2001 UCLA J.L. & Tech. 5

You've Got Mail... and Your Boss Knows It: Rethinking the Scope of the Employer E-mail Monitoring Exceptions to the Electronic Communications Privacy Act

by Benjamin F. Sidbury[1]

The reality is that in our 21st century society, people work long hours, and we all have come to accept that there will be a certain amount of personal business that will be done during business hours.[2]

I. Introduction

Myth: when you send or receive an e-mail while at your place of employment, you can prevent it from being monitored by merely deleting it. Reality: businesses routinely save e-mail on the network server and it is easily retrievable until purged from the system by a network administrator.[3] Myth: If you use an Internet-based personal e-mail account at your place of employment, your employer cannot monitor your e-mail because it does not route through the company's server. Reality: sophisticated e-mail surveillance software is capable of monitoring keystrokes and recording on-screen text and images.[4] Due to their mistaken reliance on these e-mail myths, many employees have been suspended and terminated.[5]

One plausible explanation for the trend in mass suspensions and firings is that employers are monitoring their employees' e-mail more frequently than in recent years. The fact that 73.5 percent of major U.S. corporations currently monitor employee e-mail – a considerable increase from the 14.9 percent reported in 1997 – tends to support this explanation.[6] As e-mail has become a regular means of communication in the

workplace,[7] courts have begun to recognize that employers may monitor their employees' work-based e-mail.[8] Although there are several causes of action available to an employee who is terminated or disciplined for improper use of work-based e-mail,[9] employees have been, and are likely to be, unsuccessful in defending their personal electronic privacy.[10]

The crucial piece of federal legislation that allows employers to monitor their employees' e-mail is the Electronic Communications Privacy Act of 1986 ("ECPA").[11] Although the ECPA prohibits a person or entity from intentionally intercepting an electronic communication or accessing a stored electronic communication, the Act provides a number of exceptions for employers.[12]

This article will examine the legal status of an employer's right to monitor an employee's e-mail, and it will argue that Congress should amend the ECPA to afford greater privacy protection to employees' personal use of e-mail in the workplace. Part II will trace the development of the ECPA and examine how courts have interpreted its provisions. Part III will examine why other laws do not offer an adequate alternative for addressing these concerns. Part IV will provide arguments why the current structure of the ECPA is inadequate and it will propose several solutions for Congress to consider in order to remedy the problems raised in this article.

II. The Electronic Communications Privacy Act

In 1986, Congress enacted the ECPA as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("OCCSSA").[13] The ECPA amended OCCSSA by expanding the scope of "unlawful electronic interceptions" to

include e-mail.[14] With respect to e-mail, the ECPA is divided into two relevant titles. Title II[15] of the ECPA, the Stored Communications Act, generally prohibits unauthorized access to stored e-mail and Title III[16] of the ECPA, the Federal Wiretap Act, generally prohibits the interception of e-mail.

A. Access to Stored E-mail

Title II of the ECPA prohibits a person or entity from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided."[17] In effect, this provision prohibits one from accessing e-mail from a stored database without authorization. It is significant to note, however, that this provision does not apply to the interception of e-mail en route between the sender and intended recipient.[18] It only applies to prevent an unauthorized user from accessing e-mail from a stored database, which by definition can only occur after transmission of the e-mail and after the e-mail has been received by the intended recipient.[19] For example, this provision covers read or sent e-mail, which is saved on the particular user's server or hard drive.

Title II contains two important exceptions: the "provider" exception[20] and the "user" exception.[21] Under the provider exception, the prohibition of Title II does not apply to "the person or entity providing a wire or electronic communications service."[22] This exception seems to suggest that an employer who provides an e-mail system to employees through a private company-based e-mail server (or an "in house" local area network) does not violate the "stored access" provision by monitoring employees' stored e-mails.[23] Some commentators argue, however, that this exception

does not apply to employers who merely provide a common carrier's e-mail service to employees.[24] For example, an employer who provides employees with access to e-mail through a commercial Internet service provider (such as America Online) would not likely fall under this exception. Conversely, with respect to an employer-provided private e-mail server, the exception seems to swallow the rule. Put differently, if an employer provides access to e-mail through a private in house e-mail server, the employer is free to monitor an employee's stored e-mail.

Under the user exception, the prohibition of Title II does not apply to access of stored e-mail "by a user of that service with respect to a communication of or intended for that user."[25] This exception exempts an authorized user from liability, as well as one who was expressly or impliedly given authorization to access the user's stored e-mail.[26]

As more and more corporations are providing their employees with e-mail access through a company provided e-mail server[27] (as opposed to a common carrier provided e-mail service), it appears that employers may monitor their employees' stored e-mail. It is significant to note that this Title does not impose any scope or content restrictions on the extent to which employers may monitor stored e-mail.

