COMMENT

THE NEW PRIVACY INTEREST: ELECTRONIC MAIL IN THE WORKPLACE

STEVEN WINTERS †

Table of Contents

---

†Law Clerk to the Honorable Clarence A. Brimmer, United States District Court, District of Wyoming, 1992-1993; J.D., University of Southern California, 1992; M.B.A., Multinational Marketing and Finance, University of Southern California, 1981; B.S., Economics, Philosophy, Northwestern University, 1979. The author thanks Professor Erwin Chemerinsky, Scott Hodgkins, and Noel Shipman for their assistance and input.

> [T]here are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new *noncommon carrier communications services or new forms of telecommunications and computer technology.* This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services. . . .
>
> Most importantly, the law must advance with the technology to ensure the continued vitality of the Fourth Amendment. *Privacy cannot be left to depend solely on physical protection,* or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.[1]

I. INTRODUCTION

At the First Conference on Computers, Freedom & Privacy, Professor Lawrence Tribe proposed a Twenty-Seventh Amendment to the United States Constitution. The purpose of the new amendment is to protect individual privacy rights increasingly threatened by burgeoning computer technology.[2] Tribe and others evidence concern that computer technology has so eroded our privacy that nothing less than a Constitutional Amendment will protect those vanishing rights.

Tribe's call for a new Constitutional Amendment highlights his concern for what he labels as invasions of "cyberspace." "Cyberspace" simply refers to the ephemeral space occupied by computer transmissions and communications. The United States Constitution does not expressly protect an individual from invasions of cyberspace. Courts, too, seem less willing or less able to protect an individual from these electronic invasions.[3] As a result, both our current Constitution and the common law right to privacy are ill-equipped for the voyage into cyberspace.

---

1. S. REP. NO. 541, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 (emphasis added).

2. *See* Henry Weinstein, *Amendment on Computer Rights Urged*, L.A. TIMES, Mar. 27, 1991, at A3.

3. *See, e.g.*, Shoars v. Epson America, Inc., No. SWC 112749 (Cal. Super. Ct. 1990); Flanagan v. Epson America Inc., No. BC 007036 (Cal. Super. Ct. Mar. 12, 1991) analyzed *infra* nn. 150-184 and accompanying text. *See also* Current Developments Section: *Electronic Mail Raises Issues About Privacy, Experts Say*, DAILY LABOR REPORT, Nov. 17, 1992, at A-7; Mitch Ratcliffe, *Privacy Focus of Borland Case*, MACWEEK, Vol. 6, No. 35, Oct. 5, 1992, at 1.

One of the most proliferating forms of "cyberspace" is electronic mail.[4]. Electronic mail is now used by an estimated 20 million people across the United States. More than half of those users went on-line in the past two years.[5] E-mail continues to be the subject of much debate regarding the privacy of its users.[6] The issue of workplace privacy as it relates to computer use and electronic communications is actively before Congress.[7]

This Comment examines what level of privacy employees who use electronic mail systems are entitled to expect. Part II recounts the current court-made and statutory laws which purport to protect employees' workplace privacy. Part II argues that the Supreme Court has poorly fashioned search and seizure law for the public workplace because it continues to rely on a radically outdated view of how the workplace functions. The Supreme Court has created case law which all but eliminates constitutional protection afforded public employees for work-related searches and seizures. Statutes have picked up some of the slack and in some instances protect both private and public employees. However, the statutes also have significant gaps and ambiguities. Part II urges that there are very good reasons to protect private employees who use E-mail in the workplace, not the least of which is that it is in the employer's best interest to do so.[8]

Part III suggests that the best place to find privacy protection for private employees who use computer systems at work is in state constitutions.[9] To this end, Part III analyzes *Shoars v. Epson America,*

---

4. Electronic Mail, often referred to a "E-mail," is a form of communication sent from one computer to anther, much like postal mail is sent from one location to another. However, the privacy protection afforded postal mail far outstrips that currently afforded E-mail. *See* 18 U.S.C. §§ 1708-1710 (1988) (sections concerning theft or receipt of stolen mail matter generally, theft of mail matter by officer or employee, and theft of newspapers). Moreover, unlike postal mail, E-mail reaches its intended recipient almost instantaneously and is subject to all the costs and benefits of using a networked computer system.

5. *See* DAILY LABOR REPORT *supra* note 3.

6. *See, e.g.,* Lory Zottola Dix, *Some Organizations are Defining E-Mail Privacy,* COMPUTERWORLD, Nov. 23, 1992, at 87; Bruce Caldwell, *E-Mail Privacy: A Raw Nerve For Readers,* INFORMATION WK., July 30, 1990, at 52 (the magazine's survey regarding E-mail privacy drew the largest number of responses from readers in the magazine's history); *see also* Don J. DeBenedictis, *E-mail Snoops: Reading Others' Messages May Be Against the Law,* A.B.A.J., Sept., 1990, at 26-27.

7. *See, e.g.,* H.R. REP. NO. 1218, 102d Cong., 1st Sess. §§ 2-7 (1991); Caldwell, *supra* note 6, at 36.

8. *But cf.* O'Connor v. Ortega, 480 U.S. 709, 720-24 (1987). The Court reasoned that the public employer's interests in workplace supervision, control and efficiency justified severely limiting employee privacy.

9. This, of course, assumes state constitutions have a provision protecting a person from private infringements of her privacy similar to that of the California Constitution, Art. I, § 1. *See infra* note 12.

Inc.,[10] a case which is now working its way through the California courts. This Comment contends that the California Superior Court decided *Shoars* incorrectly, both as a matter of law and of policy. Part III extends the *Shoar* analysis to show how state courts might better interpret their respective privacy laws to effect these legal and policy concerns.

In Part IV, this Comment concludes that courts have a special role to play when adjudicating work-related computer privacy issues. This part summarizes the reasons why courts should not blindly defer to legislators when adjudicating technology-related privacy issues.

II. COURT-MADE PRIVACY LAW: WHY FAVOR EMPLOYERS?

The right of privacy appears to be a diverse and growing bundle of rights which derive from four principal sources: The United States Constitution,[11] state constitutions,[12] statutory sources,[13] and the common law.[14] None of these four sources adequately protects an employee's privacy in the computerized workplace. Inadequacies exist because issues of computer privacy do not fit neatly into current Fourth Amendment law. It is true the Fourth Amendment applies only to state actions and therefore protects only public employees. However, Fourth Amendment law as decided by the Supreme Court heavily influences

---

10. *See supra* note 3.

11. The Fourth Amendment reads:

> 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.

12. *See, e.g.*, WASH. CONST. art. I, § 7 (providing that no person shall be disturbed in his or her private affairs). The purpose of this constitutional amendment is to prevent unreasonable searches and seizures and to require a standard of a reasonable expectation of privacy. City of Seattle v. See, 408 P.2d 262 (Wash. 1965), *rev'd on other grounds*, 387 U.S. 541 (1967). Generally, the Washington provision does not apply to private individuals, but government employers are within the purview of the provision. *But cf.* CAL. CONST. art. 1, § 1. California courts have held that private actors are within the purview of the constitution. Wilkinson v. Times Mirror Corp., 264 Cal. Rptr. 194, 199-200 (Ct. App. 1989); *see also* CAL. PENAL CODE §§ 630-632 (Deering 1983 & Supp. 1992) (specifically stating that private communications come within the purview of the state eavesdropping and wiretapping statutes).

13. *See, e.g.*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.) [hereinafter ECPA]; CAL. PENAL CODE §§ 630-632 (Deering 1983 & Supp. 1992).

14. Courts have developed a cause of action for injury based on an invasion of privacy. K-Mart Stores Corp. v. Trotti, 677 S.W.2d 632, 635-36 (Tex. Ct. App. 1984) (court stated that the essence of our right to privacy is our right to be left alone, to live a life free from intrusion and unwanted publicity), *writ refused*, 686 S.W.2d 593 (Tex. 1985); RESTATEMENT (SECOND) OF TORTS § 652 (1977).

both state and federal court interpretations of non-public employee's privacy rights in the workplace.[15]

Generally, a "search" under the Fourth Amendment protects "an expectation of privacy that society is prepared to consider reasonable."[16] The Fourth Amendment further requires that searches[17] must be reasonable in all circumstances. A reasonable search is one where the searcher obtains a warrant based on probable cause. Searches conducted without a warrant are adjudged *per se* unreasonable.[18] However, courts may abandon warrant and probable cause requirements when they become "impractical under the circumstances."[19] Impractical circumstances exist during emergencies, or when the need for either a warrant or probable cause will "frustrate the purpose for which the search was intended."[20] Where a warrant is found to be impractical, the probable cause standard may serve as a reference for adjudicating the search's reasonableness.[21] When the Court decides probable cause is not applicable to analyzing the reasonableness of the search, as an alternative, it may balance the need to search against the invasion of privacy resulting from the search.[22]

Traditionally, employees have received little privacy protection on the job. It is argued that employers' interests should be favored because the work is done on the employers' premises. Employers own the communications equipment used at work and it is the company's business which is being conducted on this equipment. Employers have a strong interest in monitoring employee activity for the purposes of assuring the quality and quantity of work-product, and for protecting against theft or fraud.[23] Even the Supreme Court has decided that the balance on interests should favor employers because public employers' interests in an efficient workplace outweigh the employees' privacy interests.[24]

---

15. *See infra* notes 30-62 and accompanying text (discussion of O'Connor v. Ortega, 480 U.S. 709 (1987), and its effect on subsequent federal court decisions); *see infra* notes 182-84 and accompanying text (the state of California incorporates Supreme Court-made privacy law into its analysis).

16. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

17. Exactly what constitutes a search is unclear. Whether a "search" has occurred seems to turn on some physical invasion the court can observe. *See id.*

18. Keith P. Larsen, Comment, *Governmental Intrusion into the Public Employee Workplace*—O'Connor v. Ortega, 21 CREIGHTON L. REV. 409, 419-20 (1987-1988).

19. *Id.* at 424.

20. *Id.*

21. *Id.* at 425.

22. *Id.*

23. Fred W. Weingarten, *Communications Technology: New Challenges to Privacy*, 21 J. MARSHALL L. REV. 735, 746 (1988).

24. *Ortega*, 480 U.S. at 718-22 (plurality opinion).

The important policy question underlying current work-related privacy law is whether computer technology has so shifted control to the employer that the scales need to be re-calibrated to better protect an employee's privacy rights. Privacy law requires courts to balance the interests of one group against another to determine whether an illegal invasion of privacy has occurred.[25] To this end, scholars have argued that effective judicial balancing ferrets out the needs, interests and limitations of the parties before the court.[26] Implicit within the "ferreting out" are three goals that balancing should accomplish: (1) to justify the appropriate level of generality for the issues before the court; (2) to insure that the result is based on an adequate factual background; and, (3) to not substitute deference for a cogent analysis of the parties' interests.[27] These three goals serve the greater objective of openly and candidly acquiring knowledge and better defining society's values through legal discourse.[28]

Current privacy law neglects these goals. The Supreme Court has inaccurately defined society's privacy values in the workplace because the Court has based its decisions on an outdated view of both the workplace and privacy generally.[29] Lower courts have been left to resolve the tension between the new privacy interests created in the computerized workplace and the Supreme Court's outdated view of workplace privacy.

