YOU'VE GOT MAIL! (AND THE GOVERNMENT KNOWS IT): APPLYING THE FOURTH AMENDMENT TO WORKPLACE E-MAIL MONITORING

SCOTT A. SUNDSTROM*

Electronic mail (e-mail) is rapidly supplementing, and often replacing, traditional forms of personal and business communication.[1] As workplace e-mail becomes increasingly ubiquitous, a disturbing trend is emerging. An increasing number of employers are reading

* I would like to thank the following people: the members of the *New York University Law Review*, especially Lewis Bossing, for their tireless efforts in improving both the accuracy and clarity of this Note; Ty Alper, for being both a great friend and an inspiring mentor; and my wife, Claire Haws, who will always be ☺.

[1] Numerous surveys have noted the rapid rise of e-mail use in American society. See, e.g., Bill Gates, A Recap of 1997 Hits and Misses, Seattle Post-Intelligencer, Dec. 31, 1997, at C1 (predicting that "[m]ost corporations will employ electronic mail systems by the end of [1997], and employees will typically send or receive e-mail several times a day"); Patrick McKenna, Almost Ten Million People Made Internet Purchases, Newsbytes, Dec. 12, 1997, available in Westlaw, 1997 WL 15601823 (finding 59 million e-mail users over age 16 in North America, and finding 26% of total population using e-mail in some form); Patrice Duggan Samuels, Who's Reading Your E-Mail? Maybe the Boss, N.Y. Times, May 12, 1996, § 3, at 11 (citing 1996 study by Society for Human Resource Management finding that 80% of organizations in study used e-mail); Mark S. Dichter & Michael S. Burkhardt, Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age § I.A (visited Sept. 7, 1998) <http://www.mlb.com/speech1.htm> (citing Gallup Poll finding 90% of large businesses using e-mail and estimating that 40 million workers correspond via e-mail, with number increasing 20% per year). Several features of e-mail have fueled this growth: ease of use, affordability, rapid transmission, and the ability to distribute data widely with the touch of a button. See, e.g., Yochai Benkler, Rules of the Road for the Information Superhighway § 2.1[2] (1996) (describing how digital information can be transmitted over great distances in short periods of time, "significantly compressing time and space"); Lawrence Van Gelder, When E-Mail Strikes the Wrong Target, N.Y. Times, Oct. 5, 1997, § 3, at 8 (relating tale of young attorney who accidentally sent e-mail message intended only for girlfriend to over 1,000 people at his law firm by pressing wrong button); Hotmail—The World's FREE Web-Based Email (visited Oct. 2, 1998) <http://www.hotmail.com> (advertising free e-mail service). For a comprehensive history of the development of the Internet and e-mail, see Katie Hafner & Matthew Lyon, Where Wizards Stay Up Late (1996).

The Microsoft antitrust trial demonstrates just how important workplace e-mail has become. A recent New York Times article termed the litigation "the first major [e]-mail trial." Steve Lohr, Antitrust Case Is Highlighting Role of E-Mail, N.Y. Times, Nov. 2, 1998, at C1. E-mail "is alive with ideas" and allows people to "communicate more frankly and informally than when writing a letter or a report." Id. At Microsoft e-mail "has supplanted the telephone as the most common instrument of communication." Id. As a result, a senior Justice Department official stated that "[e]-mail has just revolutionized investigations of this kind." Id.

and censoring their employees' e-mail.[2] Workplace e-mail monitoring is increasing because this new form of communication is inherently susceptible to large-scale, systematic surveillance.[3]

---

[2] Although exact figures illustrating the scope of e-mail monitoring are hard to come by, estimates of the extent of employers who monitor range from 7.7% to a third or more. See, e.g., E-Mail Common in Workplace, But Usage Policies Lacking, Newsbytes, Feb. 12, 1996, available in Westlaw, 1996 WL 7907264 (discussing results of Society for Human Resource Management study stating that 7.7% of companies surveyed perform random employee e-mail reviews); Amitai Etzioni, Some Privacy, Please, for E-Mail, N.Y. Times, Nov. 23, 1997, at C12 (stating that "various surveys" agree that over one third of employers monitor employees, generally through e-mail spot checks). To be sure, employers offer a number of strong justifications for the practice, including fear of exposure to litigation, protection of trade secrets, prevention of sexual harassment, and the reduction of productivity-reducing personal and recreational uses of office computers. See, e.g., Strauss v. Microsoft Corp., No. 91 Civ. 5928, 1995 WL 326492, at *5 (S.D.N.Y. June 1, 1995) (holding that e-mail is discoverable); Star Publ'g Co. v. Burchell, 891 P.2d 899, 900-01 (Ariz. Ct. App. 1994) (compelling production of employee e-mail communication); Melvin F. Jager & William J. Cook, Trade Secrets and Industrial Espionage: Online Piracy, White-Collar Crime Rep., Jan. 1997, at 3, 6 (describing "widespread use of electronic media such as e-mail . . . for commercial espionage" and citing statistics and cases); David K. McGraw, Note, Sexual Harassment in Cyberspace: The Problem of Unwelcome E-Mail, 21 Rutgers Computer & Tech. L.J. 491, 491 (1995) (reporting instances of sexual harassment via e-mail); Parry Aftab, E-Mail & Discovery Considerations, Leader's Legal Tech Newsl. (N.Y. Law Publ'g Co., New York, N.Y.), May 1996, at 1 (noting difficulty of deleting e-mail and calling it "litigator's nightmare"); Amy Harmon, On Office PC, Bosses Opt for All Work, No Play, N.Y. Times, Sept. 22, 1997, at A1 (describing public and private employer crack down on personal uses of workplace computers).

[3] See, e.g., Benkler, supra note 1, § 19.1 (observing that "[t]he transmissibility and processibility of digital information join to allow employers to exercise more accurate, more complete, and more immediate control over the performance of their employees"); Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 76 (1994) (stating that "Americans' growing reliance on computers has vastly increased the potential for the government to use electronic surveillance to intrude into its citizens' private lives").

Employers monitor e-mail through sophisticated computer programs that automatically apply complex linguistic analyses to every single outgoing and incoming e-mail message in a workplace. One such program, called Assentor, uses a form of artificial intelligence to screen e-mail messages for indications of racist, religious, sexual, or threatening remarks. After automatically scanning e-mail for the presence of body part names and poor grammar, the program assigns each e-mail message an offensiveness score. Messages above a cut-off score are automatically sent for review by a human being. See, e.g., Assentor Fact Sheet (visited Sept. 7, 1998) <http://www.sra.com/industry_sectors/is_assentor.html> (describing features and benefits of Assentor); Thomas Hoffman, Brokers Can Monitor E-mail More Easily, Computerworld (July 20, 1998) <http://www.computerworld.com/home/print.nsf/all/9807205B0A> (reporting use of Assentor by several companies); Carl S. Kaplan, Big Brother as a Workplace Robot, CyberTimes—The N.Y. Times on the Web (July 24, 1997) <http://www.nytimes.com/library/cyber/law/072497law.html> (detailing features of Assentor). Other companies provide software that records an employee's every keystroke in every computer application he or she uses. See, e.g., Omniquad Desktop Surveillance (visited Sept. 26, 1998) <http://www.toolsthatwork.com/ods.htm> (advertising software that provides employers with video-like recording of users' computer activity); WinWhatWhere Investigator (visited Sept. 26, 1998) <http://www.winwhatwhere.com/in-

Several factors combine to make e-mail monitoring more problematic than older, more quantitative types of workplace monitoring.[4] E-mail monitoring has the potential to affect many more workers than older forms of workplace monitoring.[5] This is because e-mail monitoring does not require the physical presence of a supervisor and can be performed completely surreptitiously at any place and at any time a worker uses a networked computer.[6] Constant, secret intrusions by employers have severe impacts on monitored workers, including stress and stress-related illnesses.[7] E-mail monitoring thus not only implicates employees' interests in maintaining dignity and autonomy in the workplace,[8] but also raises issues concerning the effects of the disclosure of the intensely personal information e-mail messages can convey.[9]

Because federal, state, and municipal employers make up a very large sector of the American economy, government employees are, as a group, significantly affected by workplace e-mail monitoring.[10] Although access to e-mail varies greatly among agencies,[11] the federal government has established a goal of providing e-mail to every federal

---

vestigator/index.htm> (promoting "virtually undetectable" software that monitors and records all computer keyboard activity).

[4] These methods of monitoring include counting the number of keystrokes an employee makes per hour or the number of minutes employees spend on the phone. See, e.g., Benkler, supra note 1, § 19.1 (comparing e-mail monitoring to other forms of employee monitoring).

[5] See id. (stating that e-mail monitoring "potentially touches a much broader group of workers" than other forms of monitoring).

[6] See id. § 19.2[1] (noting that e-mail monitoring allows employers to monitor "everything that an employee does, continuously throughout the work day, and without the employee knowing when he or she is being monitored"); John Whalen, You're Not Paranoid: They Really *Are* Watching You, Wired, March 1995, at 76, 78 ("Whereas wary employers formerly hired platoons of human watchdogs, today a whole panoply of surveillance technology can handle the business of workplace monitoring at a fraction of the cost."); see also Winick, supra note 3 (describing capabilities of monitoring software).

[7] See, e.g., Whalen, supra note 6, at 81 (discussing results of studies reporting increases in stress and illnesses among monitored workers).

[8] See, e.g., Benkler, supra note 1, § 19.1 (arguing that e-mail monitoring raises concerns about "privacy and the ability to keep personal information confidential from one's employer").

[9] See, e.g., Paul F. Gerhart, Employee Privacy Rights in the United States, 17 Comp. Lab. L.J. 175, 176 (1995) (stating that "employees and employers have reached the threshold of a state that even George Orwell did not imagine").

[10] According to Bureau of Labor Statistics data there were over 19.8 million government employees in August 1998. Search of Bureau of Labor Statistics Data, Nonfarm Payroll Statistics from the Current Employment Statistics (National) (visited Sept. 10, 1998) <http://146.142.4.24/cgi-bin/surveymost?ee> (search for Government Employment—Seasonally Adjusted).

[11] See, e.g., Governmentwide Electronic Messaging Program Management Office (GEMPMO), E-Mail Survey Results and Analysis (visited Sept. 28, 1998) <http://www.fed.gov/hptext/emailpmo/emtf/EMTF5.html> (reporting survey results indicating that some

agency[12] and promoting e-mail as the preferred method of conducting government business.[13] In addition, the federal government has instituted an aggressive telecommuting program, which has encouraged extensive use of e-mail.[14] The military also is actively encouraging use of e-mail by service members[15]—and is engaging in a program of monitoring.[16] The government may even monitor the e-mail sent by children in their "workplaces"—public schools.[17]

Given the reality of government workplace e-mail monitoring, what protections do government employees have from the prying eyes of their employers? This Note examines one potential legal protection for these employees and others subject to e-mail monitoring: the Fourth Amendment's restrictions on unreasonable searches and seizures.[18] Although the Fourth Amendment only acts as a check on government actions,[19] the scope of the Amendment's protections for

---

agencies do not have e-mail networks while others provide e-mail access to over 50% of employees).

12 See GEMPMO, Recommendations (visited Sept. 28, 1998) <http://www.fed.gov/hptext/emailpmo/emtf/EMTF8.html> (stating that "the time has come for all Federal agencies to take positive action to implement governmentwide e-mail connectivity").

13 See GEMPMO, E-Mail PMO Two-Year Plan, § 4.0 (visited Sept. 28, 1998) <http://www.fed.gov/hptext/emailpmo/4.html> (recommending that Office of Management and Budget "should promote the immediate use of e-mail as the preferred medium for the conduct of government business").

14 See, e.g., Mike Causey, Telecommuting Today, Wash. Post, July 8, 1997, at B2 (citing General Accounting Office report estimating 9,000 federal workers telecommuting in mid-1997 and predicting that number should grow to 90,000 by end of fiscal 1998).