B. Interception of E-mail

Title III of the ECPA provides that no person or entity shall "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any … electronic communication."[28] The legislative history of this provision expressly indicates that e-mail is included in the definition of "electronic communication."[29] Title III also contains two important exceptions.

First, the consent exception provides that an employee may expressly or impliedly consent to interception of e-mail. One commentator notes that consent can be inferred either through an employment contract or through a well-disseminated e-mail policy.[30]

Second, the "ordinary course of business" exception provides that an employer may intercept an employee's e-mail in the ordinary course of business using equipment or facilities provided by the employer.[31] Although no court has confronted the issue of determining the precise scope of this exception in the context of e-mail, other cases have dealt with this exception in the context of telephone monitoring.[32] These cases have generally held that monitoring is permissible if the call is business related.[33]

Courts have consistently interpreted the "ordinary course of business" exception to mean that employers may only monitor communications "to the extent necessary to determine whether they are personal and not business related."[34] These cases seem to stand for the proposition that the interception and monitoring of personal communications does not fall within the ordinary course of business exception, and is, therefore, prohibited under Title III.[35] Although the above mentioned cases arose in the context of telephone monitoring, this rational will likely extend to e-mail in that an employer may only intercept e-mail if it is business related.

C. Shortcomings of the ECPA

Although the general prohibitions contained in the ECPA are clear, the exceptions are far from clear. The central problem lies in the distinction between monitoring stored e-mail and monitoring intercepted e-mail, as the classification yields

inconsistent results. Under Title III, the interception of e-mail provision, courts have consistently held that employers may only intercept and monitor communications if the employee is provided with notice.[36] Moreover, the notice requirement applies to the interception of both business-related and personal communications.[37] Conversely, Title II is silent with respect to whether notice is required as a prerequisite for an employer to monitor an employee's stored e-mail. Although the texts of both Title II and Title III are silent with respect to notice,[38] it is axiomatic that under Title III, notice has been judicially incorporated into the statute.[39] Nevertheless, the question remains whether an employer is required to provide notice to employees as an essential prerequisite to monitoring stored e-mail.

A second distinction between the interception of e-mail provision and the stored e-mail provision is the inconsistent application of the ordinary course of business exception. Under Title III, the interception provision, employers may only intercept a communication to the extent necessary to determine whether it is business related.[40]Once an employer determines that a communication is personal in nature, the employer may not continue to monitor the communication.[41] Under Title II, the stored communications provision, an employer may monitor any stored e-mail – personal or business related – regardless of whether the employer determines that the communication is personal in nature.[42] This distinction was magnified in Fraser v. Nationwide Mutual Insurance Co., which held that an employer does not violate the ECPA by monitoring an employee's (business or personal) e-mail "after transmission is complete."[43] The court further noted that "[t]he point in time when the message is acquired is the determining factor" for whether an employer may monitor an employee's

personal e-mail.[44] This distinction creates a puzzling dichotomy, as the extent to which an employer may monitor an employee's e-mail depends not on the nature of the e-mail, but on the state of the transmission. For example, suppose Employee A sends a personal (and non-business related) e-mail to Employee B. The employer may only intercept and monitor the e-mail in transition from A to B to determine whether it is personal or business related.[45] After the employer determines that the e-mail is personal, the employer may not continue to monitor the particular e-mail.[46]After the e-mail has been transmitted to B (and reaches B's "inbox"), however, the e-mail becomes "stored" under the statutory definition.[47] Because an employer may monitor all stored communications, the employer is free to monitor the particular e-mail regardless of whether it is personal in nature.[48] This example illustrates that the distinction between "intercepting" an e-mail and accessing a "stored" e-mail is trivial, as the state of transmission – potentially a matter of mere seconds – determines the extent to which an employer may monitor an employee's e-mail. Although the law seems rather clear that an employer may not monitor an employee's personal telephone communications, the question remains, however, whether and to what extent employers may monitor e-mail after they determine that the e-mail is clearly not business related.[49]

One further problem with the ECPA's application to e-mail lies in the very nature of e-mail. As previously noted, courts have only interpreted the "ordinary course of business" exception in the context of interception and monitoring of telephone calls.[50] The nature of e-mail, however, is inherently different from telephone calls for purposes of monitoring. For example, if an employer intercepts a telephone call and determines that it is personal in nature, the employer may not continue to monitor the

call.[51] Telephone conversations are "live" in the sense that after the employer determines that the call is personal in nature, the subsequent portion of the telephone conversation, which the employer may not monitor, has not yet taken place. Conversely, an e-mail is transmitted in its entirety, which means that even if an employer determines that the e-mail is personal in nature, the employer has already intercepted (and has access to) the entire e-mail. Therefore, because the nature of e-mail differs from the nature of telephone calls, they are not analogous for purposes of the ordinary course of business exception.