A. The Seminal Case: *O'Connor v. Ortega*

The seminal case on work-related searches and seizures is *O'Connor v. Ortega*.[30] The *Ortega* case is significant for the way it developed search law rather than for Dr. Ortega's particular claim. The Court held that a reasonableness standard applies to supervisory searches of the workplace of public employees who are subject to supervisory searches of their offices. This reasonableness standard falls short of the stricter requirements of a police investigative search. *Ortega* carved out a special rule for government workplace supervisory searches and reversed prior trends in the case law which had begun to differentiate investigative from

---

25. *See supra* note 15.

26. Frank M. Coffin, *Judicial Balancing: The Protean Scales of Justice*, 63 N.Y.U. L. REV. 16, 38 (1988).

27. *Id.* at 33-39.

28. *Id.* at 41.

29. Justice Blackmun's dissent noted that the changing social landscape of the workplace. *See Ortega*, 480 U.S. at 739-40 nn. 6-7 (Blackmun, J., dissenting).

30. 480 U.S. 709 (1987). For an excellent summary of the case and its holding(s), see Larsen, *supra* note 18; Note, *Fourth Amendment—Work-Related Searches By Government Employers Valid on "Reasonable" Grounds*, 78 J. CRIM. L. & CRIMINOLOGY 792 (1986) [hereinafter Note, *Fourth Amendment*].

non-investigative searches.[31] The holding in *Ortega* suggests that employees in the public sector have little, if any, privacy in the workplace as long as the searches and seizures are work-related.[32] The holding also implies that, notwithstanding statutory protection to the contrary, *private* employees have little, if any, privacy protection in the workplace with regard to work-related searches. Consequently, this case suggests that an E-mail user at a public agency would not be protected from work-related invasions of privacy for work-related reasons under the Fourth Amendment.

In *Ortega,* Dr. Ortega was employed as a psychiatrist at a state hospital. Ortega became subject to an investigation regarding various improprieties including his alleged mismanagement of the hospital's residency program. During the investigation, hospital employees entered and searched Ortega's locked office, where numerous items were seized from Ortega's desk and files. Subsequently, Ortega was fired. Ortega sued the hospital, complaining that the search violated his Fourth Amendment rights. The district court granted summary judgment for the hospital. The Ninth Circuit affirmed summary judgment on Ortega's state claims, but reversed the district court's grant of summary judgment on Ortega's Fourth Amendment claims.[33] On appeal, two issues came before the Supreme Court: (1) whether a work-related search constituted an exception to the warrant and probable cause requirements of the Fourth Amendment, and (2) how courts should balance the competing interests of the agency-employer and the government employee in deciding whether the search was reasonable under the circumstances.

Ortega is worth examining in some detail because it fleshes out many of the limitations of Fourth Amendment law and how those limitations restrict an employee's workplace privacy. In a plurality opinion written by Justice O'Connor, the Court began by noting that Ortega's Fourth Amendment rights would be violated only where the hospital's search infringed on an expectation of privacy society is prepared to consider reasonable.[34] Such an expectation is determined, in part, by: (1) what the framers intended for the Fourth Amendment to protect, (2) how an individual uses a particular location or space (a customary approach), and (3) the Court's view of what areas society desires to protect from governmental invasion (an "objective" standard).[35]

---

31. *See, e.g.,* New Jersey v. T.L.O., 469 U.S. 325 (1985) (deciding whether Fourth Amendment protects investigative search of student's locker at school); Note, *Fourth Amendment, supra* note 36, at 822 n.249.

32. *Ortega,* 480 U.S. at 734-36 (Blackmun, J., dissenting).

33. *Id.* at 714 (plurality opinion).

34. *Id.* at 715. The plurality opinion written by Justice O'Connor was joined by Justices Rehnquist, White and Powell.

35. *Id.*

The Court found that Ortega had a reasonable expectation of privacy in his desk and file cabinets located inside his office.[36] The Court's holding that Ortega maintained an expectation of privacy in his desk followed *Gillard v. Schmidt*[37] where the Ninth Circuit determined that a right to privacy existed in a school counselor's desk. Like the desk in *Gillard*, Ortega's desk contained confidential records and was secured in a locked area. However, Ortega's desk was located in his private office rather than in a shared suite as was the counselor's desk in *Gillard*. The plurality opinion consistently noted that no hospital administrative policies were in force to discourage employees from storing personal items in their desks and files.[38]

Based on two prior Supreme Court decisions, *Oliver v. United States*[39] and *Mancusi v. DeForte*,[40] the plurality recognized Ortega's expectation of privacy. In *Oliver*, employees were found not to have a reasonable expectation of privacy where police searched a field adjacent to Oliver's home. The court distinguished an open field as "usually . . . accessible to the public and the police in ways that a home, an office or a commercial structure would not be."[41] In *Mancusi*, the defendant, DeForte, was a union official under investigation for criminal activities. State officials searched his private office without a warrant and seized union records. The *Mancusi* Court held, *inter alia*, that on the facts, the union official had an expectation of privacy in his office which was protected from the state officials' unwarranted search.

> [I]t seems clear that if DeForte had occupied a "private" office . . . and union records had been seized from a desk or filing cabinet in that office . . . DeForte would . . . expect that he would not be disturbed except by personal or business invitees, and that records would not be taken except with his permission or that of his union superiors. [This] situation was not fundamentally changed because DeForte shared an office with other union officers.[42]

Based on these two precedents, the Court found a reasonable expectation of privacy in the workplace where an employee works for a government employer. However, this expectation was a qualified one:

> 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. Public employees' expectation of privacy in their offices, desks and file

---

36. *Id.* at 719.
37. 579 F.2d 825 (3d Cir. 1978).
38. *Ortega*, 480 U.S. at 719 (plurality opinion).
39. 466 U.S. 170 (1983).
40. 392 U.S. 364 (1968).
41. *Oliver*, 466 U.S. at 179
42. *Mancusi*, 392 U.S. at 369.

> cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.[43]

The plurality's "operational realities" approach found support in *Mancusi*, where the Court suggested that, based on the facts before it, a union employee probably would not have a reasonable expectation of privacy against her union supervisors. Combining *Mancusi* and *Katz v. United States*,[44] the plurality in *Ortega* suggested that some government offices may have no expectation of privacy because they are "so open to fellow employees or to the public."[45]

The three-part inquiry utilized by the plurality to determine Ortega's expectation of privacy probably excludes protection of computer technologies like E-mail. Taken in order, the first part of this inquiry queries whether the framers intended that the Fourth Amendment protect E-mail users. One might argue that framers' intent could be extrapolated to include E-mail. However, such extrapolation more likely serves as a subterfuge for balancing the interests at stake. It would be better to balance the privacy interests openly rather than to artificially connect the Court's reasoning to framers' intent.

In the second part of the inquiry, the Court looks to how an individual uses a particular location or space. The criteria include: (1) whether that which was searched contained confidential records, and (2) whether what was searched was secured in a locked area, or was in a private office. The Court's emphasis on physical location makes it more difficult to apply the law to technologies like E-mail. Surely, E-mail can be regarded as a physical location or a "space." However, regarding it as such does not tell lower courts whether E-mail should be treated as a highly protected space, e.g., postal mail; or as a space which receives less protection, e.g., electronic publishing. The problem is that electronic mail can simultaneously contain confidential and non-confidential records depending on how one defines the "space" being searched. If the "space" includes only one computer file, and that file is confidential, then that which was searched contained confidential records. However, if the space includes more than one file, or includes all that may be accessed by an employee's E-mail code,[46] that which was searched may contain both confidential and non-confidential data. The same kind of definitional problems apply to determining whether E-mail is secured in a locked area

---

43. *Ortega*, 480 U.S. at 717 (plurality opinion).

44. 389 U.S. 347, 351 (1967) (holding that "what a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection").

45. *Ortega*, 480 U.S. at 718 (plurality opinion).

46. Most E-mail systems in the workplace give the employee a code. The code works like a key to a door. An employee's E-mail may be accessed only with this code. Of course, supervisors may have copies of this code.

or is "kept" in a private office. On one hand, an E-mail communication which originates from *any* office, private or not, seems to be confidential. The sender intends that the communication reach only certain recipients. In this sense, E-mail is analogous to postal mail or telephone conversations at work. On the other hand, E-mail could be viewed as a tool provided to employees solely for work-related use. The Supreme Court indicated that employees may not expect privacy where an employer maintains a policy which discourages employees from storing or communicating personal information on E-mail. Thus, focusing on how an employee uses E-mail does not solve the problem, but simply further describes it, because neither the employee nor the employer seems to have well-settled expectations regarding privacy rights in the E-mail context.

The third part of the expectations inquiry relies upon a court's view of what areas society desires to protect from governmental invasion. This part is supposed to be "objective" in the sense that a court objectively analyzes whether society desires to protect users of E-mail in the public workplace from governmental invasion. In *Ortega,* the Court applies this part of the test when it discusses its balancing analysis, reviewed immediately below.

Once a court finds a legitimate expectation of privacy, as it did in *Ortega,* it must analyze the reasonableness of the search under the circumstances. Traditional Fourth Amendment analysis requires that a court first determine whether the case before it should be excepted from the warrant and probable cause requirements.[47] However, in *Ortega,* the plurality moved directly to a balancing test to determine the reasonableness of the hospital's search of Ortega's office, desk and file drawers. The plurality found that a search conducted by a government employer is reasonable where the government's need for supervision, control and efficiency in the workplace outweighs the invasion of the employee's protected privacy.[48] Arguably, had the plurality first looked to whether the search of Ortega's office required an exception to the warrant and probable cause requirements,[49] the Court would have found a need for a warrant and would have affirmed the Court of Appeals' finding in favor of Ortega. Instead, the plurality found that a warrant was not required for two reasons. First, the plurality found that the case law regarding work-related searches of employees' offices favored the government employer's needs and interests.[50] Similarly, in *New Jersey v.*

---

47. Larsen, *supra* note 18 at 434.
48. *Ortega,* 480 U.S. at 719-20 (plurality opinion).
49. *See id.* at 741 (Blackmun, J., dissenting); Larsen, *supra* note 18, at 434.
50. *Ortega,* 480 U.S. at 720-21 (plurality opinion).