15 See, e.g., H.G. Reza, The Few, the Proud, the Online, L.A. Times (Orange County ed.), Dec. 25, 1997, at E1, available in LEXIS, News Library, LAT File (quoting Marine spokesman stating intent of military to exploit Internet as much as possible).

16 See id. (stating that e-mail messages are checked randomly for security reasons).

17 The chairman of the Texas Board of Education, Dr. Jack Christie, recently proposed replacing all textbooks with laptop computers for the state's 3.7 million students. See, e.g., Texas May Drop All Texts, for Laptops, N.Y. Times, Nov. 19, 1997, at B11. Dr. Christie also hinted that such computers would have Internet connectivity, which could make monitoring students' e-mail very tempting. See, e.g., Interview with Jack Christie, All Things Considered (NPR radio broadcast, Nov. 24, 1997), available in Westlaw, 1997 WL 12834462 ("And then all of the sudden, you have a modem card and you can tie into the Internet.").

18 The Fourth Amendment states:

> 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.

19 The protections of the Fourth Amendment, like those of other constitutional rights, only apply where actions are taken by governments, not private actors. See, e.g., Flagg Bros., Inc. v. Brooks, 436 U.S. 149, 156 (1978) (stating that most constitutional rights "are protected only against infringement by governments"); Jackson v. Metropolitan Edison Co., 419 U.S. 345, 349 (1974) (describing "essential dichotomy" between deprivations of

government workers' e-mail has widespread ramifications for other classes of workers. The influence of Fourth Amendment jurisprudence on common law tort actions, state constitutional law, and judicial interpretation of state privacy statutes means that all workers could benefit from the successful Fourth Amendment claims of government employees.[20]

Whether, and to what extent, the Fourth Amendment might limit e-mail monitoring in government workplaces is an open question. Currently there is no caselaw directly on point.[21] This Note argues that the Fourth Amendment should limit the government's ability to monitor the e-mail of its employees. Part I reviews basic Fourth Amendment principles and then briefly examines alternate sources of privacy protections. That Part will show that these legal remedies are inadequate to protect government employees from intrusive e-mail monitoring in the workplace. Part II of this Note argues that the Fourth Amendment, which has been held to protect individuals from a variety of unreasonable government intrusions, could also apply to searches and seizures of e-mail in general, and workplace e-mail in particular. Part III then proposes an appropriate Fourth Amendment standard for government workplace e-mail monitoring. Beginning with the Supreme Court decision in *O'Connor v. Ortega*,[22] Part III applies the federal case law involving workplace searches of government employees to the specific context of e-mail monitoring. This Note concludes that workplace e-mail monitoring is unreasonable where there is no special need justifying the types of suspicionless searches monitoring represents. Absent a special need, individualized suspicion should be necessary in order to justify monitoring employees' e-mail.

---

rights by state action and private conduct). As a result, this Note will focus on monitoring of *government* employee e-mail. All further references to employees and employers are to government employees and employers, unless clearly identified otherwise.

20 The ways in which federal courts interpret the Fourth Amendment have far-reaching implications for most other areas of privacy protection. See, e.g., Larry O. Natt Gantt, II, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 Harv. J.L. & Tech. 345, 380 (1995) (arguing that "although the Fourth Amendment does not protect private employees against privacy invasions by their employers, cases from the Fourth Amendment context are critical to discussing" how other sources of privacy protection apply to employees); see also infra Parts I.B.2, I.B.3.

21 A Westlaw search for Fourth Amendment cases involving e-mail yielded no reported decisions applying the Fourth Amendment to monitoring of government employees' e-mail. Such cases may have been filed and settled, however. See, e.g., Jim Simon, Computer Privacy at Issue in Suit, Seattle Times, Sept. 17, 1990, at D1 (describing suit by Washington State employee alleging illegal retrieval and copying of e-mail without reporting judicial decision).

22 480 U.S. 709 (1987).

I

THE PRIMACY OF THE FOURTH AMENDMENT: SHORTCOMINGS OF ALTERNATIVE SOURCES OF PRIVACY PROTECTION

A necessary precursor to finding Fourth Amendment limitations on e-mail monitoring by public employers is finding that the Fourth Amendment applies to e-mail monitoring at all. This Part begins with a brief discussion of general Fourth Amendment principles, using *Katz v. United States*[23] as an introduction to the ways courts and commentators have applied the Fourth Amendment's requirement of a "reasonable expectation of privacy" to searches and seizures of e-mail and related technologies.

The Fourth Amendment is not the only potential source of law that could operate to limit the scope of employer e-mail monitoring. Therefore, this Part also discusses three alternative sources of protection against workplace e-mail monitoring: the federal Electronic Communications Privacy Act, common law tort remedies, and state constitutional and statutory law.[24]

Whether public employees may depend upon these other protections from e-mail monitoring remains uncertain at best. Even if these sources do provide protections, the extent of those protections may well depend on the way in which courts construe the Fourth Amendment in this context. Because these alternative sources of privacy protection are currently largely inadequate, the Fourth Amendment takes on increased importance as a potential shield against government employee e-mail monitoring.

---

[23] 389 U.S. 347 (1967).

[24] The First Amendment may also provide a measure of protection to government employees. See, e.g., Pickering v. Board of Educ., 391 U.S. 563, 574 (1967) (holding that "absent proof of false statements knowingly or recklessly made by him, a teacher's exercise of his right to speak on issues of public importance may not furnish the basis for his dismissal from public employment" (citation omitted)).

An analysis of First Amendment jurisprudence is outside the scope of this Note, which focuses on Fourth Amendment privacy caselaw, a somewhat different approach to protecting government employee speech. Most often, government employees could only object to e-mail monitoring on First Amendment grounds if their employer took some retaliatory action based on the content of their e-mail messages. The Fourth Amendment, by contrast, limits the practice of monitoring itself because the act of monitoring violates employees' interests in maintaining personal privacy. Of course, one might argue that the First Amendment also limits the act of e-mail monitoring because monitoring chills speech. See, e.g., Laird v. Tatum, 408 U.S. 1, 11 (1972) ("[C]onstitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights."). For a discussion of the First Amendment and e-mail monitoring, see George B. Trubow, Constitution vs. Cyberspace: Has the First Amendment Met Its Match?, Bus. L. Today, Mar.-Apr. 1996, at 41.

A. *The Threshold Question:* Katz v. United States

Not all searches and seizures implicate the Fourth Amendment; a person must have a reasonable expectation of privacy in the subject of the search or seizure to invoke the Constitution's protections. The Supreme Court developed the "reasonable expectation of privacy" test in the seminal case of *Katz v. United States*.[25]

In *Katz*, government investigators listened to and recorded telephone calls made from a public phone booth.[26] The Court held that the Fourth Amendment was implicated when government agents tapped telephone conversations made by the defendant from a public phone.[27] In so doing, the Court rejected previous Fourth Amendment jurisprudence, which was based on trespass or "physical penetrations," and held that "the Fourth Amendment protects people, not places."[28] The Court recognized that some searches of private areas—such as the home—fell outside the Fourth Amendment, while searches that took place in public areas could implicate the Amendment.[29]

As articulated in Justice Harlan's concurrence in *Katz*, which has since been explicitly adopted by the Court,[30] the "reasonable expectation of privacy" test has two parts: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[31] Justice Harlan's test expands the scope of the Fourth Amendment to include searches that do not involve any physical trespass.[32]

---

25 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

26 See id. at 348.

27 See id. at 353 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

28 Id. at 350, 351. *Katz* overruled an earlier case, Olmstead v. United States, 277 U.S. 438 (1928), in which the Court held that a physical penetration or trespass was necessary in order to invoke the Fourth Amendment. See id. at 466; see also *Katz*, 389 U.S. at 353 ("We conclude that the underpinnings of *Olmstead* . . . can no longer be regarded as controlling.").

29 See id. at 351-52 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . [W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

30 The Harlan concurrence is the standard test in evaluating Fourth Amendment claims. See, e.g., Smith v. Maryland, 442 U.S. 735, 740-41 (1979) (adopting Harlan's two-part inquiry and citing cases).

31 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

32 See id. at 353 ("[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear

The answers to these threshold questions determine whether a particular search or seizure in a particular case is covered by the restrictions of the Fourth Amendment at all. If there is no reasonable expectation of privacy, the Fourth Amendment does not apply and the government may search and seize without a warrant, probable cause, or any of the safeguards established by the Amendment. If there is a reasonable expectation of privacy, then courts proceed to look at the reasonableness of a particular search or seizure within a particular context. Questions about reasonableness need only be asked if the Fourth Amendment applies.

B. Analyzing Alternative Sources of Privacy Protection

Although no courts have applied the *Katz* test to find that the Fourth Amendment protects employees from government workplace e-mail monitoring, litigants have argued for similar legal protections through both statutory and common law claims. Commentators have also noted that state constitutions may provide e-mail users with some protection. This section assesses the strength of those claims.

1. The Electronic Communications Privacy Act

The only federal statute that arguably applies to e-mail monitoring by employers (government or otherwise) is the Electronic Communications Privacy Act of 1986 (ECPA).[33] The ECPA includes two main categories of protection: Title I prohibits interception of messages in transit,[34] while Title II prohibits access to and disclosure of stored information.[35] Taken together, the provisions of the ECPA prohibit three types of intrusions into electronic communications: intercepting messages while they are in transit, accessing stored information, and disclosing information at any point in the process.[36]

While the ECPA may seem to provide all employees, including government employees, protection from e-mail monitoring, the Act contains several loopholes sharply limiting its usefulness to employees. First, the ECPA was not intended to govern the relations of em-

---

that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

33 Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). The ECPA was enacted to amend and update the federal antiwiretapping statute. See 18 U.S.C. §§ 2510-2520 (1994).

34 See 18 U.S.C. §§ 1367, 2521, 3117, 3121-3127 (1994).

35 See id. §§ 2701-2711.

36 See, e.g., Benkler, supra note 1, § 20.3[1] (discussing effects of ECPA's passage).

ployees to their employers,[37] but rather appears intended to regulate only those intrusions by unauthorized outsiders into the electronic communications of organizations. Some commentators believe that the ECPA simply does not cover workplace local area networks (LANs)[38] and thus provides no protection for employees when they send e-mail over their workplace computer network.[39] The language in the ECPA prohibiting *disclosure* of electronic communications only applies to those entities that provide electronic communication services "to the public."[40] Intra-office networks offer services only to employees, not the public. Thus, under this construction of the ECPA, any e-mail sent by government employees over a nonpublic network would not be subject to the Act.

Second, even if the ECPA did apply to proprietary LANs, the Act contains an exemption allowing access to stored communications when authorized by the entity providing electronic communications services.[41] On its face, this provision would allow the network provider to access *any* stored communication that had been sent over the network without violating the ECPA. If an employer owns the network, it could then access all communications sent by employees. A literal interpretation of section 2701(c)(1) may run counter to the spirit of the rest of the ECPA, however. Some argue that this subsec-

---

[37] See id. ("The ECPA is by no stretch of the imagination an employment law statute."); see also Gerhart, supra note 9, at 199 ("The ECPA was aimed at the general public . . . and does not focus on employers.").

[38] A network is a series of computers linked together which can share information with one another. A local area network usually consists solely of computers located in one building. A wide area network (WAN) is comprised of two or more LANs, in different locations, linked together to create a larger network of computers. A large corporation with offices in different cities may have a LAN within each office and a WAN tying all its offices together, allowing an employee in Des Moines to access corporate information on computers located in Miami. The Internet, by comparison, is a world-wide network of computers, a network of networks. See generally Henry H. Perritt, Jr., What is the Internet?, in What Lawyers Need to Know About the Internet 13 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. G-443, 1996) [hereinafter What Lawyers Need to Know].

