monitoring Internet Use in the Workplace*, N.Y. L. J., Feb. 7, 2000, at 3.

130. *Id.*

131. *Hearings*, *supra* note 1, at 197 (statement of Lewis Maltby).

C. Employers Should Be Allowed To Monitor

Employers have several interests in monitoring employee e-mail. While some may argue that electronic monitoring will lead to workplaces akin to something out of George Orwell's *1984*, employers have always needed to supervise employees in one form or another. An employer-supplied e-mail account is nothing more than a tool, like a drill press in a machine shop or a calculator in an accounting firm. Ultimately, the account is the company's, not the employee's. The employer thus has an interest in seeing that the account is being used appropriately and not being abused. While many might find it harsh not to allow personal communication through company e-mail, there are certainly other alternatives. Services such as Hotmail, for example, supply anonymous e-mail accounts for free. Therefore, other avenues of communication exist for those who wish to engage in more risqué personal communications.

Employers also wish to avoid a hostile workplace. They themselves can be held liable when an employee improperly uses e-mail or the Internet and harm to another employee results. But, even if no suit is brought, someone who improperly uses e-mail or the Internet may nonetheless create a hostile work environment in which other workers might not function as well as they could. Imagine, for example, the embarrassment of an employee being harassed through e-mail and the profound effect the event would have on her work, perhaps even encouraging her to quit. A positive work environment equals a more productive work environment, and employers need to be given the chance to promote such an environment.

V. CONCLUSION

Can NEMA be changed to appease those who caused it to be tabled in the first place? The current bill represents a significant compromise by both sides in the debate. It is difficult to imagine a change to the bill that would satisfy both employers and employees. Notice is a simple solution that does not place much of a burden on employers, and there could not be a less strenuous requirement. Therefore, if Congress wishes to have a policy governing Internet privacy in the workplace, then this bill marks the best chance of passage.

The use of e-mail in the workplace has introduced an interesting legal debate about whether e-mail should be afforded privacy rights protecting it from employer monitoring. While many think minimal privacy rights should exist, it is doubtful that employers and employees will ever agree. NEMA proposes a simple yet effective solution to this quandary. Notice should be provided to employees before monitoring takes place, and notice

must be given every year thereafter. Employers and employees benefit alike from this rule. While this will not satisfy everyone, notice does, at the very least, provide a needed starting point in this debate.