T.L.O.,[51] the Court justified a warrantless search by school officials because of the need to enforce "the swift and informal disciplinary procedures needed in the schools."[52] Lower court opinions also suggested that work-related searches by employers generally satisfied the reasonableness requirement of the Fourth Amendment.[53]

Second, the plurality performed its own balancing and found that government employers' interests *generally* outweigh the privacy interests of public employees. The plurality reasoned that employers often enter employees' offices and desks for work-related reasons.[54] An employer or supervisor should not be required to obtain a warrant when entering an employee's office, desk or filing cabinet for work-related purposes where an employer or supervisor desires to complete the government agency's work promptly and efficiently.[55] Here, a warrant would "seriously disrupt [the] routine conduct [of the government agency] and would be unduly burdensome . . . [because] government offices could not function if every employment decision became a constitutional matter."[56]

The plurality also found that probable cause was unnecessary when searching in a work-related context. Ortega maintained that the search was a non-investigatory, work-related intrusion, while the hospital characterized the search as investigatory, its purpose to find evidence of suspected work-related misfeasance. The plurality held that, for the non-investigatory search, "probable cause, rooted as it is in the criminal investigatory context, [does not have] much meaning when the purpose of a search is to retrieve a file for work-related reasons."[57] Likewise, an investigatory search for evidence of work-related misfeasance does not require probable cause because "[t]he delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the [government] agency's work, and ultimately to the public interest."[58] Moreover, "[i]t is simply unrealistic to expect supervisors in most government agencies to learn the subtleties of the probable cause standard."[59] In other words, probable cause is not required for either non-investigatory or investigatory intrusions as long as they are work-related.

---

51. 469 U.S. 325 (1985) (holding that where "special needs" are present, such as in public schools, warrant and probable cause requirements are impracticable).
52. *Ortega*, 480 U.S. at 720 (citing New Jersey v. T.L.O., 469 U.S. 325, 340 (1985)).
53. *Id.* at 720-21.
54. *See infra* notes 63-75 and accompanying text for arguments against this proposition.
55. *Ortega*, 480 U.S. at 722.
56. *Id.* at 722 (plurality opinion).
57. *Id.* at 723.
58. *Id.* at 724.
59. *Id.* at 724-25.

The *Ortega* Court concluded that privacy interests of the public employee are thus outweighed by the government's substantial interests in an efficient and well-run workplace. The employee's privacy interests in the workplace are "far less than those found at home or in some other contexts."[60]

The Court further reasoned that limited employer intrusions, like the one in Ortega's office, do not offend the Fourth Amendment because the sole purpose of government offices is to facilitate agency work—"[t]he employee may avoid exposing personal belongings at work by simply leaving them at home."[61]

The plurality opinion concluded that a standard of reasonableness should be applied where a public employer searches and/or seizes items from an employee's office, desk or file cabinets because both the warrant and probable cause requirements are impractical for work-related searches. Such a search is permissible in both its inception and scope where the measures adopted for the search reasonably relate to the search's work-related objectives; and, given the nature of the employee's alleged misconduct, the search does not excessively intrude on the employee's privacy.[62]

---

60. *Id.* at 725.

61. *Id.*

62. *Id.* at 729-32 (Scalia, J., concurring in the judgment). Justice Scalia wrote a separate concurring opinion. Though he agreed with the plurality's decision to reverse and remand the case, he disagreed with both the plurality's reasoning and with the standard it proffered for Fourth Amendment analysis. Starting with the plurality's standard, Justice Scalia argued that the plurality's case-by-case application of a reasonableness standard "produces rather than eliminates uncertainty" because the standard is essentially void of content. *Id.* at 730. Such a standard is meaningless because it is near impossible to figure how "open" an employee's office must be before a work-related search is reasonable under the circumstances. Based on *Mancusi*, Scalia's concurrence contended that Fourth Amendment protection exists in all offices, public or private.

> There is no reason why this determination that a legitimate expectation of privacy exists should be affected by the fact that the government, rather than a private entity, is the employer. Constitutional protection against unreasonable searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as an employer.

Id. at 730-31.

Moreover, the searcher's identity is not relevant as to whether privacy protection applies, only whether the search of Ortega's office was reasonable. Scalia argued that Ortega's office, and government offices generally, are protected by the Fourth Amendment. Scalia prefers a more "global" analysis of Fourth Amendment protection. This means a higher level of generality. Scalia would hold that Fourth Amendment protection applied to all offices of government employees unless such an office was subject to unrestricted public access. *Id.*

Since Fourth Amendment protection applied here, the case turned on whether the governmental intrusion was reasonable. Justice Scalia contended that *Ortega* is a case where "special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement[s] impractical." Scalia agreed with the result of the plurality's balancing test. Thus, Government searches that were purely work-related, or that purported to investigate workplace misconduct did not violate the Fourth

B. The *Ortega* View Wrongly Eliminates Most Workplace Privacy

The Ortega Analysis suggests that a court view E-mail as a tool provided by employers to be used by employees for work-related communications. This view further implies that courts fashion case law so as to provide public employers with unbridled discretion to monitor E-mail transmissions.

The Ortega analysis is wrong for several reasons. First, the decision probably causes the workplace to run less efficiently. The Ortega plurality seems to assume that employers need almost unlimited access to employees' offices and desks to maintain efficiency. In fact, it is equally likely that increased employee privacy would result in a more efficient workplace.[63] Increased employee privacy sends a positive message from the employer to the employee. That message implicitly states that the employer trusts the employee to be responsible for his or her time and productivity. Such a message fortifies the working relationship between employers and employees and imputes personal dignity into the workplace. Arguably, the employer who regularly intrudes on and monitors its employees' workspace "tear[s] apart the fabric of trust and cooperation that binds companies and their employees."[64] This fabric is a delicate one. At the extreme, an employer who is privy to all intra-company communications creates a workplace filled with distrust. An employee who does not trust his employer has much less of an incentive to be efficient, resourceful and productive.

Ultimately, the Court's view of workplace efficiency wrongly casts the employee as the employer's adversary. This view of work is dysfunctional because it portrays the employee as a dolt incapable of managing his given responsibilities.[65] Successful companies do not treat employees as enemies.[66] Instead, smart managers provide their employees with both personal and professional incentives to perform

---

Amendment. Because the evidence presented in the case was incomplete regarding search's purpose, Scalia agreed that the case should be reversed and remanded. *Id.* at 731.

63. Terry M. Dworkin, *Protecting Private Employees From Enhanced Monitoring: Legislative Approaches*, 28 Am. Bus. L.J. 59, 75 n.92 (1990).

64. Caldwell, *supra* note 6 at 34.

65. The author would also contend that this view of employees becomes increasingly dysfunctional as an employee's responsibilities increase.

66. ERIC G. FLAMHOLTZ & FELICITAS HINMAN, THE FUTURE DIRECTION OF EMPLOYEE RELATIONS 145-63 (1985) (arguing that an organizational leader will be successful if she has a system of beliefs and values in which all employees can participate psychologically); PAUL R. LAWRENCE ET AL., ORGANIZATIONAL BEHAVIOR & ADMINISTRATION: CASES AND READINGS 668, 678 (1976) (organization change which affects those "at the bottom" must actively engage those employees in the change process to be successful); GEORGE RITZER, WORKING: CONFLICT AND CHANGE 232-97 (1977) (arguing that the most pressing psychological problem for many unskilled and semi-skilled workers is alienation; arguing that the most pressing problem for middle managers is threats to their autonomy).

productively.[67] Implicit within the employer-employee relationship is some element of trust. Trust begets teamwork, and teamwork begets productivity. Thus, an employee who has a modicum of workplace privacy probably will work more efficiently than an employee who is constantly looking over his or her shoulder.

Second, unlimited monitoring of employee E-mail transmissions could result in a competitive disadvantage to the employer.[68] Technologies such as E-mail enable immediate and efficient exchange of information. Sharing information enhances workplace productivity and efficient decision-making. However, allowing unlimited work-related monitoring of E-mail provides employees with a disincentive to use E-mail. For example, an employee who might constructively criticize a superior on E-mail might be reluctant to do so knowing her communication was being monitored. Likewise, an employee who wants to make a good impression on his superiors may avoid using E-mail where his communication mixes the personal with the professional. Some minimum protection of E-mail privacy promotes workplace efficiency through information sharing, especially in companies that rely heavily on E-mail as a form of intra-company communication.

Third, the *Ortega* decision takes no account of an employee's personal dignity. Generally, as a society, we agree that a person needs some minimal level of privacy to function with dignity.[69] Why should it be different in the workplace? The Supreme Court's view might make more sense if the employer still legally controlled all of its property under all circumstances.[70] Justice Blackmun, writing for the dissent in *Ortega*, noted substantial evidence indicating that employees are spending an increasing amount of time in the work environment.[71] The more time employees spend at work, the more critical some minimum level of privacy will become. There also exists a substantial body of

---

67. Before the author ventured into law school, he worked from 1982 to 1988 at Bozell, Inc., an advertising agency headquartered in New York. In 1986, as supervisor of Research and Strategic Planning for the Western Division, the author conducted an in-depth analysis of Honda Motor Company for one of the agency's clients. The research revealed that, at every turn in its organization, Honda provided employees with incentives to perform efficiently and creatively. Honda is one of the most financially successful companies in the world— its success appears to be due, in part, to its incentive structure. *See* TETSUO SAKIYA, HONDA MOTOR: THE MEN, THE MANAGEMENT, THE MACHINES 207-10 (1982).

68. This argument is related to the efficiency argument insofar as inefficient companies are at a competitive disadvantage.

69. *See, e.g.*, GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1st Am. ed., Harcourt, Brace & Co. 1949) (1948).

70. *See supra* note 23 and accompanying text.

71. *Ortega*, 480 U.S. at 739. (Blackmun, J., dissenting) (family life and work life intersect increasingly as the combination of two-earner families plus single parents with children increases).

organizational behavior literature which strongly suggests that employees who have privacy at work are more productive as a result.[72] This productivity derives, in part, from the dignity an employee derives from knowing he has a reasonable expectation of privacy.[73] In contrast, the plurality characterized the workplace as purely for the purpose of work where nothing of a personal nature should be kept.[74] The plurality offered no evidence, however, as to why personal belongings should not be kept at work, or how such a rule furthers workplace efficiency. The *Ortega* opinion implies that technologies like E-mail should be given little privacy protection similar to a technology such as an objective data transmitter (e.g., stock price data).[75] For the reasons mentioned above, this Comment urges that E-mail in the workplace should receive privacy protection greater than that implied by the Ortega analysis.

C. How Subsequent Courts Have Deciphered and Applied The *Ortega* View of Workplace Privacy

Unfortunately, it is the plurality's view of the workplace, not the dissent's, which controls the current state of work-related privacy law. To date, a few courts have applied the *Ortega* holding to other fact scenarios. Examining these cases further illustrates how *Ortega* practically eliminates employee privacy in the computerized workplace. Three Circuit court decisions have applied the holding in *Ortega*.[76] These

---

72. *See, e.g.*, FERDINAND D. SCHOEMAN, PHILOSOPHICAL DIMENSION OF PRIVACY: AN ANTHOLOGY 223-44, 403 (1984) (author provides a wonderful summary of various authors' works regarding privacy; specifically, these authors argue that an individual must be able to control personal information to remain dignified); LOUIS HARRIS & ASSOCS. & ALAN F. WESTIN, THE DIMENSIONS OF PRIVACY: A NATIONAL OPINION RESEARCH SURVEY OF ATTITUDES TOWARD PRIVACY 32-41 (1981) (employers should recognize that productivity is tied to workplace privacy); *see also* ALAN F. WESTIN, PRIVACY AND FREEDOM 388-99 (1970) (discussing guidelines on wiretapping and eavesdropping legislation).