The above mentioned discrepancies illustrate that the ECPA possesses many lingering problems in its application to e-mail monitoring in the workplace. These problems raise two questions for consideration. First, do any other laws affecting e-mail monitoring in the workplace offer an adequate alternative to the problems identified above? Second, if other laws do not offer an adequate alternative, how can Congress amend the ECPA to effectively address the above mentioned problems?

III. Other Laws Affecting Employer E-Mail Monitoring

In addition to the ECPA, litigants have asserted other causes of action in situations involving employer monitoring of e-mail; these include constitutional law and tort law.

A. Constitutional Considerations

The Fourth Amendment of the U.S. Constitution prohibits the government from making unreasonable searches and seizures.[52] Courts have applied a two-part

"reasonable expectation of privacy" test to determine whether an individual's Fourth Amendment rights have been violated.[53] In order to prevail on a Fourth Amendment claim, a plaintiff must show that (1) the individual subjectively had an actual expectation of privacy, and (2) the expectation of privacy was one that society is willing to recognize as reasonable.[54] Although government employees might have an actual expectation of privacy in their e-mail, courts have been unwilling to hold that this expectation of privacy is one that society is willing to recognize as reasonable.[55] Furthermore, even if a court were to hold that society is willing to recognize that an employee's expectation of privacy in e-mail is reasonable, a Fourth Amendment cause of action is only available to government employees.[56] The Fourth Amendment is, therefore, inapplicable to employees in the private sector, and appears to be an unavailing cause of action for employees in the public sector.[57]

B. Tort Law

Because a Fourth Amendment cause of action is unavailable to private sector employees, some employees have asserted state law causes of action for invasion of privacy.[58] The particular claim, which falls under the umbrella of invasion of privacy, is an unreasonable intrusion upon seclusion of another.[59] Although the elements of this cause of action may vary between states, a plaintiff must generally show that (1) the conduct was highly offensive to a reasonable person, and (2) the plaintiff had a reasonable expectation of privacy.[60]

The first case to deal with an intrusion upon seclusion claim in the context of e-mail was Smyth v. Pillsbury Co.[61] In Smyth, an employee was terminated for violating

the company's e-mail policy despite the fact that the employer assured the employee it would not monitor or intercept the employee's e-mail.[62] The court held that the terminated employee had no reasonable expectation of privacy in e-mail, which was voluntarily transmitted to the employee's supervisor using the employer's e-mail system, despite the employer's assurances that it would not monitor or intercept employees' e-mail.[63] Furthermore, the court held that even if the employee had a reasonable expectation of privacy in his work-based e-mail, a reasonable person would not find the employer's interception and monitoring of the employee's e-mail "to be a substantial and highly offensive invasion of his privacy."[64] Smyth, which has been adopted by other jurisdictions,[65] stands for the proposition that an employee has no reasonable expectation of privacy in e-mail and an employer's monitoring of an employee's e-mail is not highly offensive to a reasonable person.[66] Some commentators suggest that even if a court were to hold that an employee has a reasonable expectation of privacy in e-mail and even if a court were to find that a reasonable person would find that e-mail monitoring is highly offensive, an employer could easily overcome these elements with a well-disseminated e-mail policy or employment contract.[67] Although an employee may assert a cause of action for an unreasonable intrusion upon the seclusion of another against an employer for e-mail monitoring, this cause of action appears to be unavailing.[68]

In sum, it appears that other laws affecting e-mail monitoring in the workplace do not provide an adequate alternative to the ECPA. Thus, to effectively remedy the problems inherent in the ECPA, Congress must amend the ECPA.

IV. Rethinking the Scope of the ECPA

The ECPA "has been noted for its "lack of clarity" and courts have struggled to interpret its provisions.[69] In order to cure the glaring loopholes and ambiguities identified above[70] and in order to advance this article's goal – to provide employees with greater privacy in the use of their personal e-mail – the ECPA must be amended in three substantive areas. First, Title II and Title III should be amended to expressly require that employers provide notice to employees before e-mail monitoring can occur. Second, Title II and Title III should be amended to incorporate the ordinary course of business exception, but should include an exception where the employer could monitor all e-mail – personal or business related – if the employer has a reasonable suspicion that illegal activity might occur. Finally, Title II and Title III should be amended to expressly prohibit employers from monitoring an employee's personal e-mail except in limited circumstances.

A. Notice

Title II, the stored communications provision, and Title III, the interception of communications provision, are silent with respect to notice.[71] In the context of telephone monitoring, however, courts have consistently imposed the requirement that the employer must provide the employee with notice before the employer may intercept and monitor the employee's telephone calls.[72] Although courts have only imposed this requirement under Title III, the interception provision, it does not necessarily follow that employers should not be required to provide notice before monitoring stored communications. Telephone calls are live and can only be monitored through

interception methods. In other words, the monitoring of telephone calls does not implicate Title II, the stored communications provision, because live telephone calls cannot be "stored" under the statutory definition.[73] In order to clarify this ambiguity, the ECPA should be amended to include a provision requiring employers to provide notice to employees before monitoring either stored communications under Title II or intercepting communications under Title III.[74] Although this amendment might seem burdensome to employers, the notice requirement could easily be satisfied through either a well-disseminated e-mail policy or an employment contract.[75] Moreover, this amendment might benefit employers in that after an employee receives notice, the particular employee would likely be discouraged from improper use of the company-based e-mail system.