[39] See, e.g., Michael D. Scott et al., Scott on Multimedia Law § 12.04[A] (2d ed. Supp. 1997) (asserting that ECPA "would not apply to corporate or other 'non-public' computer networks. . . . [A] company's review of e-mail transmitted through or stored on its computer system would not violate the ECPA"); Kent D. Stuckey et al., Internet and Online Law § 5.03[1] (Release 2 1998) (stating that ECPA "does not . . . protect against employers monitoring the e-mail of their employees"). But see Benkler, supra note 1, § 20.3[1] (arguing that ECPA's "definitional scope and express applicability to network operators offer good arguments to suggest that the ECPA applies to corporate LANs, and restricts the ability of employers to monitor the e-mail messages of their employees").

[40] 18 U.S.C. §§ 2511(3)(a), 2702(a)(1) (1994).

[41] See 18 U.S.C. § 2701(c)(1) (1994) (exempting all "conduct authorized . . . by the person or entity providing a wire or electronic communications service"). The provider of electronic communications services is known as the "network provider."

tion could instead be narrowly read to allow access for maintenance and billing purposes only.[42] Another criticism of the "complete access" theory is that a literal reading of section 2701(c)(1) creates situations where small technical differences in the configuration of employer-provided e-mail systems led to vastly different levels of protection.[43]

At least one federal district court agreed with the "complete access" theory and read section 2701(c)(1) literally. In *Bohach v. City of Reno*,[44] the plaintiffs, two police officers, sought an injunction preventing the City from continuing an internal affairs investigation.[45] In rejecting the plaintiffs' claim that the investigators' retrieval of their pagers' messages was a violation of the ECPA, the court noted that the City was the provider of the electronic communications service used by the officers.[46] It then held that "§ 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage. Because the City is the provider of the 'service,' neither it nor its employees can be liable under § 2701."[47]

Besides preventing disclosure and access to stored communications, a third way in which the ECPA might be used to protect employees from workplace e-mail monitoring is to conceive of e-mail monitoring as the *interception* of communications. Under this theory, e-mail monitoring would be subject to the stronger protections[48] of Title I of the ECPA. Interception would be understood as the act of accessing a message or preventing it from reaching its destination at any point between the time the message is sent and the time it is received by the intended recipient.

This conception of interception has not proved popular with courts construing the ECPA. Several recent cases indicate that most

---

42 See Stuckey, supra note 39, § 5.03[1][a][iv] (arguing that "complete access" theory does not comport with a consistent reading of statute).

43 See Benkler, supra note 1, § 20.3[3]. Professor Benkler offers a hypothetical in which Company M and Company N offer e-mail systems that appear identical to their employees. Company M, however, owns and operates the computer network itself, while Company N contracts with a third party for storage and processing services. Under the "complete access" theory, employees of M would have no rights against their employer under the ECPA, while employees of N would enjoy the benefit of full ECPA protections. See id.

44 932 F. Supp. 1232 (D. Nev. 1996).

45 See id. at 1232. The officers had used the police department's alphanumeric paging system to send messages to each other. See id. at 1233. The contents of these messages led to an internal affairs investigation of the officers. See id. The decision does not reveal the contents of the messages leading to the investigation.

46 See id. at 1236.

47 Id.

48 See infra note 55 and accompanying text (explaining that Title I of ECPA offers more protection than Title II).

courts will take a narrower view of what constitutes "interception" of e-mail.[49] Taken together, these decisions establish that, under the ECPA, interception can only occur during the fraction of a second the message is actually traveling along the wires connecting computers.[50]

In *Steve Jackson Games, Inc. v. United States Secret Service*,[51] the Fifth Circuit was faced with the issue of whether the seizure of a computer storing private e-mail that had been sent to an electronic bulletin board but not yet read by the recipients constituted an "intercept" proscribed by Title I of the ECPA.[52] The court determined that such a seizure was not an interception because the e-mail was not being transferred but was instead in storage incidental to transmission.[53] Other courts have reached similar conclusions regarding the definition of interception as used in the ECPA.[54] These rulings indicate that e-mail could almost always be seized before it reached its intended recipient without being "intercepted" and thus triggering the tough restrictions of Title I of the ECPA.[55] Unless an employer sets up a

---

[49] See, e.g., Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994) (holding that seizure of e-mail sent to bulletin board but not yet read by intended recipients did not constitute unlawful interception); *Bohach*, 932 F. Supp. at 1236 (same); United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (same).

[50] It may take much longer, of course, for an e-mail recipient to actually receive a message. E-mail is not usually sent directly from one computer to another. A message may be typed and sent on one computer, received by a second computer, and stored there until it is downloaded and read from the screen of a third computer used by the intended recipient. Depending on how often the intended recipient checks his or her e-mail, the message may wait hours or days on the storage computer before being noticed and read. Additionally, the path of an e-mail message sent over the Internet is unpredictable and potentially circuitous. See infra note 96.

[51] 36 F.3d 457 (5th Cir. 1994).

[52] See id. at 460.

[53] See id. at 461. The court further stated that "Title II of the ECPA clearly applies to the conduct of the Secret Service in this case" and held that there was "no indication in either the Act or its legislative history that Congress intended for conduct that is clearly prohibited by Title II to furnish the basis for a civil remedy under Title I as well." Id. at 462-63.

[54] See *Bohach*, 932 F. Supp. at 1235-36 ("The statutes therefore distinguish the 'interception' of an electronic communication at the time of transmission from the retrieval of such a communication after it has been put into 'electronic storage.'"); *Reyes*, 922 F. Supp. at 836 ("[T]he definitions [in the ECPA] thus imply a requirement that the acquisition of the data be simultaneous with the original transmission of the data.").

[55] The *Steve Jackson Games* court discussed some of the differences between Title I and Title II protections:

> First, the substantive and procedural requirements for authorization to intercept electronic communications are quite different from those for accessing stored electronic communications. For example, a governmental entity may gain access to the contents of electronic communications that have been in electronic storage for less than 180 days by obtaining a warrant. But there are more stringent, complicated requirements for the interception of electronic communications; a court order is required.

system where duplicate copies of e-mail messages are automatically made and sent to the employer for review at the exact moment of transmission, Title I "interception," as construed by the courts, would almost never occur.[56]

2. *Tort Remedies*

Government employees might find some measure of protection in various invasion of privacy torts.[57] The most useful tort action for employees facing e-mail monitoring is intrusion to seclusion.[58] To prevail on this claim, a plaintiff must show that the allegedly tortious intrusion would be highly offensive to a reasonable person.[59] In the few cases in which employees have brought invasion of privacy claims against employers for e-mail monitoring, the plaintiffs have not been able to convince courts that this standard has been met.

For example, in *Smyth v. Pillsbury Co.*,[60] the plaintiff, a Pillsbury employee terminated for sending "inappropriate and unprofessional comments" over the corporate e-mail system, had been repeatedly told that all workplace e-mail communications would remain confidential and privileged.[61] Smyth argued that he had relied on these assurances when sending the e-mails that caused his termination.[62] The court gave three reasons for dismissing Smyth's suit. First, Smyth could have had no reasonable expectation of privacy in e-mail sent

---

> Second, other requirements applicable to the interception of electronic communications, such as those governing minimization, duration, and the types of crimes that may be investigated, are not imposed when the communications at issue are not in the process of being transmitted at the moment of seizure, but instead are in electronic storage.

36 F.3d at 463 (citations omitted).

56 See, e.g., Jarrod J. White, Commentary, E-Mail@Work.Com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997) (arguing that under narrow interpretation of interception used in *Steve Jackson Games*, "interception of E-mail within the prohibition of the ECPA is virtually impossible").

57 See, e.g., Dichter & Burkhardt, supra note 1, § II.A.1 (listing four torts protecting right to privacy including intrusion to seclusion, misappropriation, unreasonable publicity, and false light).

58 See, e.g., Restatement (Second) of Torts § 652B (1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

59 See id.

60 914 F. Supp. 97 (E.D. Pa. 1996).

61 See id. at 98. In the e-mail messages, Smyth indicated his displeasure with management by threatening to "kill the backstabbing bastards," and referred to an upcoming holiday party as the "Jim Jones Koolaid affair." Id. at 98 n.1.

62 See id. at 98.

over the company system.[63] Even if an employee could have a reasonable expectation of privacy in such e-mail, the court continued, a reasonable person would not have found the defendant's interception highly offensive because the interception of e-mail neither required Smyth to disclose personal information nor invaded his person or personal effects.[64] The court then concluded by holding that Pillsbury's interests in preventing inappropriate and unprofessional comments in the workplace outweighed Smyth's interests in keeping his e-mail correspondence private.[65]

While *Smyth* is the only reported decision dealing with invasion of privacy tort claims for workplace e-mail monitoring, unreported decisions from other courts have reached similar conclusions.[66] Based on these cases, the chances for successful tort actions for invasion of privacy appear poor. Since courts analyze invasion of privacy torts in much the same way as they apply Fourth Amendment law, however, state courts often rely on Fourth Amendment jurisprudence when evaluating invasion of privacy claims.[67] As a result, if courts come to view the Fourth Amendment as limiting the permissible scope of workplace e-mail monitoring in government offices, the chances for successful tort actions for all employees will increase significantly.

3. *State Constitutional Protections*

Many states have constitutional provisions resembling those of the Fourth Amendment. At least twelve states have constitutional or statutory provisions that go beyond the Fourth Amendment and explicitly provide a right to privacy. Nine states provide a general right to privacy,[68] while three others specifically protect the privacy of per-

---

[63] See id. at 101 ("Once plaintiff communicated the alleged unprofessional comments to . . . his supervisor . . . over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."); see also infra text accompanying notes 129-32.

[64] See *Smyth*, 914 F. Supp. at 101.

[65] See id.

[66] See, e.g., Shoars v. Epson America, Inc., No. B073234, slip op. at 9 (Cal Ct. App. filed Apr. 14, 1994) (holding that e-mail messages sent or retrieved as part of defendant's business were not confidential as to defendant itself); Bourke v. Nissan Motor Corp., No. B068705, slip op. at 7-8 (Cal. Ct. App. filed July 26, 1993) (finding no objectively reasonable expectation of privacy because plaintiffs had signed waiver and were aware that their e-mail messages were read by coworkers).

[67] See Gantt, supra note 20, at 380 ("The balancing analysis in the tort context is essentially the same in Fourth Amendment jurisprudence, . . . and [thus] many state courts have followed the Fourth Amendment balancing approach in addressing tortious invasion of privacy claims.").

[68] See Alaska Const. art. I, § 22; Ariz. Const. art. II, § 8; Cal. Const. art. I, § 1; Haw. Const. art. I, § 6; Mont. Const. art. II, § 10; S.C. Const. art. I, § 10; Wash. Const. art. I, § 7; see also Mass. Gen. Laws Ann. ch. 214, § 1B (West 1989); R.I. Gen. Laws § 9-1-28.1 (1997).

sonal communications.[69] California courts have even held that California state constitutional privacy rights apply to private, as well as public, actors.[70] Additionally, some state courts have held that their state constitutions offer broader protection against searches and seizures in many contexts than does the federal Constitution.[71] In many states, then, state constitutional law offers a potentially useful source of privacy protections against e-mail monitoring. The extent of this protection is uncertain, however, because there are no cases in which the issue of government employee e-mail monitoring has been litigated.

The Fourth Amendment remains extremely important in assessing privacy claims based on state constitutions, however. Because the Amendment applies to all the states, it offers a floor of privacy protections below which no state can fall.[72] States also look to Fourth Amendment jurisprudence when construing their own constitutions.[73] Some states have even adopted a "lockstep" approach that prohibits their courts from construing their state constitutional search and seizure provisions more broadly than federal Fourth Amendment law would allow.[74] Novel readings of the Fourth Amendment should

---

[69] See Fla. Const. art. 1, § 12 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated."); Ill. Const. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means."); La. Const. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy.").