73. *See Ortega*, 480 U.S. at 718 (plurality opinion); *see also* ORWELL, *supra* note 69, at 8-20.

74. *Ortega*, 480 U.S. at 725 (plurality opinion).

75. *See* Victoria Slind-Flor, *What is E-mail Exactly?*, NAT'L. L.J., Nov. 25 1991 at 3.

76. There are other decisions which purport to follow the holding. *See, e.g.*, Leckelt v. Board of Comm'rs, 909 F.2d 820 (5th Cir. 1989) (hospital requiring its employees to be tested for infectious diseases did not violate employee's privacy where employer's intrusion for work-related purposes judged by a reasonableness standard); Moxley v. Regional Transit Servs., 722 F. Supp. 977 (W.D.N.Y. 1989) (where Fourth Amendment intrusion serves special government needs, reasonableness of search is determined by balancing governmental interest against employee's privacy interests); American Fed'n of Gov't Employees, Local 1616 v. Thornburgh, 713 F. Supp. 359 (N.D. Cal. 1989) (urinalysis found to be not justified under *Ortega* by balancing employee's right to privacy against government interests which justify intrusion); Bangert v. Hodel, 705 F. Supp. 643 (D.D.C. 1989) (employees do not lose Fourth Amendment protection because they work for the government instead of a private employer); Diaz Camacho v. Lopez Rivera, 699 F. Supp. 1020 (D.P.R. 1988) (work-related searches by government-employer held reasonable where inception and scope of intrusion are reasonable).

are *Schowengerdt v. General Dynamics Corp.*,[77] *Shields v. Burge*,[78] and *Walker v. Darby*.[79] In particular, *Walker v. Darby* is reviewed separately, in some detail, because it is one of the few cases which deal directly with electronic invasions of privacy in the workplace.

1. *EXPECTATION OF PRIVACY*

In *Schowengerdt*, the circuit court held, *inter alia*, that Schowengerdt had a reasonable expectation of privacy in "areas given over to his exclusive use" unless his employer had notified him that his office might be subject to a work-related search on a regular basis.[80] Schowengerdt had alleged that his employer provided no such notification and, consequently, it was not clear the search of his office was work-related. As a result, the circuit court reversed for *Schowengerdt* on the issue of expectation of privacy in Schowengerdt's desk, and remanded regarding the work-relatedness of the search and seizure and the reasonableness of the search under the circumstances.[81]

The *Schowengerdt* court relied on *O'Connor v. Ortega* to decide whether Schowengerdt had an expectation of privacy in his office where his employer did not notify him of possible work-related searches. The Ninth Circuit held that, under *Ortega*, Schowengerdt could have had a reasonable expectation of privacy in his desk, and therefore reversed the district court. The Ninth Circuit found that "all members of the *Ortega* Court agreed that '[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government.'"[82]

The *Schowengerdt* court also noted that eight of the Justices agreed in *Ortega* that some expectations of privacy held by employees may be unreasonable due to the "operational realities of the workplace."[83] While Justice O'Connor, writing for four Justices, contended that an office may be so open as to afford no privacy protection, five Justices disagreed. The *Schowengerdt* court pointed out that Justice Scalia and the four dissenting Justices held that employees' desks, offices and files are protected against unreasonable searches by government employers. Moreover, Justice O'Connor's *Ortega* opinion had argued that public employees' privacy expectations may be diminished by office practices and procedures or by

---

77. 823 F.2d 1328 (9th Cir. 1987).
78. 874 F.2d 1201 (7th Cir. 1989).
79. 911 F.2d 1573 (11th Cir. 1990).
80. *Schowengerdt*, 823 F.2d at 1335.
81. *Id.* at 1336.
82. *Id.* at 1334 (citing *Ortega*, 480 U.S. at 717 (plurality opinion)).
83. *Id.* It was surely wrong for the circuit court to state that eight of the justices in *Ortega* held that some expectations of privacy held by employees may be unreasonable due to the "operational realities of the workplace." *See Ortega*, 480 U.S. at 731-32 (Scalia, J., concurring in the judgment), 735-37, 744-46 (Blackmun, J., dissenting).

legitimate regulation. The *Schowengerdt* court found that pre-*Ortega* rulings supported Justice O'Connor's view even though the remaining five Justices did not embrace or reject O'Connor's contention. Thus, the *Schowengerdt* court concluded that, where an employee is forewarned of an office search for work related purposes, the employee's expectation of privacy diminishes accordingly.[84]

2. *THE REASONABLENESS OF THE SEARCH*

Consistent with its understanding of *Ortega*, the *Schowengerdt* court held that, despite Schowengerdt's reasonable expectation of privacy in his office, a warrantless search of the office would be legal if it were both (a) work-related, and (b) reasonable under the circumstances. Based on *Ortega*, the *Schowengerdt* court defined "reasonable" as follows:

> Ordinarily a search of an employee's office by a supervisor will be "justified at its inception" when there are reasonable grounds for suspecting the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a non-investigatory, work-related purpose such as to retrieve a needed file . . . . The search will be permissible in its scope when "the measures adopted are reasonably related to the objectives of the search as not excessively intrusive in light . . . of the nature of the [misconduct]."[85]

The *Schowengerdt* analysis suggests that a public employee has no privacy on a government E-mail system unless the system is used exclusively by the employees. Such exclusive use could be attained by using a password which only the employee and a network administrator knew.[86] The expectation would diminish accordingly where the employer provided notice of a possible work-related search of the system. Thus, *Schowengerdt* implies that a warrantless search of an employee's E-mail files could be conducted if the search were both work-related and reasonable under the circumstances. Both inquiries appear to be questions of fact.

In *Shields v. Burge*,[87] the Seventh Circuit also elaborated on what constituted a "reasonable work-related" search. Shields was a police sergeant and narcotics investigator for the state. Based on reports that Shields was trafficking marijuana, he was removed from his narcotics beat. Subsequently, an internal investigation of Shields' alleged misconduct was begun. The superintendent of the internal investigation,

---

84. *Schowengerdt*, 823 F.2d at 1334, 1335.

85. *Id.* at 1335-36 (quoting *Ortega*, 480 U.S. at 725 (plurality opinion) (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 (1985))).

86. Jim Nash, *E-mail Lawsuit Cranks Open Privacy Can of Worms*, COMPUTER WORLD, Aug. 30, 1990, at 1.

87. 874 F.2d 1201 (7th Cir. 1989).

Burge, learned that Shields may have tipped off a suspected criminal that the criminal was being investigated by the state. As part of the internal investigation against Shields, two officers working for Burge searched a desk in Shields' office. They also searched Shields' automobile and a locked briefcase in the automobile. The searches were performed without a warrant and without Shields' consent.[88]

During the internal investigation, a special prosecutor appointed by the state court investigated whether Shields had committed any crimes. An indictment was issued, but no convictions resulted. Shields alleged in his complaint that the search of his desk, automobile and locked briefcase violated the Fourth Amendment. The district court granted the government summary judgment on this count because it found the search to be reasonable under *Ortega*.[89] The Seventh Circuit court affirmed, discussing the *Ortega* decision at length.

The *Shields* court found that the plurality's reasonableness standard in *Ortega* governed work-related searches in the workplace. It further outlined two types of interests which supported the search of Shields' desk as reasonable. First, both the government and the public have a strong interest in stopping work-related misconduct by police officers. Second, both the government and the public have an interest in halting drug use and drug trafficking.[90] However, the court applied a different standard to the search of Shields' briefcase.

D. Applying *Ortega* to Searches of a "Hybrid Nature"

The *Shields* court distinguished the search of Shields' locked briefcase from the search of his car and desk. Citing *Ortega*, the *Shields* court noted that the standard for a workplace search is not necessarily the same as the standard applied to searching a briefcase in the workplace area.[91] The search of the locked briefcase was of a "hybrid nature." On the one hand, the search involved a more personal intrusion than just searching a workplace area. On the other hand, the search was justified by the same interests as those justifying a workplace search.[92] The hybrid nature of the briefcase search led the court to discuss significant precedent upon which it set up a continuum of work-related search justifications to which it compared the search of Shields' briefcase.[93]

---

88. *Id.* at 1202.
89. *Id.* at 1202-03.
90. *Id.* at 1204
91. *Id.* at 1207.
92. *Id.* at 1208.
93. Kirkpatrick v. Los Angeles, 803 F.2d 485 (9th Cir. 1986); Security and Law Enforcement Employees v. Carey, 737 F.2d 187 (2d Cir. 1984); Biehunik v. Felicetta, 441 F.2d 228 (2d Cir.), *cert. denied*, 403 U.S. 932 (1971).

One case indicated that strip searches of prison employees to investigate work-related misconduct must be supported by a warrant and probable cause because of the highly intrusive nature of visual body-cavity searches.[94] A second case upheld a "seizure" of police officers for a lineup. The lineup was to determine if any of the officers had been involved in alleged police brutality. In this case, the court stressed the unique interest of the government and the public in police integrity. These interests limited the full privacy and liberty police officials otherwise enjoyed.[95] A final case held that strip-searching a police officer to investigate work-related misconduct violated the Fourth Amendment, absent a reasonable suspicion that the search would turn up evidence of the misconduct.[96]

Compared to these three cases, the court adjudged warrantless search of Shields' briefcase as reasonable. Searching a locked briefcase was less intrusive than a strip search. Moreover, those conducting the internal investigation did have some information indicating that Shields had engaged in misconduct at work. Though this information may not have risen to the level of a "reasonable suspicion," the *Shields* court held that the search's less intrusive nature, the search's work-related nature, and the special interest in police integrity added up to a reasonable search.[97] *The Shields* decision implies that police officers may retain substantially less rights to privacy than other types of public employees. "Some information" of work-related misconduct probably will suffice to make a search reasonable given the public's special interest in police integrity.

Regarding "reasonableness," *Shields* and *Schowengerdt* together suggest that a work-related search of an employee's E-mail may be of a "hybrid" nature, especially where there is no notice given by the employer. A plaintiff would have to characterize the E-mail transmissions at issue as similar to the locked briefcase in Shields' office. Such a characterization would be easier where the employer had no policy stating that E-mail should be used only for work-related matters, and the employee's E-mail files had a private access code known only to the employee and the systems manager. The access code would be analogous to a briefcase lock. Arguably, the more the facts of a given case indicate the employee expected her E-mail transmissions to be confidential, the less likely a court will find that an employer's work-related search was reasonable.