B. Incorporating the Ordinary Course of Business Exception

Perhaps the most confounding feature of the ECPA is the statute's distinction between access to stored e-mail and the interception of e-mail.[76] Courts have consistently held that employers may intercept and monitor communications in the ordinary course of business; that is, employers may intercept and monitor communications to the extent necessary to determine whether they are business related.[77] Courts have made it equally clear, however, that the interception and monitoring of an employee's personal communications does not fall within the ordinary course of business exception, and is prohibited under Title III.[78] Conversely, an employer may monitor all stored e-mail – personal or business related.[79] As previously noted, the extent to which an employer may monitor an employee's e-mail depends not

on the nature of the e-mail, but on the state of the transmission.[80] This distinction caused great confusion and uncertainty in a recent case,[81] which suggests that Congress has produced an unworkable statutory framework for employer monitoring of e-mail.

Fraser v. Nationwide Mutual. Insurance. Co. illustrates the unworkable statutory framework of the ECPA in its application to employer monitoring of e-mail.[82] In Fraser, an employee was discharged for violating the company's e-mail policy, and the employee brought suit alleging that the employer violated both Title II and Title III of the ECPA.[83] The employer, Nationwide, acquired the particular e-mail by retrieving it from a database that contained "already received and discarded [e-mails] stored on the server."[84] Judge Brody went to great lengths to distinguish between access to stored e-mail and interception of e-mail.[85] The judge noted that Nationwide's retrieval of e-mail stored on the company's server was not an interception because interception can only occur "during the transfer, or during the course of transmission."[86] The judge failed to mention, however, that if the e-mail had been intercepted, Nationwide could only monitor it to the extent necessary to determine whether it was business related.[87] This suggests that because the ordinary course of business exception is a judicially created exception to employer monitoring of communications and has never been applied to e-mail, it is unclear whether courts will adopt this exception in the context of e-mail.[88] Moreover, as a matter of policy, litigants should not be required to rely on judicially created exceptions. Title III should be amended to codify the ordinary course of business exception, and provide that employers may only intercept and monitor e-mail to the extent necessary to determine whether it is business related. In other words,

this proposed amendment would allow employers to intercept and fully monitor an employee's business related e-mail.

Some commentators caution that restricting the extent to which an employer may monitor its employees' e-mail may lead to an increase in trade secret misappropriation.[89] This concern could be eliminated by adding a clause to the ECPA permitting an employer to intercept an employee's e-mail – business related or personal – if the employer has a reasonable suspicion that the employee might disclose trade secrets or engage in other illegal activities that might harm the business.[90] Codifying the ordinary course of business exception into Title III would, therefore, definitively clarify the extent to which an employer may intercept an employee's e-mail.

The more complex problem arises under Title II, the access to stored e-mail provision. A person or entity violates Title II by accessing, without authorization, a stored communication from "electronic storage."[91] In Fraser, the court held that the employer's act of accessing an e-mail "from storage after the e-mail had already been sent and received by the recipient" did not implicate Title II, the Stored Communications Act.[92] Although Title II expressly exempts the provider of the e-mail system from liability and although Nationwide was, in fact, the provider of the particular e-mail system (which should have ended the inquiry as to whether Nationwide was liable under Title II), the court ignored this exemption.[93] Instead, the court arbitrarily determined that an e-mail stored on the provider's server that is retrieved from "post-transmission storage" is not in "electronic storage" under Title II.[94] Not only is Judge Brody's interpretation of "electronic storage" absurd, but post-transmission storage of e-mail is exactly what Congress intended to be covered by the Stored Communications Act.[95] Although

Nationwide was the correct party to prevail, Nationwide should have prevailed merely because it was the e-mail system provider.[96] This case illustrates the ambiguities inherent in the ECPA, and indicates that the ECPA should be amended.

In addition to interpretational problems in Title II , the state of transmission loophole remains a prevalent concern. Under the current regime of Title II, an employer is free to monitor all stored e-mail, whether business related or personal.[97] There is no rational justification for why an employee should have greater privacy protection in the transmission of e-mail than in the storage of e-mail. In order to create uniformity between Title II and Title III, Title II should be amended to incorporate the ordinary course of business exception. This amendment would, in effect, allow employers to monitor stored e-mail only to the extent necessary to determine whether it is business related. Additionally, just as the above mentioned proposed amendment to Title III would permit employers to (1) intercept and fully monitor all business related communications and (2) monitor all communications – business related or personal – if the employer has a reasonable suspicion that illegal activity might occur, these exceptions would also extend to stored e-mail under Title II.