[70] See Cal. Const. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining safety, happiness, and privacy."); Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994) (stating that "Privacy Initiative . . . of the California Constitution creates a right of action against private as well as government entities").

[71] See, e.g., State v. Owen, 453 So. 2d 1202, 1205 (La. 1984) (rejecting Fourth Amendment standing doctrine established in United States v. Salvucci, 448 U.S. 83 (1980) and Rakas v. Illinois, 439 U.S. 128 (1978)); Commonwealth v. Edmunds, 586 A.2d 887, 895-905 (Pa. 1991) (rejecting "good faith" exception to exclusionary rule established in United States v. Leon, 468 U.S. 897 (1984)). For an excellent discussion of this "New Federalism," see generally Nina Morrison, Note, Curing "Constitutional Amnesia": Criminal Procedure Under State Constitutions, 73 N.Y.U. L. Rev. 880 (1998).

[72] The Fourth Amendment, as incorporated through the Fourteenth Amendment, is applicable to the states. See, e.g., Mapp v. Ohio, 367 U.S. 643, 654 (1961); Wolf v. Colorado, 338 U.S. 25, 27-28 (1949).

[73] See Gantt, supra note 20, at 380 ("Supreme Court Fourth Amendment jurisprudence has fundamentally influenced judicial opinions applying all legal sources of privacy protection.").

[74] See, e.g., Fla. Const. art. 1, § 12 (stating that search and seizure rights "shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court").

prompt these states to expand privacy protections emanating from both constitutional and tort law.

Because both tort law and state constitutional law are so heavily influenced by federal Fourth Amendment jurisprudence, the scope of the Fourth Amendment, as applied to government workers by federal courts, will have an effect that reaches far beyond government workplaces. As a result, applications of the Fourth Amendment to e-mail monitoring become important for all workers, not just those who work in the public sector. The next Part begins the process of applying the Fourth Amendment to e-mail in the government workplace.

II
THE FOURTH AMENDMENT MEETS E-MAIL: IS THERE A REASONABLE EXPECTATION OF PRIVACY?

As a first step in answering *Katz*'s threshold question regarding the existence of reasonable expectations of privacy as applied to e-mail monitoring, this Part looks at how courts have construed the Fourth Amendment when confronted with other new technologies. One useful method for dealing with new technologies is to analogize them to older ones. Analogizing to fit e-mail within the established Fourth Amendment framework becomes more complicated, though, when considering expectations of privacy in the workplace. Several attributes of the office environment can defeat an otherwise reasonable expectation of privacy. This Part identifies obstacles to using the Fourth Amendment to limit searches in the workplace, and suggests reasons why they are not insurmountable.

A. Applying the Fourth Amendment to New Technologies: Translation and Analogies

Applying the Fourth Amendment to technologies the Founders never envisioned has proven troublesome for courts. For example, when first confronted with a case involving the constitutionality of wiretapping, the Supreme Court held that the Fourth Amendment was inapplicable.[75] The Court reasoned that the Founders intended the Fourth Amendment to limit common law trespass on property; since wiretapping involved no physical trespass, the Amendment was not implicated.[76] It took nearly forty years for the Court to reject this

[75] See Olmstead v. United States, 277 U.S. 438, 466 (1928).
[76] See id. at 463-66.

view of the Fourth Amendment and find that wiretapping was indeed included within its scope.[77]

The difficulty in adapting constitutional norms to new technologies stems in part from the nature of the federal Constitution, which Lawrence Lessig calls a "codifying constitution."[78] A codifying constitutional regime "aims at preserving something essential from the then-current constitutional or legal culture—to protect it against change in the future."[79] Lessig argues that "the Bill of Rights . . . was a constitutional regime that sought to entrench certain practices and values against change."[80] Courts have had a hard time preserving the values codified in the Bill of Rights when confronted with changes in technology that allow law enforcement to invade privacy in more places and in more ways than were imaginable at the time the Fourth Amendment was adopted.

The method for dealing with technological change Lessig suggests, and the one used by Justice Brandeis in his marvelous dissent in *Olmstead v. United States*,[81] is translation.[82] Translation, as applied to e-mail, involves "identif[ying] values from the original Fourth Amendment, and then translat[ing] these values into the context of cyberspace."[83] When translating the Fourth Amendment, courts must "read beyond the specific applications that the Framers had in mind, to find the meaning they intended to constitutionalize."[84]

---

77 See Katz v. United States, 389 U.S. 347, 353 (1967). In a line of telecommunications privacy cases following *Olmstead*, the Court had always required a physical trespass or penetration in order for the Fourth Amendment to be implicated. See, e.g., Goldman v. United States, 316 U.S. 129, 134-35 (1942) (holding that use of detectaphone placed against wall to hear conversations next door did not violate Fourth Amendment because there was no trespass); On Lee v. United States, 343 U.S. 747, 751-54 (1952) (holding that use of microphone and transmitter by informer inside home of defendant did not implicate Fourth Amendment because there was no trespass); Silverman v. United States, 365 U.S. 505, 509-12 (1961) (holding that placement of footlong microphone against heating duct violated Fourth Amendment because it intruded into constitutionally protected area).

78 Lawrence Lessig, Reading the Constitution in Cyberspace, 45 Emory L.J. 869, 869 (1996).

79 Id.

80 Id.

81 277 U.S. 438, 471-85 (1928) (Brandeis, J., dissenting).

82 See Lessig, supra note 78, at 873.

83 Id. (emphasis removed).

84 Id. Laurence Tribe makes a similar point about applying constitutional rights in the face of new technologies. He argues that "[n]ew technologies should lead us to look more closely at just what values the Constitution seeks to preserve." Laurence H. Tribe, The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier (March 26, 1991) <http://www.sjgames.com/SS/tribe.html>. We should not assume that the existence of "technologies the Framers didn't know about make their concerns and values obsolete." Id.

Translation is obviously a difficult task and depends in large part on what values one believes the Framers meant to codify. The "reasonable expectation of privacy" standard in *Katz* is the current way in which the Court seeks to translate the core values in the Fourth Amendment and apply them to the realities of late-twentieth century life. Implicitly, *Katz* states that the Framers of the Fourth Amendment really meant to limit government intrusions into all areas where citizens have a reasonable expectation of privacy, regardless of whether those areas are homes or public phone booths.

Although *Katz* provides a framework for translating Fourth Amendment values to new technologies, the reasonable expectation of privacy test still requires courts to ask immensely important and difficult normative questions about the values society should honor.[85] One way to ease the difficult task of translation, and to determine whether there is a reasonable expectation of privacy in e-mail communications, is to analogize e-mail to other, older forms of communication. At least two widely used technologies immediately present themselves: telephone calls and traditional postal mail.[86]

E-mail might be analogized to telephone calls because both are forms of electronic communication. The aptness of the phone analogy varies depending on the form e-mail takes. E-mail may be transmitted and received in several ways, including instant messaging,[87] "chat rooms,"[88] and listservs.[89] Instant messaging is the form of e-mail most like a phone call, although the speed of communication is limited by the parties' typing abilities. Chat rooms are like a type of party line in

---

[85] See, e.g., Note, Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication, 110 Harv. L. Rev. 1591, 1607 (1997) [hereinafter Note, Keeping Secrets] ("Deciding which expectations of privacy are reasonable . . . requires a judgment about the kind of society in which we want to live. . . . [W]e cannot divorce the level of privacy that the Constitution does protect from a judgment about how much privacy our society ought to protect.").

[86] See, e.g., Chris J. Katopis, "Searching" Cyberspace: The Fourth Amendment and Electronic Mail, 14 Temp. Envtl. L. & Tech. J. 175, 196-99 (1995) (analyzing possible application of telephone monitoring laws to e-mail); Note, Keeping Secrets, supra note 85, at 1597-99 (discussing analogy of e-mail to postal mail and telephone calls).

[87] Instant messaging takes place when two users at their respective computers at the same time use special software to type and read messages in real time. Instant messaging allows both persons to respond to one another instantly, providing a conversation-like interaction.

[88] Chat rooms may be conceptualized as multiple party instant messaging. They are most often found on commercial networking services such as America Online. A commercial service provider may offer its subscribers the capability to enter multiple chat rooms, each with a different theme based on age, interests, sexuality, and so forth.

[89] Listservs act as an e-mailed newsletter, automatically sending e-mail updates about a particular topic to subscribers. For example, several airlines maintain listservs that provide information about discounted airfares on a weekly basis.

which many parties can participate simultaneously, but are also subject to typing-speed restrictions. The closest telephone equivalents to listservs are perhaps services which allow a caller to listen to a recording and access oft-updated information.[90]

If courts viewed e-mail as akin to a telephone call, the Fourth Amendment would apply in most cases. *Katz* established that there is a reasonable expectation of privacy in telephone calls.[91] Courts have found, however, that different types of telephone calls receive different levels of Fourth Amendment protection. Similarly, different forms of e-mail might not have the same, or any, expectation of privacy.

Some courts have held that persons making calls on cordless phones do not enjoy a reasonable expectation of privacy because they should know that their conversations can be easily intercepted.[92] The difference in the expectations of privacy between regular and cordless telephones cannot depend on ease of interception alone, however.[93] It is very easy for the government to tap phone lines and intercept calls on wired phones. A more accurate distinction would be that conversations on cordless phones are more likely to be intercepted accidentally by members of the public when, for example, next door neighbors use cordless phones sharing the same radio frequency.[94] Applying this notion to e-mail could lead to the conclusion that persons sending messages to or from chat rooms and listservs would have little or no expectation of privacy. These forms of communication involve large numbers of people communicating in easily accessible cor-

---

[90] An example is MovieFone, which allows callers to listen to updated movie schedules and plot synopses. The main difference is that, after subscribing, information from a listserv is automatically sent to a subscriber, while accessing MovieFone requires a user to make a phone call to the service.

[91] See Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

[92] See, e.g., McKamey v. Roach, 55 F.3d 1236, 1239 (6th Cir. 1995) (holding that interception of conversations made on cordless phone are not subject to ECPA because they are so easily intercepted); In re Askin, 47 F.3d 100, 103 (4th Cir. 1995) (same); Tyler v. Berodt, 877 F.2d 705, 706-07 (8th Cir. 1989) ("Courts have not accepted the assertions of privacy expectation by speakers who were aware that their conversation was being transmitted by cordless telephone."). But see United States v. Smith, 978 F.2d 171, 179 (5th Cir. 1992) (noting that changes in technology have made cordless phone conversations more private).

[93] See, e.g., Note, Keeping Secrets, supra note 85, at 1598 ("Pure ease of interception cannot render an expectation of privacy unreasonable, however, because such a rule would remove well-settled Fourth Amendment protections.").

[94] See id. (speculating that ease of interception "refers to the likelihood that others may intercept the communication in the course of their regular affairs").

ners of cyberspace.[95] Most e-mail, however, is sent directly from one person to another and thus preserves the expectation of privacy that flows from one-on-one communication like the phone call in *Katz*. Moreover, one-on-one e-mail is not accidentally intercepted by members of the public in the way that cordless phone conversations often are.[96]

The telephone analogy fails, however, to take into account two important aspects of e-mail: that it is written and that it has a permanence that telephone conversations lack.[97] These characteristics make e-mail more like traditional postal mail. Like postal mail, electronic mail is written and can be saved for future reference. Courts have long recognized that the Fourth Amendment applies to searches and seizures of postal mail.[98] When a sealed container is sent through the mails, the government may not search it without a warrant.[99] This rationale arguably applies to e-mail sent from one person to another.[100] More open forms of e-mail, such as chat rooms and listservs, are more like postcards. Postcard senders cannot have a reasonable expectation of privacy in their messages because anyone can read them at any point during the course of delivery.[101]

---

95 The nature of chat rooms allows the public easily to view participants' communications. See infra notes 120-21 and accompanying text.