---

94. *Shields*, 874 F.2d at 1208 (citing *Carey*, 737 F.2d at 207).
95. *Id.* at 1208 (citing *Biehunik*, 441 F.2d at 231).
96. *Id.* (citing *Kirkpatrick*, 803 F.2d at 489).
97. *Id.* at 1209.

E. Wiretapping Versus Work-Related Monitoring: *Walker v. Darby*

In *Walker v. Darby*,[98] the court discussed in less detail the holding in *Ortega*. The case is doctrinally different because Walker sued his employer under Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[99] Despite this difference, the case is worth examining in detail because it pointedly addresses issues of wiretapping and the privacy of employee communications in the workplace. Of the three cases discussed, the issues in *Walker* most resemble issues which might arise in the workplace regarding computer technologies such as E-mail.

Walker was a letter carrier in the United States Post Office in Florence, Alabama. Walker was African-American, his supervisors were Caucasian. Walker and other employees believed Walker's supervisors were trying to terminate Walker's employment for race-motivated reasons. Someone warned Walker that his supervisors were monitoring his conversations at his work station. Walker then noticed two objects that looked like intercoms affixed to his workstation. Walker sued his supervisors, Darby and others, for illegal interception of his conversations and invasion of privacy.[100]

The district court granted summary judgment for Darby who was the named defendant for the United States Postal Service. On appeal, the Eleventh Circuit found that, for Walker's claim to survive summary judgment, a court must find that questions of material fact exist regarding: (1) whether Walker's communications were actually intercepted by his supervisors through the use of some device, (2) whether Walker had an expectation of privacy that his conversations would not be intercepted, and (3) if Walker had such an expectation, whether it was justified under the circumstances.[101]

The Eleventh Circuit held in favor of plaintiff Walker based on two key factors. First, the district court believed that a plaintiff could raise an issue of material fact regarding "actual interception" only where he could prove specific contents of a particular conversation were intercepted.[102] The Eleventh Circuit disagreed and held that "actual interception" may be proved without direct evidence because a successful wiretap depends on the perpetrator's ability to conceal the tap.[103]

---

98. 911 F.2d 1573 (11th Cir. 1990).

99. 18 U.S.C. §§ 2510-2521 (1988 & Supp. II 1990). Title III was later amended by the ECPA. *See supra* note 13 and *infra* notes 121-44 and accompanying text.

100. *Walker*, 911 F.2d at 1575.

101. *Id.* at 1577. Note how the "expectation of privacy" standard helps guide the court's analysis. *See supra* notes 15-16 and accompanying text.

102. *Id.*

103. *Id.* at 1578; The *Walker* court cited Awbrey v. Great Atl. & Pac. Tea Co., 505 F. Supp. 604 (N.D. Ga. 1980), and Scutieri v. Paige, 808 F.2d 785 (11th Cir. 1987), where the

Second, the *Walker* court found that questions regarding Walker's expectation of privacy were part of the same inquiry. Walker needed a *subjective* expectation that his conversations would not be intercepted; and, that expectation had to be *objectively* reasonable.[104] The court distinguished this inquiry from determining whether Walker had a reasonable expectation of privacy in his workplace area at the post office.[105]

This distinction was critical to Walker's case. Otherwise, he would be subject to the lower standard of reasonableness for search and seizure outlined in *Ortega.* In *Ortega,* the Supreme Court utilized a balancing test to compare the government's interest as an employer in the workplace against the employee's interest in personal privacy. The balancing test tipped in favor of the employer because supervisors, co-workers and even the public had access to the employee's workplace. In contrast, no such governmental interests tempered the analysis in *Walker.* Walker must have had a subjective belief his conversations would not be intercepted, and that belief must have been objectively reasonable. In other words, another average reasonable person in Walker's situation would have believed his or her conversations would not be monitored under the circumstances.[106]

The *Walker* court pointed out that other Circuits had found that a suit under the anti-wiretapping statute[107] stated a cause of action even absent an expectation of privacy in the Fourth Amendment search and seizure context.[108] For example, an employee may not expect total privacy in her office, but she still would be protected by the anti-wiretapping statute where she was "[unaware] of the specific nature of

---

Eleventh Circuit held that a wiretapping claim may be established by circumstantial evidence.

104. *Id.*

105. *Id.* at 1578 n.7.

106. This distinction may *seem* muddled because Walker's situation at work is going to affect the objective part of the analysis. But it is not hard to imagine a continuum of privacy expectations: on that continuum, concealed wiretapping is "worse" than a search of a person's workplace for work related purposes. Because wiretapping is worse, it does not get the benefit of the balancing test (Title III therefore is more protective than the *Ortega* Court's interpretation of Fourth Amendment protection). Walker's case was even stronger because those tapping his conversations appeared to be racially motivated, and were not acting in their official capacity as Walker's supervisors. If Walker's supervisors had been acting in their "official" capacity, would that make the wiretapping less egregious? This query refers to the intent of the person doing the wiretapping or the work-related search and seizure. One of the key disagreements between the plurality and the dissent in *Ortega* was each side's characterization of the hospital supervisor's intent when searching Ortega's office.

107. The court relied on 18 U.S.C. §§ 2510-2521 (1988 & Supp. II 1990).

108. *Walker,* 911 F.2d at 1578, This point is critical when analyzing the kinds of privacy protection state constitutions might afford employees in the workplace. *See infra* notes 167-73 and accompanying text.

another's invasion of [her] privacy."[109] The *Walker* court concurred with decisions by both the Sixth Circuit[110] and an Illinois district court[111] which distinguished an expectation of privacy from an expectation of non-interception:

> We agree that there is a difference between a public employee . . . [who expects] privacy in [her] personal conversations . . . in the workplace, and [an employee who expects [her] conversations will not be intercepted by a device which allows] those conversations to be overheard inside an office in another area of the building.[112]

The *Walker* court further asserted that Walker's expectation of privacy did not arise out of a legitimate attempt by his employer to police his work-related conduct.[113] Unlike the parties in *Ortega*, Walker argued that his supervisors intended to intercept his conversations based on a personal vendetta, whereas Darby contended that no actual interception took place.[114] Neither party argued that Walker's supervisors were acting in an official capacity.[115] As a result, the *Walker* court reversed and remanded the case based on the inference that "Walker might have expected conversations uttered in a normal tone of voice to be overheard . . . , [but that] he would [not] have expected his conversations to be electronically intercepted and monitored in an office in another part of the building."[116]

Interestingly, the concurring opinion in *Walker* believed that much of the majority's opinion regarding Walker's subjective and objective expectations of privacy was dicta. The concurring opinion reasoned that the district court never discussed these issues and neither party's brief raised the issue. Thus, whether an employee had an expectation of non-

---

109. *Walker*, 911 F.2d at 1579 (citing Bianco v. American Broadcasting Cos., 470 F. Supp. 182, 185 (N.D. Ill. 1979)).

110. Boddie v. American Broadcasting Cos., 731 F.2d 333, 339 n.5 (6th Cir. 1984).

111. Bianco v. American Broadcasting Cos., 470 F. Supp. 182, 185 (N.D. Ill. 1979) (holding that there are circumstances where a person does not have an expectation of total privacy, but can still find protection under the anti-wiretapping statute where he was not aware of another's invasion of his privacy).

112. *Walker*, 911 F.2d at 1579.

113. *Id.* at 1579 n.8.

114. A good example of bad lawyering by the defendant's attorney. Attorneys for Darby should have argued in the alternative that, even if the court found there was interception, it was for work-related reasons.

115. *Walker*, 911 F.2d at 1579 n.8. Note how this case is similar to the mixed motive analysis in employment law. Mixed motive analysis arises in the context of employment discrimination where an employer's actions may have been both legally and illegally motivated. For example, an employer fires an employee with some racially discriminatory motive, but the employer alleges that it would have taken that action against the employee anyway, regardless of skin color. *See* Texas Dep't of Community Affairs v. Burdine, 450 U.S. 248, 252-54 (1981).

116. *Walker*, 911 F.2d at 1579.

interception in his place of work should not have been addressed on appeal until the district court tried the issue.[117]

Ortega, Schowengerdt, Shields, and *Walker,* taken together, suggest two critical points regarding work-related employee privacy. First, federal courts have so narrowly circumscribed the public employee's Fourth Amendment work-related privacy rights that these rights have all but vanished completely.[118] Where an employee is forewarned of an office search, the employee's expectation of privacy diminishes accordingly. These cases show that court-made law favors employers. Second, with an eye to the future, if we think it wise to expand work-related privacy for employees, such an expansion will have to be found in either federal statutes[119] or state constitutions.[120]

F. Congress' Attempt To Better Protect Employees' Work-Related Privacy

There is no federal statute on point which protects computer or electronic communications within a private business organization.[121] To the extent a court might adduce this privacy protection, it would arise under the Electronic Communications Privacy Act of 1986 (ECPA).[122] The ECPA protects users of telephones and other communications equipment from wiretapping and similar invasions of privacy. The Act also includes within its purview electronic mail, cellular phone service, other forms of electronic communication, and a broadened scope which incorporates communications other than those carried over public networks. Under the ECPA, private individuals and organizations may be prosecuted for intercepting electronic communications of outside third parties without authorization to do so.[123] However, the ECPA does not directly address the private business user who communicates by E-mail.

---

117. *Id.* at 1579-80.

118. This idea of vanishing constitutional rights was adapted from an article by Erwin Chemerinsky, *The Supreme Court, 1988 Term—Foreword: The Vanishing Constitution,* 103 HARV. L. REV. 43, 96-98 (1989).

119. *See infra* notes 123-45 and accompanying text.

120. *See infra* notes 146-86 and accompanying text.

121. *See, e.g.,* Alice La Plante, *Is Big Brother Watching?,* INFOWORLD, Oct. 22, 1990, at 58, 60. *But see infra* notes 150-86 and accompanying text.

122. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at scattered sections of 18 U.S.C.). For a good analysis of the ECPA *see* Russell S. Burnside, *The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunications Technologies,* 13 RUTGERS COMPUTER & TECH. L.J. 451 (1987); Robert I. Webber, Note, *The Privacy of Electronic Communication: A First Step in the Right Direction,* 1 J.L. & TECH. 115 (1986).

123. John Pallato, *Congress Closes Gap Between Law and Computer Technology; Computer Crime Prevention,* PC WEEK, Jan. 20, 1987, at 55-56.