C. Prohibiting the Monitoring of Personal Communications

This article does not advocate for unlimited e-mail privileges in the workplace, but for privacy in personal communications. As previously noted, courts have consistently held that the interception and monitoring of personal communications does not fall within the ordinary course of business exception, and is, therefore, prohibited under Title III.[98] If the ordinary course of business exception were codified in Title II and Title

III, it follows that the monitoring of personal e-mail is not within the ordinary course of business and would be prohibited under the ECPA. Thus, Title II and Title III should be amended to expressly prohibit employers from monitoring personal communications.[99] Although the nature of e-mail makes this somewhat difficult to enforce, the statute would definitively clarify to courts and employers that personal e-mail may not be monitored.[100]

V. Conclusion

Because more employers are monitoring their employees' e-mail,[101] it seems inevitable that courts will be faced with the challenge of interpreting the ECPA under many different factual scenarios. Under the current framework of the ECPA, however, courts will likely continue to interpret its provisions erroneously.[102] In order to resolve the lingering effects of a poorly drafted statute and in order to provide employees with greater privacy in their personal communications, the ECPA should be amended to prohibit employers from monitoring employees' personal e-mail. Additionally, the proposed amendments would require employers to provide employees with notice before monitoring business-related e-mail.

The distinction between the interception of e-mail and access to stored e-mail is particularly problematic and unjustified, as the state of transmission of the e-mail affects the extent to which an employer may monitor the employee's e-mail.[103] Congress should reevaluate the justification for this distinction, and take appropriate action to remedy this glaring loophole.

Footnotes

1. J.D., magna cum laude, Syracuse University. The author wishes to thank Professor Lisa A. Dolak for her helpful comments and suggestions on earlier drafts of this article. The author is an associate in the intellectual property department at Alston & Bird, LLP in Charlotte, NC. The views expressed herein do not represent the firm or its clients. An earlier version of this article appeared in 5 J. of Internet L. 16 (July 2001).

2. Chris Oakes, 23 Fired for E-mail Violations, Wired News, Dec. 1, 1999, <http://www.wired.com/news/politics/0,1283,32820,00.html> (last visited Jan. 19, 2001) (statement of Barry Steinhardt, Associate Director of the American Civil Liberties Union).

3. Chris Oakes, Seven Deadly E-mail Thoughts, Wired News (August 4, 2000) <http://www.wired.com/news/business/0,1377,38007,00.html>(last visited Jan. 19, 2001).

4. See Andrew E. Serwer, Watching You Work, <http://abcnews.go.com/sections/business/DailyNews/serwer_talk_010222.html> (last visited Feb. 22, 2001) (discussing the many sophisticated e-mail monitoring technologies and how various e-mail monitoring software has been extremely popular with a wide range of companies).

5. See Jonathan Kay, Someone Will Watch Over Me: Think Your Office E-mails are Private? Think Again. What You Write, or Forward, Can Get You Fired – and Land Your Company in Court, National Post, Jan. 1, 2001, at 63. According to this article, Dow Chemical Company fired over 75 employees in 2000 for forwarding inappropriate or harassing "jokes" to coworkers. In November 1999, The New York Times fired 22 staff

members for sending and/or forwarding dirty jokes through the company e-mail server. And in December 2000, several Computer Associates employees were fired for e-mailing a sexually explicit joke around the office.

6. Serwer, supra note 4. The survey was conducted in 2000 by the American Management Association. See also H. Thomas Davis, The Law of LAN: Monitoring Employees' Electronic Communications – Monitoring of Employee E-mail is on the Rise, as are Concerns About Employees' Privacy Rights, Network Magazine, Feb. 1, 2001, at 50.

7. See generally Jay Weinstein, Social and Cultural Change: Social Science for A Dynamic World, 190-214 (1997) (discussing the increased use of technology in business communications).

8. See, e.g., Smyth v. Pillsbury Co., 914 F. Supp. 97, 100 (E.D. Pa. 1996); Bourke v. Nissan, Case No. B068705 (Cal. Ct. App. 1993) <http://www.loundy.com/CASES/Bourke_v_Nissan.html> (last visited Mar. 29, 2001).

9. See infra notes 53-69 and accompanying text.

10. See, e.g., Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

11. See 18 U.S.C. §§ 2510-2521 (1986); see also 18 U.S.C. §§ 2701-2711 (1994) (Video Privacy Protection Act of 1988).

12. Id.

13. See 18 U.S.C. §§ 2510-2520. Note that the Omnibus Crime Control and Safe Streets Act was enacted in part to prevent unlawful telephone wiretapping.

14. Id.; see also Kevin J. Baum, Comment, E-mail in the Workplace and the Right of Privacy, 42 Vill. L. Rev. 1011, 1025 (1997).