96 E-mail transmissions are actually quite secure, even when sent without the aid of encryption software.

> [E]mail is generally more secure from interception than other forms of communication because of the way the Internet works. Information transmitted over the Internet is . . . broken into small "packets" of data, each of which typically reaches its final destination via a different path. Some packets may travel from New York to Washington via Bangkok, for example, while others may travel through Toronto. These packets are reassembled into a single message only at the end of their travels. The precise route traveled typically varies from message to message. This is part of the reason that the time for email transmission can vary so widely—different messages may arrive by very different routes. . . . This "packet" transmission method means that, in most cases, email messages are less likely to be readily intercepted than more familiar means of communication.

Victoria A. Cundiff, Trade Secrets and the Internet: A Practical Perspective, Computer Law., Aug. 1997, at 6, 8.

97 See Aftab, supra note 2, at 4 (noting that most computer systems make backup copies of e-mail and that e-mail is difficult to delete).

98 See, e.g., Ex parte Jackson, 96 U.S. 727, 733 (1877) (holding that mail searches must conform to Fourth Amendment standards).

99 See, e.g., United States v. Choate, 576 F.2d 165, 174 (9th Cir. 1978) ("[I]t is settled that the Fourth Amendment's protection against 'unreasonable searches and seizures' protects a citizen against the warrantless opening of sealed letters and packages addressed to him in order to examine the contents.").

100 See, e.g., Winick, supra note 3, at 116 n.212 (arguing that logic of Fourth Amendment law protecting traditional postal mail should extend to e-mail).

101 See, e.g., Note, Keeping Secrets, supra note 85, at 1597 (arguing that because anyone can read contents of postcards, expectation of privacy in contents would be unreasonable).

In *United States v. Maxwell*,[102] a court found both the telephone and postal mail analogies useful. In *Maxwell*, the FBI received reports, including forwarded e-mail messages, indicating that certain persons were sending child pornography over America Online (AOL), a commercial network service provider.[103] Based on this information, the FBI obtained a warrant to search the e-mail files of several AOL subscribers.[104] The warrant identified the files to be searched by screen name.[105] Maxwell used at least two screen names: Reddel ("ready one") and Zirloc. Although e-mail files for both screen names were seized, the warrant listed only the first name.[106] Maxwell objected to the seizure of e-mail listed under the screen name Zirloc on Fourth Amendment grounds because "Zirloc" was not listed in the warrant. He moved to suppress all information seized from the Zirloc screen name.[107]

In assessing Maxwell's motion to suppress the Zirloc-related material, the court had to decide whether Maxwell possessed a reasonable expectation of privacy in AOL's e-mail system.[108] In holding that Maxwell did enjoy such an expectation of privacy, the court used both the telephone and postal mail analogies to aid in its analysis.[109] Stating that "the technology used to communicate via e-mail is extraordinarily analogous to a telephone conversation,"[110] the court noted that the Fourth Amendment applies to telephone calls because "the maker of a telephone call has a reasonable expectation that police officials

---

Only one federal case has considered the issue of whether a postcard seizure violates the Fourth Amendment, albeit in the context of the search of a private home. In United States v. Fernandez, No. 89 CR. 522, 1989 WL 156282 (S.D.N.Y. Dec. 20, 1989) the court held that the seizure of a postcard sent to the defendant violated the Fourth Amendment because the government could not demonstrate that the incriminating nature of the postcard was "immediately apparent" at the time of its seizure. Id. at *1. In fact, the postcard was not incriminating at all, but was merely used to help identify the defendant. See id. at *2. The court did not address whether the defendant had a reasonable expectation of privacy in the postcard's contents.

102 45 M.J. 406 (C.A.A.F. 1996).

103 See id. at 412.

104 See id.

105 See id. at 413. E-mail sent through AOL is identified by a screen name. Each subscriber who maintains an account on AOL can have one or more screen names. Often, a family will subscribe to AOL and each family member will have a different screen name. Each screen name acts as a totally separate user and each screen name can use the service independently of anyone else. See id. at 411.

106 See id. at 413. Additionally, the warrant misspelled Maxwell's screen name as "REDDEL." See id.

107 See id. at 415.

108 See id. at 416.

109 See id. at 417.

110 Id.

will not intercept and listen to the conversation."[111] As for the postal analogy, the court observed that like a letter, e-mail is sent and lies sealed until the recipient retrieves the transmission.[112] The sender of either postal mail or e-mail "enjoys a reasonable expectation that the initial transmission will not be intercepted by the police."[113]

Both of these analogies led the court to hold that senders of e-mail do have a reasonable expectation of privacy in the messages they send, thus implicating the Fourth Amendment when the state seeks to search or seize e-mail.[114] *Maxwell* was followed by another court in *United States v. Charbonneau*[115] which held that the defendant possessed a "limited reasonable expectation of privacy in the e-mail messages he sent and/or received on AOL."[116] These cases indicate that courts are willing to find that, at least under certain conditions, e-mail users have a reasonable expectation of privacy and that the government must comport with the Fourth Amendment when searching or seizing e-mail messages.

B. Obstacles on the Road to a Reasonable Expectation of Privacy: Plain View, Disclosure, and Consent

While *Maxwell* and *Charbonneau* indicate that courts *may* find that e-mail users at home have a reasonable expectation of privacy, these cases provide little guidance as to the application of the Fourth Amendment when e-mail is used in the government workplace. Finding a reasonable expectation of privacy for e-mail sent from work over a government employer-provided e-mail system adds layers of complexity to the Fourth Amendment analysis. Three "exceptions" to the Fourth Amendment—the doctrines of plain view, disclosure, and consent—present obstacles that government employees must overcome in order to demonstrate that they have a reasonable expectation of privacy in their e-mail.

1. Plain View

The plain view doctrine allows for warrantless searches and seizures when law enforcement officials lawfully come upon some-

111 Id. at 418.

112 See id. E-mail lies "sealed" in the user's computer "mailbox" rather than in a physical mailbox.

113 Id.

114 See id. ("[T]he transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant.").

115 979 F. Supp. 1177 (S.D. Ohio 1997).

116 Id. at 1184.

thing in plain view.[117] Justice Harlan's concurrence in *Katz* articulated the rationale for the doctrine: "[O]bjects, activities, or statements that [one] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to [one]self has been exhibited."[118] Plain view searches and seizures therefore violate none of the privacy interests protected by the Fourth Amendment, because if an article is in plain view, "neither its observation nor its seizure . . . involve[s] any invasion of privacy."[119]

In certain circumstances, electronic messages are subject to the plain view exception to the warrant requirement. Messages sent in AOL chat rooms can, and have been, observed by outsiders, including law enforcement officials.[120] Participants in these chat rooms demonstrate no intention of keeping their comments to themselves and consequently possess no reasonable expectation of privacy in their electronic communications.[121]

E-mail or other messaging systems that have no password, and are thus open to all employees, leave messages in plain view.[122] Users of such systems should not have a reasonable expectation of privacy. Most workplace e-mail systems, however, provide employees with an individual password that prevents others from accessing their e-mail. By restricting access, a password takes messages out of plain view.[123]

---

117 Although subject to numerous exceptions—the plain view doctrine being one example—a search or seizure under the Fourth Amendment generally requires a warrant to be valid. See, e.g., Mincey v. Arizona, 437 U.S. 385, 390 (1978) ("[I]t is a cardinal principle that 'searches conducted outside the judicial process, without prior approval by a judge or magistrate, are per se unreasonable under the Fourth Amendment—subject to only a few specifically established and well-delineated exceptions.'" (quoting Katz v. United States, 389 U.S. 347, 357 (1967))).

118 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

119 Horton v. California, 496 U.S. 128, 133 (1990).

120 See, e.g., *Charbonneau*, 979 F. Supp. at 1179 (describing how FBI agent posed as pedophile in chat rooms and observed and recorded electronic conversations among users interested in exchanging child pornography).

121 See, e.g., United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996) ("Messages sent to the public at large in the 'chat room' . . . lose any semblance of privacy."); accord *Charbonneau*, 979 F. Supp. at 1185 (stating that e-mail posted in chat room is "not afforded any semblance of privacy").

122 See, e.g., Bohach v. City of Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (finding no reasonable expectation of privacy in paging system which operated like e-mail because system had no password requirement and no access restrictions). But cf. United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (holding that defendant had reasonable expectation of privacy in contents of pager's memory). For a more detailed discussion of *Bohach*, see supra notes 44-47 and accompanying text.

123 Even with a password, persons other than the sender and intended recipient might be able to view an e-mail message, perhaps by reading it from the monitor of an unattended computer screen. A password need not, however, make an e-mail *impossible* for anyone other than the sender and recipient to view in order for it to take the message out of plain view. Harlan's conception of plain view, see supra note 118, requires only an

Thus, the plain view doctrine would not apply to e-mail messages sent on a password system directly from one person to another. These messages are rarely intentionally exposed to anyone other than the sender and the recipient. Consequently, even though the plain view doctrine does remove chat room messages from the ambit of the Fourth Amendment, this exception should not affect Fourth Amendment limitations on e-mail monitoring in most workplaces.

2. *Disclosure*

The disclosure of personal communications to state officials by one of the parties to the communication presents a more difficult hurdle to applying the Fourth Amendment to e-mail monitoring. Such disclosure, if voluntary, does not implicate the Fourth Amendment.[124] This means that an e-mail recipient can forward messages to anyone, including law enforcement officials, without implicating the original sender's Fourth Amendment interests.[125] The rationale for this result stems from those cases where the Supreme Court has allowed the introduction of evidence obtained by bugging an undercover agent.[126] The Court held that when individuals discuss illegal activity with others, they assume the risk that those with whom they speak are government agents.[127] Furthermore, the Court held that individuals cannot rely on their misplaced confidence that those with whom they conduct illicit activities will not disclose their crimes.[128]

"intention" to keep something to oneself, not success. See supra note 93 and accompanying text.

124 "Disclosure" by a recipient of an e-mail message to law enforcement is a variant of the "third-party consent" exception to the Fourth Amendment. If a person permits a third party to use or control property, the person has assumed the risk that the third party may consent to a search of the property. See, e.g., Frazier v. Cupp, 394 U.S. 731, 740 (1969) (holding that when defendant left his duffel bag at his cousin's house, he "must be taken to have assumed the risk that [his cousin] would allow someone else to look inside").

125 See, e.g., *Maxwell*, 45 M.J. at 419 (characterizing e-mail turned over to FBI as "'fair game' for introduction into evidence and for use in procuring a search warrant").

126 See Hoffa v. United States, 385 U.S. 293, 300-03 (1966) (holding that Fourth Amendment protections do not apply when defendant accepts risk that audience for speech may be undercover government agent); Lopez v. United States, 373 U.S. 427, 439 (1963) (holding that bugging undercover agent is permissible when the device "neither saw nor heard more than the agent himself").

127 See *Lopez*, 373 U.S. at 439 ("We think the risk that petitioner took in offering a bribe to [the undercover officer] fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording."); see also id. at 465 (Brennan, J., dissenting) ("The risk of being overheard by an eavesdropper or betrayed by an informer . . . is probably inherent in the conditions of human society.").