Congress passed the ECPA to close loopholes in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[124] These loopholes in privacy protection were created by advancing communications technologies, particularly in the area of computer communications.[125] The important loopholes in Title III, for purposes of this discussion, are threefold: (1) Title III limited privacy protection to narrowly defined categories of "wire" and "oral" communications;[126] (2) Title III protected only against unauthorized "aural interception of voice communications";[127] and (3) Title III did not cover communications between computers, or between a computer and a human.[128]

The ECPA remedied these loopholes. First, the ECPA amended the definitions of "wire" and "oral" in Title III to include the term "electronic."[129] An "electronic communication" specifically includes E-mail.[130] The phrase "electronic communication" is defined broadly and is intended to cover any communication not carried by sound waves, and not carrying the human voice.[131]

Second, Title III was amended to include the words "aural *or other acquisition*."[132] Amending this section allowed Congress to include non-aural, electronic communications within the purview of Title III's protection.[133] The term "intercept" in Title III now includes acquiring the contents of an electronic communication non-aurally, in addition to acquiring a wire or oral communication aurally.[134] For example, using an electronic wiretap to read and store a competitor's computer modem transmissions without consent would violate Title III even though the wiretapping involves no human ear listening.

Finally, the ECPA amended sections 2701 through 2711 of Title III for stored wire and electronic communications. An "outside" or third party may not intercept electronic mail under these sections.[135] The amendments make it criminal for a person to intentionally access an electronic communication without authorization; to go beyond the authorization when accessing the communication; to "intentionally

---

124. 18 U.S.C. §§ 2510-2521 (1988 & Supp. II 1990).
125. *See generally* S. REP. NO. 541, *supra* note 1.
126. 18 U.S.C. § 2511(1)(a) (1988).
127. Burnside, *supra* note 122, at 463.
128. *Id.* at 482.
129. ECPA § 101(c)(1)(A), 100 Stat. at 1851 (modifying 18 U.S.C. § 2511(1)(a) (1988)).
130. S. REP. NO. 541, *supra* note 1, at 14.
131. Burnside, *supra* note 122, at 495 (quoting 1986 U.S.C.C.A.N. at 3568).
132. 18 U.S.C. § 2510(4) (1988) (emphasis added).
133. Burnside, *supra* note 122, at 502.
134. 18 U.S.C. § 2510(4) (1988).
135. Burnside, *supra* note 122, at 509.

obtain" a communication; or, to alter or prevent authorized access to a communication.[136]

With regard to "electronic communications," particularly electronic mail, courts have not yet applied the ECPA.[137] However, recently, in Colorado Springs, Colorado, an interesting issue regarding E-mail privacy surfaced. The city's mayor admitted he had read hard-copy printouts of electronic mail messages sent between City Council members.[138] The mayor felt he had a right to read the E-mail, since state laws demand that most City Council business be conducted in public. Furthermore, the city's E-mail policy required a secretary to print out all E- messages periodically, then delete them from the city computer to save space. The printouts were retained in case any of the messages were deemed covered by the state's broad public-records law. City officials did post official notices in the Colorado Springs computer message system because the system was partially open to the public. The mayor claimed he intended to review these E-mail printouts to insure government employees were performing their jobs in a forthright manner. The city officials would never have kept the printouts had they thought their actions criminal. In fact, he thought his actions were legal because of the state's public-records laws.[139]

Applying the ECPA to the facts, the mayor's actions come within the purview of the Act because he is an "outside" or third party who is a public actor. Inadvertent interceptions by third parties are not crimes under the ECPA because amended sections 2510 and 2511 of Title III require that the actor's *mens rea* be "intentional."[140] The legislative history of the subsection reveals that Congress desired that the wiretapper's conduct or his causing a certain damaging result from wiretapping must be the wiretapper's "conscious objective."[141] Arguably, the mayor did not have the conscious objective of causing a damaging result to those employees whose E-mail he read. On the other hand, he

---

136. 18 U.S.C. § 2701(a)(1)-(2) (1988); Burnside, *supra* note 122, at 509.

137. Courts have applied the ECPA to cases involving cellular phone service. *See, e.g.*, Schubert v. Metrophone, Inc., 898 F.2d 401 (3d Cir. 1990) (cellular phone service providers who do not encrypt or otherwise protect cellular phone transmissions held not to have "intentionally" divulged contents of cellular phone communications, and therefore not liable under ECPA); Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989), *cert. denied*, 493 U.S. 1022 (1990) (interception of incriminating cordless phone conversation by citizen not illegal under ECPA); Edwards v. State Farm Ins. Co., 833 F.2d 535 (5th Cir. 1987) (listener who overheard incriminating cordless phone conversation on his radio scanner and reported contents of conversation to federal investigators not liable under ECPA).

138. DeBenedictis, *supra* note 6, at 26; *see also* Rob Kolstad, *Daemons and Dragons: Mail Privacy, Electronic Mail*, UNIX REVIEW, Vol 10, No. 8, at 79-81 (Aug. 1992).

139. DeBenedictis, *supra* note 6, at 27.

140. S. REP. NO. 541, *supra* note 1, at 3577. Interestingly, for civil actions, the state of mind required may be something less than intentional, "with a knowing or intentional state," 18 U.S.C. §§ 2511-2512 (1988).

141. S. REP. NO. 541, *supra* note 1, at 3577.

did intend to intercept the E-mail communications, and that action in itself may constitute a harm.[142]

Courts have held that states may enact broader privacy protection than that required by the ECPA. Where state protection against wiretapping or eavesdropping is less stringent than the ECPA, federal law controls. However, where state law is more stringent, a potential offender is subject to the higher standard.[143] State law is pre-empted only where it is more permissive than federal law.[144] This point is critical when considering whether state law might provide broader privacy protection than its federal counterpart. Under the ECPA, states may enact broader privacy protection in the workplace should they see fit to do so.

It bears repeating that current federal law does not directly cover the situation where a private employer wiretaps or monitors employee E-mail transmissions. Instead, the ECPA appears to focus on "third party" interception. This focus provides some proof that Congress enacted the ECPA because it was principally addressing the problem of a company's stealing valuable electronic information from its competitors. Yet, nothing in the legislative history of the ECPA clearly suggests that Congress did not intend the ECPA to cover a private employer's monitoring of an employee's E-mail transmissions.[145]

III. STATE LAW: LOOKING FOR BROADER RIGHTS TO WORK-RELATED COMPUTER PRIVACY

The best chance for protecting private employees who use E-mail lies in the area of state law. Many states have enacted criminal and civil statutes which appear to protect user-privacy on technologies like E-mail.[146] Also, many of the highest state courts have interpreted their respective state constitutions to provide broader privacy protection than the Federal Constitution.[147] To this end, all of the cases filed in this area

---

142. No court has addressed the issue of whether the requisite intent is a desire for a damaging result, or simply intentional monitoring.

143. United States v. Marion, 535 F.2d 697 (2d Cir. 1976) (government lost argument that less stringent state law wiretapping statute controlled); 18 U.S.C. §§ 2516(2), 2517(5) (1988).

144. People v. Jones, 106 Cal. Rptr. 749 (Ct. App.) (holding that Congress intended states to supplement federal law in this area; federal law should serve as the minimum standard), *appeal dismissed*, 414 U.S. 804 (1973).

145. *See infra* notes 166-69, 178-80 and accompanying text.

146. *See, e.g.*, CAL. PENAL CODE §§ 630-632 (Deering 1983 & Supp. 1992).

147. *See, e.g.*, Immuno A.G. v. Moor-Janowski, 567 N.E.2d 1270, 1278 (N.Y.) (protection afforded by free press and speech provisions in New York Constitution is broader than minimum protection afforded by federal Constitution), *cert. denied*, 111 S. Ct. 2261 (1991); Hope v. Perales, 571 N.Y.S.2d 972, 978 (Sup. Ct. 1991) (due process clause of New York Constitution provides broader protection than analogous federal provision).

thus far have been pinned to privacy rights articulated in state constitutions or state statutes.[148]

Experts predict that "whatever California courts decide will probably be a model for the nation."[149] Currently, the critical case in California is *Shoars v. Epson America, Inc.*[150] In *Shoars*, the plaintiff was employed as an Office Systems Programmer Analyst in the Information Resources Department at Epson America, Inc. Her responsibilities included providing user support and training in office automation software and personal productivity tools with special emphasis on supporting Epson's employees in the use of electronic mail. About seven hundred Epson employees had desktop computers which, through electronic mail, created access to approximately nine million other computers worldwide. E-mail was presented to Epson employees by Epson management as an alternative to FAX, telephone and U.S. mail. All of Epson's E-mail users needed a personal password to access their own messages.

Plaintiff's direct supervisor systematically printed up and read all of the E-mail that was entering and leaving Epson's place of business where plaintiff worked. Plaintiff's supervisor accomplished this monitoring by placing a "tap" on the electronic mail gateway where the mainframe computer interfaced with the outside E-mail communications service. The tap automatically downloaded and printed up every private communication entering or leaving the office.

Plaintiff, as part of her job description, had been informing Epson employees that their E-mail transmissions were confidential. She also believed that no one in Epson had given her supervisor consent to read the transmissions. Plaintiff entered the unlocked office of her supervisor while he was on vacation and discovered that the tap was in place, and that her supervisor had printed up thousands of pages of employee E-mail. Plaintiff subsequently confronted her supervisor and demanded that he dismantle the tap and destroy the printed up messages. Plaintiff's supervisor advised plaintiff the tap was not her business and threatened

---

148. To the author's knowledge, the cases filed so far are as follows: Cubby v. Compuserve, 90 Civ. 6571 (N.Y. Sup. Ct. filed 1991) (electronic gossip column sued for libel under state law); Cameron v. Mentor Graphics, No. 716361 (Cal. Super. Ct. filed Nov. 7, 1991) (employer sued under state law for wrongfully firing plaintiffs based on information it gained while monitoring plaintiffs E-mail communications); Bourke v. Nissan Motor Co., Inc., No. YC 003979 (Cal. Super. Ct. filed 1991) (plaintiffs sue employer under state law for wrongful termination based on information gained by the employer while monitoring E-mail transmissions); and Shoars v. Epson Am., Inc., No. SWC 112749 (Cal. Super. Ct. filed 1990) (plaintiff suing employer for wrongful termination under state statute where employer obtained information by accessing plaintiff's E-mail communications).

149. Slind-Flor, *supra* note 75, at 22.

150. Ruling on Submitted Matter, Flanagan v. Epson Am., Inc., No. BC007036 (Cal. Super. Ct. 1991).

to fire her if she did not keep quiet about her discovery. In turn, plaintiff, using the E-mail at work, sent a private message to the Manager of Network Software and E-Mail Administrator at Epson's Santa Clara office, requesting that he issue her a new E-mail account number, one to which plaintiff's supervisor would not have access. Plaintiff's supervisor intercepted the transmission, and fired plaintiff shortly thereafter for gross insubordination.[151]

Plaintiff sued Epson under California Penal Code section 631 which provides a private right of action for wiretapping in the workplace.[152] Section 631 prohibits "[a]ny person who by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electronically, acoustically, inductively or otherwise." The section requires consent from all parties before a communication may be tapped. Section 631 also states that a person may not "read or attempt to read [the communication], . . . learn the contents or meaning of any message, report or communication

---

151. Second Amended Complaint at 6, Shoars v. Epson Am., Inc., No. SWC 112749 (Cal. Super. Ct. 1990).

152. CAL. PENAL CODE §§ 630-632 (Deering 1983 & Supp. 1992).

Most states have statutes similar to that of California's. *See, e.g.*, CONN. GEN. STAT. ANN. §§ 53a-187-189 (West 1992); GA. CODE ANN. §§ 16-11-66 through 69 (Harrison 1993); KAN. CRIM. CODE ANN. §§ 21-4004 through 4006 (Vernon 1992); MICH. COMP. LAWS ANN. § 750.539d (West 1992); 18 PA. CONS. STAT. ANN. §§ 5705-5748 (1993). The legislative intent of these statutes is to provide private employers and employees with some protection regarding the intercepting and wiretapping of private communications in the workplace. These statutes differ. Some require one-party consent while others require all-party consent where a communication is being tapped. About half the state statutes provide for civil liability in addition to criminal. Criminal fines range from $500 to $150,000 and sentences range from one to seven years.