15. See 18 U.S.C. §§ 2701-2711 (1994). Title II, the Stored Communications Act, is short for the Stored Wire and Electronic Communications and Transactional Records Access Act. See Baum, supra note 14, at 1023.

16. See 18 U.S.C. §§ 2510-2521 (1986).

17. 18 U.S.C. § 2701 (1994).

18. Id.

19. See id.

20. See 18 U.S.C. § 2701(c)(1) (1994).

21. See 18 U.S.C. § 2701(c)(2) (1994).

22. Id. § 2701(c)(1).

23. See id; see also Larry O. Gantt, II, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 Harv. J.L. & Tech. 345, 359 (1995).

24. See Baum, supra note 14, at 1024; see also Gantt, supra note 23, at 360 nn.101-02 (providing examples of numerous common carriers of Internet-based e-mail, such as America Online, Compuserve, AT&T Mail, etc.). Other commentators suggest that this point is unclear, and judicial interpretation is necessary to clarify this ambiguity. See Paul E. Hash & Christina M. Ibrahim, E-mail, Electronic Monitoring, and Employee Privacy, 37 S. Tex. L. Rev. 893, 899 (1996).

25. 18 U.S.C. § 2701(c)(2) (1994).

26. See id; see also Baum, supra note 14, at 1025.

27. See, e.g., Kimbrelly Kegler, Note & Comment, Electronic Banking: Security, Privacy, and CRA Compliance, 2 N.C. Banking Inst. 426, 437, n.66 (1998).

28. 18 U.S.C. § 2511(1)(a) (1994).

29. S. Rep. No. 99-541, at 8 (1994).

30. Baum, supra note 14, at 1027.

31. 18 U.S.C. § 2510(5)(a) (1994); see also Amy Rogers, You Got Mail but Your Employer Does Too: Electronic Communication and Privacy in the 21st Century, 5 J. Tech. L. & Pol'y 1, 13 (2000) (hereinafter Rogers).

32. See, e.g., Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412, 417 (11th Cir. 1986).

33. See id.; see also Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that telephone calls may only be intercepted and monitored to determine whether the nature of the call is business related). Some courts have divided the ordinary course of business exception into two categories for purposes of determining whether monitoring is permissible: "legitimate business purpose" cases and "subject of the call" cases. See Thomas R. Greenberg, Comment, E-mail and Voice Mail, Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev. 219, 239 (1994); see also Baum, supra note 14, at 1026-27. Under the "legitimate business purpose" exception, an employer must demonstrate a legitimate business purpose for intercepting and monitoring the employee's communication. See Greenberg, supra note 33, at 239. To determine whether a legitimate business purpose exists, courts consider whether "(1) the employer had a reasonable business justification for the intrusion; (2) the employees were provided with notice of the possibility of monitoring; and (3) the employer acted consistently with respect to the extent of monitoring of which employees were warned." Id. at 239 n.104. Under the "subject of the call" exception, employers may intercept communications "relating to the business of the employer." Greenberg, supra note 33,

at 241; see also Baum, supra note 14, at 1027. Courts have held that if the employee is given notice, monitoring is permissible to ensure quality control and to reduce personal use. See James v. Newspaper Agency Corp., 591 F.2d 579, 581 (9th Cir. 1979) (holding that monitoring for purposes of quality control is permissible provided that the employee is given notice); Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 397 (W.D. Okla. 1978) (holding that an employer may monitor a telephone switchboard for purposes of determining whether an employee is using the switchboard for personal use provided that the employee is given notice); see also Baum, supra note 14, at 1026.

34. Baum, supra note 14, at 1027; see also Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that telephone calls may only be intercepted and monitored to determine whether the nature of the call is business related); Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412, 417 (11th Cir. 1986) (holding that monitoring work related calls is within the ordinary course of business if the employee is given notice); Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983) (holding that the monitoring of personal calls is not generally within the ordinary course of business).

35. See supra note 33.

36. See Deal v. Spears, 980 F.2d 1153, 1157-1158 (8th Cir. 1992) (requiring notice to monitor business communications); Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412, 417 (11th Cir. 1986) (requiring notice to monitor business communications); James v. Newspaper Agency Corp., 591 F.2d 579, 581 (9th Cir. 1979) (requiring notice to monitor for quality assurance purposes); Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 397 (W.D. Okla. 1978) (requiring notice to determine whether telephone

calls were personal); see also Greenberg, supra note 33, at 239 n.104.

37. See supra note 33 and accompanying text.

38. See 18 U.S.C. §§ 2510-2521 (1986); 18 U.S.C. §§ 2701-2711 (1994).

39. See supra notes 33-34 and accompanying text.

40. See supra notes 33-35 and accompanying text.

41. See supra notes 33-35 and accompanying text.

42. See supra notes 20-24 and accompanying text. Under the provider exception, an employer who provides employees with access to e-mail through a private server may monitor any stored communications.

43. Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633(E.D. Pa. 2001).

44. Id. at 634.

45. See supra notes 34-35 and accompanying text.

46. See id.; see also Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983).

47. See 18 U.S.C. § 2510(17) (defining storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and…any storage of such communication by an electronic communication service for purposes of backup protection of such communication").

48. Note further that the employer could also monitor the e-mail through A's "sent mail" folder, which also falls under the definition of stored mail. See supra note 47.

49. Although it would be beyond the scope of this article to examine the extent to which an employer may monitor an employee's voice-mail, a recent decision noted that voice-mail is analogous to e-mail for purposes of the ECPA. Fraser, 135 F. Supp. 2d at 635. An employer does not violate the ECPA by accessing an employee's voice-mail after

the voice-mail has been recorded into the employee's voice-mail box and after the employee retrieves the voice-mail. Id. But if the employer retrieves the voice-mail before the voice-mail has been heard by the intended recipient, the employer "intercepts" the voice-mail and may not monitor the voice-mail unless the nature of the voice-mail is business-related. Id.

50. See supra notes 32 and accompanying text.

51. Monitoring personal calls is not within the ordinary course of business. See supra notes 35 and accompanying text.

52. The Fourth Amendment of the U.S. Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

53. See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (noting that the determination of whether one's privacy interests are protected requires "an actual [subjective] expectation of privacy and, second, that the expectation be one that society is prepared to recognize as [objectively] reasonable"); see also California v. Ciralo, 476 U.S. 207, 211 (1986).

54. See id.

55. See Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) (holding that police officers had no reasonable expectation of privacy for e-mail messages sent through the city's computer system); see also Scott A. Sundstrom, 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 (1998). C.f. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (holding that even if the employee had an actual expectation of privacy in his e-mail, society is unwilling to recognize the expectation of privacy as reasonable); McLaren v. Microsoft Corp., 1999 WL 339015 (Tx. Ct. App. 1999) (holding that there is no reasonable expectation of privacy in workplace e-mail). The reasonable expectation of privacy inquiry raised in preceding two cases, however, arose in the context of the common law invasion of privacy tort claim.

56. See Burton v. Wilmington Parking Authority, 365 U.S. 715, 722 (1961) (holding that governmental intrusion is required to trigger the Constitution); see also Gilmore v. City of Montgomery, Ala., 417 U.S. 556 (1974) (holding that state action is required to trigger the Constitution).

57. See supra note 56 and accompanying text. Note, however, that the California state constitution extends Fourth Amendment guarantees to private employees. See Flanagan v. Epson Am., Inc., No. BC007036 (Cal. Jan. 4, 1991 (unreported)); Shoars v. Epson Am., Inc. (Cal. Ct. App. (unreported)), rev. denied, No. S040065, 1994 Cal. LEXIS 3670 (Cal. June 29, 1994)). Although this cause of action is available to private sector employees in California, both cases held for the employer and held that society is not willing to recognize the employees' expectation of privacy in their e-mail as reasonable. See id.; see also Jennifer C. Dombrow, Note, Electronic Communications and the Law: Help or Hindrance to Telecommuting?, 50 Fed. Comm. L.J. 685, 706-07 (1998).

58. See generally J. Dianne Brinson & Mark F. Radcliffe, Internet Law and Business Handbook, 376 (2000) (hereinafter Brinson & Radcliffe).

59. See Restatement (Second) of Torts § 652B.

60. Id.; see also Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); McLaren v. Microsoft Corp., 1999 WL 339015 (Tx. Ct. App. 1999).

61. 914 F. Supp. 97 (E.D. Pa. 1996).

62. Id. at 98.

63. Id. at 101.

64. Id.

65. See, e.g., McLaren v. Microsoft Corp., 1999 WL 339015 (Tx. Ct. App. 1999).

66. See supra notes 60-65 and accompanying text.

67. See Baum, supra note 14, at 1035; Brinson & Radcliffe, supra note 58, at 376. Note further that an e-mail policy would serve as notice for purposes of Title III of the ECPA. See supra notes 34-38 and accompanying text.

68. See supra notes 60-65 and accompanying text.

69. Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001) (citing Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994)); see also United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998), cert. denied, 525 U.S. 1071 (1999).

70. See supra notes 36-51 and accompanying text.

71. See 18 U.S.C. §§ 2510-2521 (1986); 18 U.S.C. §§ 2701-2711 (1994).

72. See Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (requiring consent of at least one party to intercept business communications); James v. Newspaper Agency Corp., 591 F.2d 579, 581 (9th Cir. 1979) (installation not done surreptitiously and with advance knowledge of both management employees for a legitimate business purpose

was not a violation of 18 U.S.C. 2510); Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 397 (W.D. Okla. 1978) (requiring notice to determine whether telephone calls were personal); see also Greenberg, supra note 33, at 239 n.104.