128 See *Hoffa*, 385 U.S. at 302.

Smyth v. Pillsbury Co.[129] illustrates an application of the disclosure doctrine in the context of e-mail. The *Smyth* court examined the plaintiff's reasonable expectation of privacy in the e-mail messages that were the source of his termination.[130] The court held that the plaintiff did not have a reasonable expectation of privacy in the e-mail he voluntarily sent to his supervisor "notwithstanding any assurances that such communications would not be intercepted by management."[131] The court reasoned that Smyth lost any expectation of privacy he may have possessed in his e-mail because he disclosed it to his supervisor.[132]

The fact that individual e-mail messages may be forwarded or disclosed to law enforcement officials without the consent of the original sender should not destroy an expectation of privacy in general e-mail use, however. Although specific phone conversations may easily be taped and disclosed by one of the parties, *Katz* held that phone conversations in general still retain reasonable expectations of privacy. The fact that e-mail messages can be forwarded, and thus disclosed, with little effort should not cause courts to view *all* e-mail as disclosed unless there is a conscious choice on the part of the recipient to give up both her privacy and the privacy of the sender in the act of transmitting a particular communication. Purposefully undisclosed e-mail should remain private.[133]

Of course, sending *any* e-mail over an employer's workplace e-mail system might be viewed as a variant of disclosure. After all, when employees send and store e-mail messages on a system at work, they have necessarily disclosed the contents of any messages to the owner of the system, who is often also the employer. While this argument might seem intuitively correct, it ignores the theory of Fourth Amendment protections announced in *Katz* and refined in subse-

---

129 914 F. Supp. 97 (E.D. Pa. 1996). For a discussion of *Smyth* see supra notes 60-65 and accompanying text.

130 *Smyth*, 914 F. Supp. at 101. The court examined the plaintiff's reasonable expectation of privacy even though the case was brought as a tort action for invasion of privacy since the Fourth Amendment would not have applied to Pillsbury, a private sector employer. See id.; see also supra note 67 and accompanying text.

131 Id. The *Smyth* court could have dismissed the complaint based solely on the plaintiff's disclosure of the offensive e-mail. The court instead mingled a disclosure analysis with a broader ruling that there could be no expectation of privacy in an e-mail system "apparently utilized by the entire company." Id. Why the court felt compelled to find that users of a corporate e-mail system have no privacy and how it reached this holding are unclear.

132 See id.

133 Cf. United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996) ("[O]nce the Government wanted to search the [defendant's] computer files further based upon these chance scraps of [disclosed] information, a warrant was required.").

quent cases. In order to enjoy the protections of the Fourth Amendment, a person need only have a reasonable expectation of privacy in the area searched or thing seized.[134] As the Court held in *Mancusi v. DeForte*,[135] a property interest is not a necessary precondition for a reasonable expectation of privacy.[136]

In *DeForte*, the defendant, a vice president of a union, objected to the warrantless search of the office he shared with other union officials and the subsequent seizure of union records.[137] The Court noted that the records that were seized belonged to the union, not to DeForte.[138] Despite this fact, the Court held that DeForte could object to the warrantless seizure of documents he did not own because the "capacity to claim the protection of the [Fourth] Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from government intrusion."[139]

Like *DeForte*, *Katz* demonstrates that Fourth Amendment protections against unreasonable searches and seizures exist independent of property interests. The Court found that the Amendment applied to calls Katz made from a *public* phone booth.[140] Similarly, individuals do not lose reasonable expectations of privacy in postal mail simply because letters and packages are handled by parties not owned or controlled by the sender.[141]

In cases such as *DeForte* and *Katz*, the Court showed that *ownership* of e-mail infrastructure should not affect Fourth Amendment protection for e-mail. The question of whether relinquishing *control* of e-mail messages to employers during transmission and storage affects reasonable expectations of privacy complicates the issue. In some instances, entrusting a third party with information destroys an expectation of privacy. In *United States v. Miller*,[142] the Court held that the defendant possessed no reasonable expectation of privacy in financial documents held by a bank.[143] Public employers might try to

---

134 See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

135 392 U.S. 364 (1968).

136 See id. at 368.

137 See id. at 365.

138 See id. at 367.

139 Id. at 368 (citing *Katz*, 389 U.S. at 352).

140 See *Katz*, 389 U.S. at 352.

141 See Ex parte Jackson, 96 U.S. 727, 733 (1877) (holding that Fourth Amendment warrant requirements are applicable to sealed mail).

142 425 U.S. 435 (1976).

143 See id. at 442-43 ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks . . . in the ordinary course of business. . . . The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

apply *Miller* to e-mail monitoring by arguing that employees disclose information to their employer when using e-mail in the same way that bank customers disclose their financial information to their bank. Copies of all incoming and outgoing e-mail pass through, and are usually stored on, a central computer on their way to the recipient.[144] Employers could argue that employees disclose the contents of their e-mail messages because they are stored on computers over which the employer has control and access.[145]

Using *Miller* as a basis for arguing that *all* e-mail messages are disclosed to the employer is ultimately unpersuasive, however. First, access to bank records was authorized by a federal statute, the Bank Secrecy Act.[146] The express purpose of the Act was to require records to be maintained because they were highly useful in criminal, tax, and regulatory investigations and proceedings.[147] No such statute compels the maintenance of e-mail files. Second, bank records and e-mail comprise "two vastly different fields."[148] Bank records are "transactional" while e-mail should be considered "expressive in nature."[149]

Finally, and most importantly, a bank has a different purpose for searching financial records than a system administrator would have for investigating e-mail messages stored in a routing computer. Bank officials must examine the content of financial records in order to process them—they need to know the source or destination and the amount of funds to be transferred in order to complete processing. System administrators, on the other hand, have no legitimate need

144 See, e.g., Electronic Mail Primer (visited Sept. 15, 1998) <http://www.qhsc.com/internet/intro/e-mail.html> (describing how e-mail works); Paul McFedrie, A Brief E-Mail Primer (visited Sept. 15, 1998) <http://www.mcfedries.com/Ramblings/email-workings.html> (same); Leonard Tuara, Electronic Mail, in What Lawyers Need to Know, supra note 38, at 181, 183 (describing e-mail as storage system and comparing it favorably to voice mail).

145 Even when employees are given individual passwords, the system administrator is still able to read all e-mail messages. The password keeps other employees and outsiders from particular e-mail accounts but does not prevent the employer who administers the system from having full access to all messages on the system. See Gantt, supra note 20, at 349-50 (describing ability of employer to access employee e-mail despite individual passwords); 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, 141 (1994) (describing ability of system administrators to monitor and print out e-mail).

146 12 U.S.C. § 1951 (1994).

147 See *Miller*, 425 U.S. at 442-43 (discussing purpose of Bank Secrecy Act).

148 Katopis, supra note 86, at 202.

149 Id. Although the financial data contained in bank records may be sensitive, e-mail messages have the potential to express far more varied, and more private, information.

regularly to examine the contents of e-mail messages as a function of maintaining an electronic mail system.[150]

Furthermore, any form of communication other than face-to-face conversation involves transferring information to a third party, whether it be a phone company or postal employees. Simply because a third party has the *ability* to read communications does not destroy an expectation of privacy. Viewing the information must be a *necessary* part of the role the third party plays in order for there to be a disclosure of information.

3. *Consent*

Perhaps the greatest obstacle to applying the Fourth Amendment to government workplace e-mail monitoring is the effect that workplace policies may have on employees' reasonable expectations of privacy in their e-mail. Some commentators have suggested that employees consent to searches of their e-mail if their employer has promulgated an explicit policy stating that employees' e-mail may be monitored at any time.[151] In other words, by accepting or continuing employment under the terms of the policy, employees consent to monitoring of their e-mail.

An example of an e-mail monitoring policy that could be considered a consent to monitoring is the one currently in place for Department of Defense (DoD) employees.[152] The policy states that "[u]se of this DoD computer system . . . constitutes consent to monitoring of this system."[153] Such monitoring "may occur at any time" and "will usually go unnoticed even by skilled users."[154] The scope of the monitoring is unlimited: "All information, including personal information, placed on or sent over this system may be monitored."[155]

---

150 See, e.g., Randolph S. Sergent, Note, A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181, 1214 (1995) ("[F]or the multiple-user computer system the contents of user files are not disclosed to the system manager because the system manager has no legitimate use for them in running the system.").

151 See, e.g., Gantt, supra note 20, at 382 ("[A]n employee's expectation of privacy can virtually be eliminated by office regulations and practices, and no privacy right is even implicated without such an expectation."); Lee, supra note 145, at 148 ("[A] publicized monitoring policy reduces an employee's expectation of privacy . . . ."); Dichter & Burkhardt, supra note 1, § II.A.1.c ("[I]f employees are notified concerning the types of searches that may be conducted and the areas that may be searched, their reasonable expectations of privacy in those areas may be reduced.").

152 See Scot L. Gulick, Memorandum from Office of General Counsel to all Computer Users, The Standards of Ethical Conduct (United States Dep't of Defense), Sept. 1997, at 1 (on file with the *New York University Law Review*).

153 Id. at 2.

154 Id. at 1.

155 Id. at 2.

Where the Fourth Amendment would otherwise limit a search or seizure, a person may forfeit such protections by consenting to a search.[156] Most workers could be expected to consent to monitoring if they decide that earning a livelihood is more important than enjoying privacy protections in the workplace. With employees routinely agreeing to workplace policies and thus granting ongoing consent, government employers would be free to monitor without infringing on their employees' Fourth Amendment rights.

Courts may view conditioning employment on a waiver of Fourth Amendment rights, however, as an unconstitutional condition on government employment. The Supreme Court has articulated the doctrine of unconstitutional conditions in the following manner:

> [E]ven though a person has no "right" to a valuable governmental benefit and even though the government may deny him the benefit for any number of reasons, there are some reasons upon which the government may not rely. It may not deny a benefit to a person on a basis that infringes his constitutionally protected interests . . . .[157]

In the one case where the Supreme Court dealt with conditioning receipt of a government benefit on waiver of Fourth Amendment rights, the Court held that the condition was constitutional. *Wyman v. James*[158] upheld a welfare regulation requiring an in-home visit by government social workers in order for families to receive welfare benefits.[159] While the holding in *Wyman* appears to implicitly support

---

156 See Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973) (stating that "a search conducted pursuant to a valid consent is constitutionally permissible").

157 Perry v. Sindermann, 408 U.S. 593, 597 (1972). The Supreme Court has long struggled with the doctrine of unconstitutional conditions. See, e.g., Brooks R. Fudenberg, Unconstitutional Conditions and Greater Powers: A Separability Approach, 43 UCLA L. Rev. 371, 374 & n.14 (1995) (asserting that "[t]he Supreme Court's [unconstitutional conditions] decisions are wonderfully inconsistent" and citing cases and commentary). Opponents of the doctrine, often conservative judges, argue that it conflicts with the logic of the "greater includes the lesser" syllogism: If the Constitution permits the government the greater power of denying a benefit altogether, the lesser power of conditioning receipt of the benefit must also be constitutional. See, e.g., Posadas de Puerto Rico Assocs. v. Tourism Co. of Puerto Rico, 478 U.S. 328, 345-46 (1986) (Rehnquist, C.J.) (stating that "the greater power to completely ban casino gambling necessarily includes the lesser power to ban advertising of casino gambling"). The inherent tensions within the doctrine have engendered a large and highly complex literature, far beyond the scope of this Note. See generally Richard A. Epstein, The Supreme Court, 1987 Term—Foreword: Unconstitutional Conditions, State Power, and the Limits of Consent, 102 Harv. L. Rev. 4 (1988) (presenting model for explaining unconstitutional conditions jurisprudence); Fudenberg, supra (analyzing "greater includes the lesser" argument and proposing nonseparability approach); Kathleen M. Sullivan, Unconstitutional Conditions, 102 Harv. L. Rev. 1413 (1989) (arguing that rights-denying conditions on government benefits require close scrutiny by courts to determine constitutionality of such conditions).

158 400 U.S. 309 (1971).