Before *Ortega* was decided in 1986, courts generally held that the employer owned all property in the workplace and therefore, had a right to examine that property at any time. It followed that employers had the right to search work areas, desks, lockers or other property to obtain evidence of theft, to prevent diversion of goods, or to prevent illegal drugs on the premises. No search warrant was needed except in criminal cases where constitutional warnings and precautions had to be followed. The employers' major limitation was that they were not permitted to search those areas where an employee has a reasonable expectation of privacy.

However, as early as 1984, some courts began to chip away at this rule. For example, in K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984), *writ refused*, 686 S.W.2d 593 (Tex. 1985), an employee used a company locker for personal storage. She kept her own lock and gave no key to her employer. The Texas court upheld a finding of damages for the employee on evidence that the employer wrongfully searched the employee's locker and purse. The court stated that the employee had an expectation of privacy for the locker and its contents. This expectation was based on the fact that the company allowed the employee to put her own lock on the locker. The court further held and reversed and remanded (in favor of K-mart) for the judge's failure to instruct the jury that, in the workplace, to constitute an invasion of privacy, it must be "highly offensive to the reasonable person." *Id.* at 636.

while the same is in transit or passing over any such wire, line or cable, or is being sent from, or received at any place within the state."[153]

Section 632 proscribes intentional eavesdropping on a confidential communication using "any electronic amplifying or recording device" without the consent of all parties involved. Eavesdropping is illegal "whether the communication is carried on among such parties [in person] . . . or by means of a telegraph, telephone or *other device*"[154] (emphasis added). Interestingly, in section 632(b), the code defines the term "person" to include individuals as well as businesses.[155]

> Section 632(c) states that a confidential communication includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires [that] it be confined to the parties [who are communicating at the time], but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.[156]

Although sections 631 and 632 describe the use of similar equipment which intercepts private communications, the *manner* in which the equipment is used has been distinguished by the California state courts. In *People v. Ratekin*,[157] a California court of appeals held that wiretapping meant intercepting communications by an unauthorized connection to the transmission line. In contrast, eavesdropping meant intercepting a communication by using equipment not connected to a transmission line. Thus, the cause of action in *Shoars* was brought under section 631 because defendant Epson physically placed a "tap" on the electronic mail gateway

---

153. CAL. PENAL CODE § 631(a) (Deering 1983 & Supp. 1992). Violations of section 631 entitle the plaintiff to money damages. This damage provision is important where a plaintiff, like Shoars, files a class-action suit.

154. Section 632(a) states that

> [e]very person who, intentionally and without consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication . . . shall be punished by a fine not exceeding $2500, or imprisonment in county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

Id. § 632(a).

155. It is not clear whether this definition of "person" in § 632(b) applies to the term "person" in § 631(a).

156. CAL. PENAL CODE § 632(c) (Deering 1983 & Supp. 1992). Two recent cases in which § 632 has been applied to plaintiffs' benefit are People v. Gibbons, 263 Cal. Rptr. 905 (Ct. App. 1989) (the crime of eavesdropping is not limited to covert recording of oral communications, but extends to the recording of other forms of communication); and Frio v. Superior Court, 250 Cal. Rptr. 819 (Ct. App. 1988) (a communication may be "confidential" for purposes of § 632 even though it relates solely to ongoing business matters between a business person and his client).

157. 261 Cal. Rptr. 143 (Ct. App. 1989)

where the mainframe computer interfaced with the outside E-mail communications service.

Arguably, Shoars might have had a stronger case if she could have brought a cause of action under section 632. Section 632(c)'s "reasonable expectation of privacy under the circumstances" standard weighs in plaintiff's favor where Epson represented that E-mail was a confidential form of communication to the employees. Unfortunately, Epson's "listening in" on employees' E-mail transmissions involved a physical tapping of an electronic line as opposed to equipment not connected to a line. However, under section 630, the California legislature's strong statement of intent to broadly apply sections 631 and 632 to "new devices and techniques [used] for the purpose of eavesdropping on private communications" might encourage a court to apply the reasonable expectation standard articulated in section 632 to causes of action under section 631.[158] Furthermore, recovery of monetary damages are allowed for violations under sections 630 to 632. The damages are three thousand dollars per violation or three times the amount of any actual damages sustained by the plaintiff. Injunctive relief is also available.[159]

Thus far in *Shoars*, the Superior Court of California sustained Epson's demurrer by reason of plaintiff's failure to state sufficient facts on which a cause of action may be based. The court found that E-mail was not covered by section 631 of the California Penal Code for three reasons. First, the court contended that it was not clear plaintiff had an expectation of privacy. Without such an expectation, there could be no invasion of that privacy through wiretapping. The superior court did not elaborate on this statement.[160]

Second, the court assumed, and found *arguendo*, that even if plaintiff had an expectation of privacy, E-mail was not covered by section 631 based on the California Supreme Court's interpretation of section 631 coverage in *Ribas v. Clark*.[161] In *Ribas*, Ribas and his wife were obtaining a divorce. Ribas's wife had Clark monitor a critical telephone conversation regarding the couple's divorce. Ribas's wife later used this information to

---

158. CAL. PENAL CODE § 630 (Deering 1983). Section 630, which applies to both sections 631 and 632, is a statement of legislative intent. It is a strong statement which declares that

> advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

159. *Id.* § 637.2.

160. This claim probably refers to the court's presumption that the employer's interests in an efficient, well-run workplace outweigh whatever privacy interests the employees have vested in their use of E-mail. This explanation, though, is purely speculative.

161. 696 P.2d 637 (Cal. 1985).

try to rescind the divorce. Ribas sued Clark for an invasion of his privacy under section 631. The California Supreme Court held, *inter alia*, that section 631 covers intra-spousal wiretapping and eavesdropping.[162]

Third, the court in *Shoars* held that section 631 did not cover interception of E-mail communications despite the broad statement of intent offered by the California legislature in section 630 of the California Penal Code.

> Given this three-part analysis, the superior court concluded that, Although it may well be that plaintiff's right to privacy with respect to the electronic communications described in the complaint ought to be, as a matter of public policy, entitled to protection, this court believes that such an extension of Penal Code § 631, if it is to be made, is the proper province of legislature, which is better equipped than a court to determine the precise nature of such an extension, as well as appropriate exceptions and exemptions therefrom. In this connection, the court notes the U.S. Congress has enacted separate statutes pertaining to Wire and Electronic Communications Interception and Interception of Oral Communications [18 U.S.C. § 2510, *et seq.*] and pertaining to Stored Wire and Electronic Communications and Transactional Records Access [18 U.S.C. § 2701, *et seq.*][163]

In a footnote to the above conclusion, the court cited an article which discusses the ECPA.[164] The court's footnote quoted liberally regarding the background and purpose of the ECPA, concluding that

> under section 2701, although it may be illegal for others to gain access without authorization or to exceed authorized access to a system [under the ECPA], "the person or entity providing a wire or electronic communications service" is not liable for any offenses regarding stored communications, i.e., voice-mail, E-mail, or other recorded communications.[165]

In other words, there simply is no ECPA violation if "'the person or entity *providing* a wire or electronic communications service' intentionally examines everything on the [electronic mail] system."[166]

There are several problems with the trial court's ruling in *Shoars*. First, the trial court concluded it was not clear plaintiff had an expectation

---

162. *Id. See also* Thompson v. Dulaney, 970 F.2d 744 (10th Cir. 1992) (finding no interspousal exception to wiretapping statute). The reader might wonder why the superior court cited this case in support of a "narrow" reading of § 631 which excludes within its purview E-mail. *See infra* notes 170-84 and accompanying text for a critical discussion of the superior court's holding in *Shoars*.

163. Ruling on Submitted Matter at 4, Flanagan v. Epson Am., Inc., No. BC 007036 (Cal. Super. Ct. 1991).

164. *Id.* at 5-6 n.1 (citing Ruel T. Hernandez, Note, *Electronics Communications Privacy Act of 1986 and Online Computer Privacy*, 41 FED. COM. L.J. 17 (1988)).

165. *Id.* at 5-6 n.1; 18 U.S.C. § 2701(c)(1) (1988).

166. Ruling on Submitted Matter at 5-6 n.1, *Flanagan*.

of privacy on the employer's electronic mail system. This conclusion completely ignored the reasoning employed by the Eleventh Circuit in *Walker v. Darby*.[167] Recall that in *Walker* the court concurred with decisions by both the Sixth Circuit and a state district court which distinguished an expectation of privacy from an expectation of non-interception.[168] Further, the court held that an expectation of privacy is not required in order to find an expectation of non-interception.[169] The *Shoars* court completely ignored this distinction,[170] and instead pre-emptively concluded that the controlling question was whether plaintiff had an expectation of privacy.

The reasoning in *Walker* suggests that a plaintiff may sustain a cause of action under the California Penal Code anti-wiretapping statute even absent an expectation of privacy under a Fourth Amendment analysis. The plaintiff in *Shoars* may not have expected total privacy in her office, but she is still protected by the anti-wiretapping statute where she is *unaware* of the specific nature of another's invasion of her privacy. Under this reasoning, an employee who expects privacy in her personal conversations in the workplace may be distinguished from an employee who expects that her E-mail conversations would not be intercepted by a device which allows those (electronic) conversations to be monitored inside an office in another area of the building.[171]

Shoars could argue that her supervisors intended to intercept her E-mail conversations because she had discovered that her supervisor was acting contrary to company policy. Recall that Shoars had informed Epson employees that their E-mail transmissions were confidential. She also believed that no one in Epson had given her supervisor consent to read the transmissions. This belief probably satisfies the objective prong of the standard articulated in *Walker*.[172] When Shoars discovered the electronic tap, she confronted her supervisor, and demanded that he dismantle the tap and destroy the printed up messages. Shoars' supervisor threatened to fire her if she revealed what she had found. Hence, it appears Shoars was fired because she discovered her supervisor covertly and thus illegally reviewing employee E-mail.