73. See supra note 47.

74. It is significant to note that the Senate Judiciary Committee recently debated the Notice of Electronic Monitoring bill, which would require employers to disclose monitoring practices to employees when they are hired and to update employees on these practices on an annual basis. See Brock N. Meeks, Banning Secret Workplace Snooping, available at http://www.msnbc.com/news/435656.asp (last visited July 8, 2001). The bill contained an exception, however, that would allow employers to monitor an employee's e-mail without providing the employee with notice if the employer has "a reasonable suspicion that illegal activity is taking place." Id. The bill was not adopted, however, because it contained a number of problems and ambiguities, particularly because the bill failed to define the form of notice that employers would be required to provide. See Witnesses Urge Fine-Tuning of Legislation Requiring Notice of Electronic Monitoring, 69 Bureau of Nat'l Aff. Legal News 9, at 2141 (Sept. 12 2000).

75. See Baum, supra note 14, at 1027.

76. See supra notes 40-49.

77. See supra notes 31-35 and accompanying text.

78. See supra note 33 and accompanying text.

79. See 18 U.S.C. § 2701 (1994).

80. See supra notes 40-49 and accompanying text.

81. See Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633 (noting the

ECPA's "lack of clarity"). (E.D. Pa. 2001).

82. See id.

83. Id. at 626.

84. Id. at 631.

85. See id. at 632-38.

86. Id. at 634.

87. See generally Fraser, 135 F. Supp. 2d 623.

88. See supra notes 31-35 and accompanying text.

89. See, e.g., Laurie Thomas Lee, Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop", 28 J. Marshall L. Rev. 139, 165-66 (1994); see also United States v. Carr, 805 F. Supp. 1266, 1272 (E.D.N.C. 1992).

90. Note that a similar clause appeared in the Notice of Electronic Monitoring bill, which allowed employers to monitor an employee's e-mail without notice if the employer has a reasonable suspicion that the employee might engage in illegal activity. See supra note 74.

91. 18 U.S.C. § 2701.

92. Fraser, 135 F. Supp. 2d at 636.

93. See 18 U.S.C. 2701(c) (providing that the "person or entity providing...the electronic communications service" is exempted from liability under Title II, the Stored Communications Act); see also Fraser, 135 F. Supp. 2d at 631.

94. Fraser, 135 F. Supp. 2d at 636 (emphasis added). This is perhaps the most perplexing part of the decision, as Judge Brody ignores conventional principles of statutory interpretation to reach her conclusion. The Stored Communications Act

defines "electronic storage" as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and…(b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication". 18 U.S.C. § 2510(17). Although the statutory definition of electronic storage is not disjunctive in that it uses "and" rather than "or," Judge Brody does not address this in her opinion. See id. Instead, Judge Brody asks whether post-transmission storage is either "temporary or intermediate storage" or storage for backup purposes. Fraser, 135 F. Supp. 2d at 636. Judge Brody determines that "temporary and intermediate storage" can only occur if the intended recipient has not yet viewed the e-mail, an interpretation that is not supported by case law or the legislative history of the ECPA. See id. She, therefore, holds that post-transmission storage is not a temporary or intermediate storage. Id. Next, Judge Brody concludes that the post-transmission storage of e-mail is not storage for backup purposes. Id. . This conclusion is not supported by law or logic. Many commentators assume (based on common sense) that the post-transmission storage of e-mail is for backup purposes. See LeEllen Coacher, Permitting Systems Protection Monitoring: When the Government Can Look and What it Can See, 46 Air Force L. Rev. 155, 173 (1999); Rogers, supra note 31, at 15. Moreover, the legislative history of the ECPA contradicts Judge Brody's conclusion; it appears that Congress intended post-transmission storage to fall within the purview of the Stored Communications Act. See H.R. Rep. No. 106-932 (2000).

95. See H.R. Rep. No. 106-932 (2000). Note further that under Judge Brody's interpretation of Title II, anyone without authorization, such as a hacker, would be free to access an e-mail from post-transmission storage, as this conduct would not fall under

the purview of the Stored Communications Act. This is clearly not what Congress intended. See id.

96. See 18 U.S.C. 2701(c).

97. See supra notes 40-49 and accompanying text.

98. See supra note 35 and accompanying text.

99. Note that this prohibition should incorporate by reference the reasonable suspicion exception identified above. See supra notes 89-90 and accompanying text. In other words, employers would be permitted to monitor employees' personal e-mail if the employer has a reasonable suspicion that illegal activity might occur.

100. As previously noted, the monitoring of e-mail and the monitoring of telephone calls are not analogous for purposes of the ordinary course of business exception. See supra notes 50-51 and accompanying text.

101. See supra note 6 and accompanying text.

102. See Fraser, 135 F. Supp. 2d 623.

103. See supra notes 40-49 and accompanying text.