159 See id. at 326.

the power of government employers to require that employees waive their Fourth Amendment rights to privacy in e-mail, the case is distinguishable for several reasons. First, the welfare program in *Wyman* was focused on dependent children.[160] Since "[t]here is no more worthy object of the public's concern" than its children, the Court held that the government could take special measures to protect the young.[161] Second, the Court noted the public's strong interest in learning how welfare benefits are actually used by recipients.[162] Finally, the Court reasoned that the home visit requirement served a beneficial purpose apart from facilitating receipt of benefits: "[T]he visit is 'the heart of welfare administration' . . . [because] it affords 'a personal, rehabilitative orientation, unlike that of most federal programs.'"[163]

None of these special interests is present in the context of workplace e-mail monitoring. E-mail monitoring of employees does not protect children,[164] does not concern the distribution of public funds, and does not involve a separate salutary purpose for the party monitored. Because *Wyman* dealt with circumstances so far removed from those at play in the government workplace, the case cannot be read as permitting the government to condition employment on consent to e-mail monitoring. This does not mean that *Wyman* is irrelevant to the question of consent to e-mail monitoring. The case simply suggests that the government must put forth important interests when it conditions the receipt of a benefit on relinquishment of Fourth Amendment rights.

While *Wyman*'s compelling interest requirement works to limit the power of the government to coerce waiver of constitutional rights, the decision ignores the fundamental issue permeating unconstitutional conditions jurisprudence: Why should the voluntary waiver of

---

160 See id. at 318.

161 Id. The Court's concern for children has led it to limit important constitutional rights in other circumstances. See, e.g., FCC v. Pacifica Found., 438 U.S. 726, 749-50 (1978) (denying First Amendment challenge to FCC prohibition on broadcast of indecent language based on broadcasting's unique accessibility to children).

162 See *Wyman*, 400 U.S. at 319. The Court compared welfare benefits to private "charity" and stated that one who dispensed such charity would "naturally [have] an interest and [expect] to know how his charitable funds are utilized and put to work." Id.

163 Id. at 319-20 (quoting Note, Rehabilitation, Investigation and the Welfare Home Visit, 79 Yale L.J. 746, 746 (1970)).

164 *Wyman*'s focus on children, read literally, is inapplicable to e-mail monitoring (with the arguable exception of situations where the monitoring is aimed at child pornography) because children, of course, are not employed by the government. The Court's concern for the welfare of children, however, may be read more broadly as an interest in the public welfare. Under such a reading, there may be times when the public does have an interest in monitoring government employees' e-mail. Such cases arise when employees deal with subjects of importance to national security. See infra Part III.B.

Fourth Amendment rights by government employees concern courts? After all, aren't workers themselves in a better position than courts to determine whether a government paycheck is more important than constitutional rights?

Kathleen Sullivan explains why courts should worry when the government attempts to condition employment on the waiver of constitutional rights. She argues that by placing conditions on benefits, the government creates perverse systemic effects on the exercise of constitutional rights.[165] Constitutional rights, such as the Fourth Amendment, do more than simply protect individuals from government authority. Such rights "also help determine the overall distribution of power between government and rightholders generally."[166] Individual workers often lack "both the information and the stake necessary to assess the value of their own exercise of rights to third parties and to the polity as a whole."[167] In the context of workplace e-mail monitoring, government employees will fail to consider that their waiver of Fourth Amendment rights threatens to erode the privacy interests of all employees.[168]

Whether courts would limit broad monitoring policies as unconstitutional conditions is ultimately a difficult question. Courts have required that workplace searches by government employers be found unreasonable before they may be held unconstitutional. The law establishing the contours of Fourth Amendment reasonableness of government workplace searches is discussed in Part III. Part III argues that under existing law a strong case can be made that e-mail monitoring is unreasonable absent either individualized suspicion or "special needs."

III
E-MAIL MONITORING IN THE WORKPLACE CONTEXT: ARE WE BEING REASONABLE?

Determining that the Fourth Amendment applies to e-mail in the government workplace is only the first step in evaluating whether the Amendment places limits on e-mail monitoring. The next step is to examine the standards by which various workplace searches and seizures have been evaluated. The Fourth Amendment has never been held to prohibit all searches and seizures, even where there is a reasonable expectation of privacy. Rather, the Amendment limits

165 See Sullivan, supra note 157, at 1490.

166 Id.

167 Id. at 1491.

168 See Gantt, supra note 20 and Parts I.B.2, I.B.3 (noting impact of federal Fourth Amendment jurisprudence on all sources of workplace privacy protection).

searches by requiring that they be reasonable. For criminal searches, reasonableness usually requires probable cause and a warrant. The standard of reasonableness for searches in the government workplace, however, is less stringent. Most workplace searches are not undertaken to detect criminal activity but are focused on discovering malfeasance in the workplace that does not rise to the level of a criminal violation.

A. *The Fourth Amendment in the Government Workplace:* O'Connor v. Ortega

The different standard of reasonableness for searches in the government workplace has been sketched in a line of cases following the Court's decision in *O'Connor v. Ortega*.[169] Dr. Magno Ortega worked at Napa State Hospital in California, with primary responsibility for training young physicians in psychiatric residency programs.[170] During an investigation of Ortega for alleged moral and fiscal improprieties, hospital personnel entered Ortega's office and seized several items from his desk and file cabinets, including a Valentine's Day card, a book of poetry sent by a former resident, and files containing Medicare billing records.[171] In response to this search and seizure, Ortega filed a civil rights claim under 42 U.S.C. § 1983 alleging that the Hospital had violated his Fourth Amendment rights.[172]

A plurality of the Supreme Court decided the result in *O'Connor*.[173] After noting that government workplace searches did implicate the Fourth Amendment,[174] and acknowledging that Ortega had a reasonable expectation of privacy in his desk and file cabinets,[175] the plurality then articulated instructive standards for determining reasonable expectations of privacy in the workplace. First, the

---

169 480 U.S. 709 (1987).

170 See id. at 712.

171 See id. at 712-13.

172 See id. at 714.

173 Justice O'Connor wrote the opinion for the plurality, which included Chief Justice Rehnquist and Justices White and Powell. See id. at 711. Justice Scalia wrote a separate opinion concurring in the judgment. See id. at 729.

174 See id. at 714 (noting that Fourth Amendment applies to government officials in "various civil activities" and citing New Jersey v. T.L.O., 469 U.S. 325, 334-35 (1985)).

175 See id. at 718. Five members of the Court (the dissenters and Scalia) believed that Ortega had an expectation of privacy in his entire office, see id., while the plurality believed that Ortega had a reasonable expectation of privacy only in his desk and file cabinets and would have remanded the issue as to his entire office. See id. Whether searches of the entire office, or only part of it, were subject to the Fourth Amendment was ultimately unimportant in the case because the searches the Court discussed fell under the protection of the Fourth Amendment under both the plurality's and the dissenters' opinions.

Justices rejected the contention that public employees never have Fourth Amendment rights.[176] The opinion implied, however, that the Fourth Amendment offers less protection against noncriminal searches conducted in the government workplace: "The operational realities of the workplace . . . may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official."[177] Reasonable expectations of privacy can be reduced by "actual office practices and procedures, or by legitimate regulation."[178]

Perhaps the most important aspect of *O'Connor* is the standard of reasonableness it establishes for workplace searches. The plurality articulated a balancing test, weighing "the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace."[179] The plurality then applied the test to decide the "more difficult issue" of whether probable cause should be the appropriate standard for workplace searches.[180] In making this determination, the Justices stated that the context in which the search takes place is of primary importance since there are a "plethora of contexts in which employers will have an occasion to intrude to some extent on an employee's expectation of privacy."[181] According to the plurality, the search of Ortega's office could be classified as either "a noninvestigatory work-related intrusion"[182] or "an investigatory search for evidence of suspected work-related employee misfeasance."[183] In *O'Connor*, the distinction made no difference; balancing various government employer interests against those of employees, the plurality argued that probable cause was an inappropriate standard for either category of workplace searches.[184]

---

176 See id. at 717 ("Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer.").

177 Id.

178 Id.

179 Id. at 719-20.

180 See id. at 722. Probable cause is generally a prerequisite for obtaining a constitutionally-sound search warrant. See U.S. Const. amend. IV; Illinois v. Gates, 462 U.S. 213, 239 (1983) (stating that, in order for warrant to issue, "[s]ufficient information must be presented to the magistrate to allow that official to determine probable cause").

181 *O'Connor*, 480 U.S. at 723.

182 A work-related intrusion takes place, for example, when one employee enters another employee's desk "for the purpose of finding a file or piece of office correspondence." Id.

183 Id.

184 See id. at 724 (concluding that requiring probable cause would "impose intolerable burdens on public employers"). The plurality identified a number of interests weighing against the probable cause standard, including the interest of the government employer in maintaining an efficient workplace, the important functions that government agencies per-

As these "special needs" of the government employer made the probable cause standard impracticable, the plurality held that government workplace searches should be evaluated for constitutionality under a reasonableness standard.[185] In particular, an investigatory search by a supervisor would be justified at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct."[186] The search would be permissible in scope when "'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct].'"[187] These standards for justifying and conducting searches are crucial to applying the Fourth Amendment to workplace e-mail monitoring because monitoring may be considered one of *O'Connor*'s investigations for work-related misconduct.[188]

B. The Importance of Individualized Suspicion

The plurality in *O'Connor* left unanswered a major question about the reasonableness inquiry, one that greatly affects the constitutionality of workplace e-mail monitoring: whether individualized sus-

---

form, the different nature of searches for law enforcement purposes, and the difficulties that the subtleties of the probable cause standard would pose for government employers. See id. at 723-25. Against these interests, the plurality balanced the privacy interests of employees. Such interests "while not insubstantial, [were] far less than those found at home or in some other contexts." Id. at 725. This was because the invasion was relatively limited; employees could avoid invasions by simply leaving items at home. See id.

185 See id. Summarizing their views, the plurality stated:

> We hold, therefore, that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable.

Id. at 725-26.

186 Id. at 726.

187 Id. (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).

188 The other type of search addressed by *O'Connor*, searches for a needed file or piece of correspondence, will usually not take place with e-mail. Digital data stored in files feature physical and temporal attributes different from those associated with paper files. Nearly infinite copies of e-mail messages can be made in a matter of milliseconds, thus reducing the chances that a needed file will be available in only one place. Also, after an e-mail message is sent, a copy is usually left on the sender's computer, again reducing the likelihood that a particular e-mail can only be found by searching through other employees' e-mail. Finally, e-mail monitoring is premised on finding misconduct at work—stopping the dissemination of confidential information, preventing sexual harassment, or catching efficiency-reducing activities—and not on finding stray paperwork.

picion[189] is a necessary component of a reasonable search in the government workplace.[190]

Some commentators have criticized *O'Connor* and its progeny for the amount of latitude they give government employers to search their employees' workstations and belongings, and have concluded that these cases provide little protection against e-mail monitoring.[191] This Note argues that these commentators overstate the point. Their view ignores the fact that in *O'Connor* and its progeny, the searches the courts considered were based either on individualized suspicion or special workplace characteristics, such as national security, which made the searches reasonable.

Although the Court in *O'Connor* did not specifically hold that individualized suspicion or special workplace characteristics were necessary for constitutionally valid searches, subsequent cases have found that these factors play important roles in justifying searches of government workplaces. In *Shields v. Burge*,[192] a police officer objected to a search of his desk by law enforcement officials.[193] Following *O'Connor*, the Seventh Circuit examined the reasonableness of the search. In finding the search reasonable, the court relied on the fact that Officer Shield's employers had information creating individualized suspicion about him.[194] Although the basis for suspecting Shields of illicit activity was "thin," Shields himself did not dispute that the police department possessed enough information specifically about him to remove him from his prior assignment and begin an investiga-

189 Reasonable suspicion has been described in different ways. Justice White wrote that it requires "specific and articulable facts that the area to be [searched] harbors an individual posing a danger to those on the arrest scene." Maryland v. Buie, 494 U.S. 325, 337 (1990). Now-Chief Justice Rehnquist viewed individualized suspicion "as a guard against arbitrary exercise of authority" and wrote that in order to show individualized suspicion, an "officer must articulate some reason for singling the person out of the general population." Ybarra v. Illinois, 444 U.S. 85, 107 (1979) (Rehnquist, J., dissenting).

190 See *O'Connor*, 480 U.S. at 726 ("Because [hospital officials] had an 'individualized suspicion' of misconduct by Dr. Ortega, we need not decide whether individualized suspicion is an essential element of the standard of reasonableness that we adopt today.").

191 See, e.g., Benkler, supra note 1, § 19.3[1] ("The prospects for meaningful constitutional limitation of government monitoring of its employees within such a restrictive framework do not seem significant."); Gantt, supra note 20, at 385 ("[E]mployee monitoring limited to work-related activities or communications almost certainly will not implicate Fourth Amendment protection . . . ."); Steven Winters, Comment, The New Privacy Interest: Electronic Mail in the Workplace, 8 High Tech. L.J. 197, 209 (1993) (arguing that *O'Connor* "implies that courts fashion case law so as to provide public employers with unbridled discretion to monitor E-mail transmissions").

192 874 F.2d 1201 (7th Cir. 1989).

193 See id. at 1202 (describing search of state police officer's desk as part of investigation for possible violations of departmental rules and regulations).

194 See id. at 1204.

tion.[195] The sparse record of wrongdoing which served as the basis for searching Shields's office troubled the court: "It is a close question whether the thin record before us supports the desk search's reasonableness."[196] The decision suggests that without any indication of wrongdoing by Shields, his desk could not have been reasonably searched.

Similarly, in *United States v. Taketa*,[197] investigators searched a Drug Enforcement Administration agent's office because a coworker had notified the office supervisor that Taketa was engaging in illegal activity.[198] This information launched an internal investigation directed at Taketa focusing on uncovering "work-related employee misconduct."[199] The Ninth Circuit found the search reasonable and articulated a standard for searches based on work-related misconduct: "[T]he correct inquiry is whether there was reasonable cause to believe that evidence of employee misconduct was located on the property that was searched."[200]

Schowengerdt v. United States,[201] another Ninth Circuit case, concerned the search of a civilian employee's office at a top-secret naval weapons design plant.[202] Because of the nature of the work and the fact that employees handled large amounts of classified material, "[e]xtensive security precautions [were] taken at the facility."[203] The search of Schowengerdt's office was based on an anonymous tip that the office contained material "of interest to the security department" and specified the location, Schowengerdt's credenza, of the material.[204] Officials searched the credenza and found a manila envelope, marked "Strictly Personal and Private. In the event of my death, please destroy this material as I do not want my grieving widow to read it."[205] The envelope contained evidence of Schowengerdt's participation in an avid extramarital sex life.[206] The court found this search reasonable due to the special nature of the workplace: "[E]mployees were constantly being searched and surveilled for com-

195 See id.

196 Id. at 1205.

197 923 F.2d 665 (9th Cir. 1991).

198 See id. at 668-69. The coworker reported that Taketa had shown her how to illegally alter a pen register, a device that only records the phone numbers a suspect dials, into a device which would illegally intercept entire telephone conversations. See id. at 668 & n.1.

199 Id. at 674.

200 Id.

201 944 F.2d 483 (9th Cir. 1991).

202 See id. at 485.

203 Id.

204 Id.

205 Id.

206 See id.

pliance with security precautions in a manner that would be considered unduly invasive in a more conventional work place. . . . [I]n this peculiarly unprivate work environment, Schowengerdt had no reasonable expectation of privacy in his desk and credenza, locked or unlocked."[207] Although there was individualized suspicion in this case, the court implied that general expectations of privacy could be curtailed this severely in only a few "peculiarly unprivate" workplaces.

Although the courts in all of these cases found workplace searches reasonable, each court required justification greater than that which could generally be offered for most e-mail monitoring. A policy of monitoring e-mail that involves random searches or that includes all employees is not based on individualized suspicion.[208] Unless there are special characteristics of the workplace that justify suspicionless searches, individualized suspicion should remain a requirement.

The importance of either individualized suspicion or special workplace circumstances as grounds for valid searches was demonstrated in a line of Supreme Court cases evaluating the validity of drug tests administered by government officials. In *Skinner v. Railway Labor Executives' Ass'n*,[209] the Court upheld mandatory drug tests for railroad personnel involved in certain types of train accidents.[210] *National Treasury Employees Union v. Von Raab*[211] allowed compelled urinalysis for Customs Service employees who carried guns, were involved in drug interdiction efforts, or dealt with classified documents.[212] *Vernonia School Dist. 47J v. Acton*[213] permitted random drug testing of high school students who wished to participate in school athletic programs.[214] Taken together, these three cases appeared to allow government officials wide latitude to make searches without individualized suspicion. The only apparent requirement was a government claim of some generalized "special need" in order to justify the searches.[215]

---

207 Id. at 488.

208 A broad-based e-mail monitoring policy, especially if conducted randomly or with software such as Assentor, does not target specific employees' e-mail based on individualized suspicion. See supra note 3 (describing Assentor).

209 489 U.S. 602 (1989).

210 See id. at 634.

211 489 U.S. 656 (1989).

212 See id. at 679.

213 515 U.S. 646 (1995).

214 See id. at 664-66.

215 In these cases, the general "special need" articulated by the government was the promotion of public safety by identifying drug users.

The Court's recent decision in *Chandler v. Miller*,[216] however, forces a reevaluation of the scope of *Skinner*, *Von Raab*, and *Vernonia* by narrowing the range of "special needs" justifiably permitting searches without individualized suspicion. In *Chandler*, the Court struck down a Georgia statute requiring candidates for certain state offices to certify that they had taken a drug test and that the results were negative.[217] Justice Ginsburg, writing for the Court, began her analysis by noting that "[t]o be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing."[218] Justice Ginsburg then recognized, however, that this general rule may not be appropriate where special needs other than crime detection are present. In these cases, "courts must undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties."[219] The special need proffered by the state "must be substantial—important enough to override the individual's acknowledged privacy interest, sufficiently vital to suppress the Fourth Amendment's normal requirement of individualized suspicion."[220]

The Court next evaluated Georgia's alleged "special need" against this standard. Georgia contended that the statute was justified because "the use of illegal drugs draws into question an official's judgment and integrity; jeopardizes the discharge of public functions, including antidrug law enforcement efforts; and undermines public confidence and trust in elected officials."[221] The Court, however, disagreed with the state's arguments. Georgia's claimed "special need" lacked a vital component: "Notably lacking in respondents' presentation is any indication of a *concrete danger* demanding departure from the Fourth Amendment's main rule."[222] Georgia officials could not demonstrate that the harms the statute were supposed to address were anything but hypothetical.[223] Additionally, Georgia "offered no reason why ordinary law enforcement methods would not suffice" to fulfill certain goals of the statute.[224]

---

216 117 S. Ct. 1295 (1997).

217 See id. at 1305.

218 Id. at 1301 (citing *Vernonia*, 515 U.S. at 670-71 (O'Connor, J., dissenting)).

219 Id. at 1301.

220 Id. at 1303.

221 Id. The justifications offered by Georgia, and rejected by the Court, are much stronger than most that could be offered to support e-mail monitoring in almost any government workplace; they implicate some of the core features of our system of representative government.

222 Id. at 1303 (emphasis added).

223 See id.

224 Id. at 1304.

The *Chandler* concrete danger requirement apparently can be met in only a few specific ways. In both *Skinner* and *Vernonia* government officials produced concrete evidence demonstrating a localized drug problem.[225] These cases indicate that courts will find a concrete danger when confronted with a demonstrated track record of misconduct in a particular social or professional context.

Although in *Von Raab* there was no history of drug use by Customs Service employees, the Court found another, quite limited,[226] concrete danger in that case's holding. The Customs Service employees' work in *Von Raab* involved drug interdiction efforts, exposing those employees to special dangers.[227] These sensitive assignments meant that the employees and their work product in *Von Raab* could not be subjected to "the kind of day-to-day scrutiny that is the norm in more traditional office environments."[228] *Von Raab* thus stands for the limited proposition that when government employees are engaged in highly sensitive work, suspicionless searches of such employees are reasonable. The concrete danger stems from the great damage this special, limited class of employees can wreak on vital and sensitive government interests.

Chandler would thus appear to require that government officials show a real and substantial risk to public safety in order to establish a special need strong enough to allow searches in the absence of individualized suspicion.[229] Under this standard, e-mail monitoring will rarely be reasonable searching. The only government workplaces that could easily demonstrate such a concrete danger are those that deal with highly sensitive information—primarily intelligence and defense agencies. Where employees deal with issues of national security, as in *Schowengerdt*, the need to search stems from the real harm that disclosure of secret information can cause to substantial national interests.

---

225 See id. at 1301 (stating that *Skinner* drug testing program was adopted "in response to evidence of drug and alcohol abuse by some railroad employees, the obvious safety hazards posed by such abuse, and the documented link between drug- and alcohol-impaired employees and the incidence of train accidents"); id. at 1302 (noting that, in *Vernonia*, there had been "immediate crisis" caused by sharp increase in drug use in school district requiring response by school officials responsible for children's welfare).

226 The *Chandler* Court stated that *Von Raab* is "[h]ardly a decision opening broad vistas for suspicionless searches" and "must be read in its unique context." Id. at 1304.

227 See id. (noting routine exposure of Customs Service employees to organized crime and that employees were frequent targets of bribery).

228 National Treasury Employees Union v. Von Raab, 489 U.S. 656, 674 (1989).

229 See *Chandler*, 117 S. Ct. at 1305 ("[When] public safety is not genuinely in jeopardy, the Fourth Amendment precludes the suspicionless search, no matter how conveniently arranged.")

Most government workplaces would have to prove some other concrete danger in order to legally monitor e-mail under this reading of *Chandler*. They could monitor only if there was a demonstrable history of abuse of e-mail. Such a history would need to involve abuses so widespread and so destructive that the public safety would be deemed at risk. A pattern of misconduct that meets the rigorous *Chandler* standards would no doubt be extremely difficult for a government employer to prove.

CONCLUSION

E-mail monitoring of employees presents a real and growing threat to the privacy of workers. Yet there are no adequate statutory or common law remedies to protect employees from constant, suspicionless searches of their e-mail. The Fourth Amendment can and should be used to protect this increasingly vital form of communication. Although some commentators may currently doubt the applicability of the Fourth Amendment to workplace e-mail monitoring, this Note argues that government employees can demonstrate a reasonable expectation of privacy in their e-mail communications and thus gain the protections of the Amendment.

Under the Fourth Amendment standard developed in this Note, e-mail monitoring may take place only if the government employer can establish individualized suspicion or can demonstrate an adequate "special need" under the standards set down in *Chandler v. Georgia*. The Court's decision in *Chandler* indicates its unwillingness to accept mere platitudes in place of a demonstrable danger when the government seeks to undertake searches in the absence of individualized suspicion. In order to initiate suspicionless monitoring, a government workplace must possess special characteristics that create a concrete danger only addressable through e-mail monitoring. The Supreme Court's change of tenor in *Chandler* should prompt lower courts to examine more critically the justifications put forth for suspicionless searches and become more receptive to using the Fourth Amendment to limit government workplace e-mail monitoring.

When courts hold that the Fourth Amendment protects government employees' e-mail from monitoring, *all* employees will benefit. Federal Fourth Amendment jurisprudence produces ripple effects in other areas of privacy law including state court interpretations of state law and tort remedies. Strengthened by a more robust reading of the Fourth Amendment, these other sources of law will help protect private sector employees from suspicionless intrusions in their workplaces.