In contrast, the defendant in *Shoars* could distinguish *Walker* by arguing that Shoars' supervisors are private actors who were attempting

---

167. 911 F.2d 1573 (11th Cir. 1990).

168. *See supra* notes 110-112 and accompanying text.

169. 911 F.2d at 1579.

170. While California courts may choose not to adopt the reasoning of federal courts, the *Shoars* court simply chose to ignore the issue.

171. *Walker*, 911 F.2d at 1579.

172. *Id.* at 1578-79. Shoars must have had a subjective belief her electronic conversations would not be intercepted, and that belief must have been objectively reasonable.

to police her work-related conduct.[173] Shoars' supervisors, as part of a private business, were acting in an official capacity by reviewing E-mail communications. Thus, the *Walker* analysis should not apply in *Shoars* because (1) Walker's arguments were made pursuant to the ECPA which does not cover *private* actors, and (2) the monitoring was work-related.

At least the *Shoars* trial court should have addressed the expectation of privacy issue based on the inference that Shoars would not have expected her electronic conversations or other employees' transmissions to be electronically intercepted or monitored by her supervisor in his office. The distinction articulated by the *Walker* court could be utilized to bring Shoars within the purview of California's anti-wiretapping statute because the statute clearly covers private actors.

The second problem stems from the court's reliance on *Ribas v. Clark*[174] The *Shoars* Court cited *Ribas* in support of a "narrow" reading of section 631 excluding E-mail from the statute's purview. A careful reading of *Ribas* reveals that this case does not support the trial court's conclusion. In *Ribas*, the California Supreme Court cited favorably the legislative intent in section 630 of the California Penal Code, writing that

> [t]his philosophy [to broadly protect citizens against invasions of their privacy] appears to lie at the heart of virtually all the decisions construing the Privacy Act (citations omitted). Section 631 was aimed at one aspect of the privacy problem . . . .[175]

The *Ribas* court went on to hold that

> section 631 [prohibits] far more than illicit wiretapping (citations omitted), [In past cases] we considered [section 631] to proscribe three separate acts: (1) intentional wiretapping, (2) willful attempts to learn of the contents of the communication in transit, and (3) attempts to use or publicize information obtained in either manner (citations omitted). Additionally, the Privacy Act has long been held to prevent one party to a conversation from recording the conversation without the other's consent.[176]

The Ribas court further noted that secret monitoring denies the speaker the important right to control the nature and extent of how the speaker's statement is disseminated.[177]

It is difficult to understand how plaintiff's cause of action in *Shoars* does not fit into either the second or third proscriptions articulated by the California Supreme Court in *Ribas*. Under the second proscription, Epson's interception of employee's E-mail constitutes a willful attempt by Shoars' employer to learn the contents of a confidential communication.

---

173. *Id.* at 1579 n.8.
174. 696 P.2d 637 (Cal. 1985).
175. *Id.* at 640 (citations omitted).
176. *Id.* (citations omitted).
177. *Id.* at 640-41.

Under the third proscription, using the intercepted transmissions to fire Shoars is an attempt to use or publicize information obtained through interception. Thus, the actual text in section 631, the legislative intent articulated in section 630, and the opinion of the California Supreme Court in *Ribas* combine to strongly favor placing E-mail communications within the protection of section 631.

Third, the Superior Court employed a flawed rationale in its ruling by alluding to the ECPA in support of its conclusion that E-mail is not covered under section 631. This analogy to federal law proves uninformative. Nowhere in the ECPA's language, nor in its legislative history, is state law mentioned. It is at least equally likely that federal legislation serves as a floor for privacy protection, not as a ceiling; and therefore states are free to enact stricter privacy laws. Moreover, section 631, with its broader legislative intent, should not be limited in scope simply because the ECPA, a federal statute, does not cover a private employer's intentional monitoring of its employees' communications. In fact, it is not clear that even the ECPA bars suits by private employees against surreptitious employer monitoring of E-mail communications. The legislative history for section 2701(c)(1) of the ECPA[178] states that "it is not a violation of [the ECPA] if the conduct *was authorized* by the person or entity providing the wire or communications service, or if the conduct *was authorized* by the user of that service with respect to communications of or *intended for* that user."[179]

In *Shoars*, management represented to the employees that E-mail communications were confidential. Under the ECPA, whether Shoars' supervisor "was authorized" to monitor E-mail transmissions appears to be a triable issue of fact. Likewise, whether employees' E-mail was "intended" for Shoars' supervisor also appears to be an issue of fact.

Furthermore, it is not clear from the ECPA or its legislative history that "a person or entity" providing E-mail service is synonymous with the employer or a supervisor within the company. Many companies purchase their E-mail services from an outside supplier.[180] Technically, this outside supplier "provides" the E-mail service to the employer. The employer, in turn, provides the E-mail service to the employees. The specific language of the ECPA does not equate "employer" with "E-mail provider." It is at least equally likely Congress intended to impose employer liability where a supervisor covertly monitored employee

178. Section 2701(c) lists exceptions to the crime of unlawful access to stored communications, i.e., it explains when an employer or other person may lawfully access electronic communications.

179. S. REP. NO. 541, *supra* note 1, at 36 (emphasis added).

180. For example, MCI supplies such a service.

E-mail communications which were represented to employees as confidential.

The *Shoars* court's reluctance to allow a cause of action under section 631 for intercepting E-mail communications probably turned on the fact that the actual language of section 631 never mentions the magic words "electronic mail." But, excluding E-mail from the coverage of the section ignores the legislative intent of section 630, and misreads the California Supreme Court's broad interpretation of privacy protection presented in *Ribas v. Clark.*

State courts should hold that electronic mail is within the purview of a state's anti-wiretapping or anti-eavesdropping statutes where: (1) the legislative intent of the statutes supports such a reading, or (2) the state courts have implied such a reading, despite the fact that the actual state statute does not mention the actual words "electronic mail." The *Shoars* trial court erred because both elements (1) and (2) were present. Neither the Constitution nor federal statutes afford such protection to private employees. Including electronic mail within the purview of state statutes like section 631 is not only consistent with the state's interest in employment law, but is also consistent with the trend toward giving private employees more privacy protection.[181]

We know that Congress did not amend Title III of the ECPA until technological advances made Title III obsolete. State courts should not exclude E-mail from the purview of their analogous state statutes simply because those statutes neglect to mention the words "electronic mail." Such a narrow reading of state statutes effectively resolves the issue in favor of employers by ignoring state legislative intent. States have as much an interest in protecting employees as they do in employers. Based on the superior court's holding in *Shoars,* sections 630 and 631 may require amendments to specifically include forms of communications like electronic mail. Certainly, this is an issue with which the state court will have to grapple if *Shoars* is appealed.

On appeal, should a California court find that Shoars is protected under sections 630 and 631, it would not be the first time California courts have found that state law provides broader privacy protection than comparable federal law. In *Hill v. NCAA,*[182] the California Court of Appeal held that the NCAA violated student athletes' right to privacy by requiring that all athletes be drug-tested. According to the court, article 1, section 1 of the California Constitution[183] provides broader privacy

---

181. *See, e.g.,* H.R. REP. NO. 2168, 96th Cong., 2d Sess. § 8 (1980).

182. 273 Cal. Rptr. 402 (Ct. App.) (opinion superseded by grant of review by the California Supreme Court), *review granted,* 801 P.2d 1070 (Cal. 1990).

183. Article 1, Section 1 of the California Constitution reads:

protection than Fourth Amendment law because article 1 both covers private and public actors, and requires the state to show a compelling interest before it can invade a fundamental right to privacy.[184] The NCAA lost on appeal because it could not meet the higher state-imposed constitutional burden.

Analogously, a state court of appeals might find that Shoars comes within the purview of sections 630 and 631 because the state generally provides greater privacy protection than does the Federal Constitution. Recall that sections 630 and 631 are criminal statutes, not civil. While *Hill v. NCAA* is of constitutional significance, the *Shoars* case deals directly with privacy as a criminal matter. Arguably, the state has a very strong interest in regulating criminal intrusions of privacy. At minimum, a court of appeals should recognize a cause of action under section 631 because such recognition squares with both precedent and state legislative intent.

IV. CONCLUSION: THE GAP BETWEEN NEWLY CREATED COMPUTER SPACES AND PROTECTING PRIVACY IN THOSE SPACES

Courts must take into account an overarching policy concern regarding their role when adjudicating work-related computer privacy issues. The concern is under what rationale a court can allow a privacy cause of action when: (1) a new technology like E-mail is created, (2) an employee believes his right to privacy on this technology has been invaded by his employer, (3) no new law has been legislated to address the new privacy issues associated with the technology, and (4) old law does not clearly cover the area of privacy in question.

A gap exists in between the time when a new communication technology is created and the later time at which a statute is designed by Congress or a state legislature to regulate the new technology. During that period, the letter of the law may not protect the users of the new technology from invasions of privacy. In this gap, courts retain exclusive jurisdiction to decide whether newly-created privacy issues may be brought within the purview of the old law. Often, a court confronted with a "gap" issue will decide that it is the province of legislators, not courts, to extend statutes to cover privacy issues raised by new technologies.[185] Such a decision by a court is fully acceptable as long as

---

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

CAL. CONST. art. 1, § 1.

184. *Hill*, 273 Cal. Rptr. at 408, 410.

185. This is exactly what the trial court in *Shoars v. Epson America* held.

the court owns up to what such a decision means. Denying a plaintiff a cause of action means that the court is deciding in favor of the defendant., based not on the merits of the case, but, based on a value-judgment by the court regarding its role in the legislative/adjudicative process.

As the magnitude of the gap increases, a court should allow a cause of action under old law instead of waiting for a legislator to legislate accordingly.[186] The decision to defer to the legislature decides the issue in favor of the defendant in a veiled manner; yet, such a decision still shapes the landscape of employer-employee relations, no less than a decision on the merits. Where a plaintiff is an employee as in *Shoars*, the meaning of such deference by courts is clear: an employer does not violate an employee's right to privacy in the workplace unless a law created by a legislative body specifically proscribes such a violation; otherwise, we favor the employer's interests by default.

It is wrong for the *Shoars* court to favor the employers' interests by default. A court adjudicating a "gap" case which denies the employee a cause of action decides the issue in favor of the employer under the illusion of deference to the legislature. This type of deference favors the employer without a discussion as to *why* the employer should be favored. This Comment has argued that the workplace may run more efficiently if the employee's privacy interests are favored. At least, courts must remain aware of how their deference and inaction work a hardship on plaintiffs, regardless of how they ultimately would balance the interests at stake. To act otherwise in the "gap" institutionalizes a view of the workplace which, like the view promulgated in *Ortega*, is outdated.

---

186. This may be more true where a the court believes that disallowing plaintiff's cause of action *seems* to turn on a technicality of language, i.e., the statute in question *seems* to cover privacy and technology, but new technology is not mentioned in the statute by name. Of course, a court's ability to extend the purview of a privacy statute will depend doctrinally on the typical rationales court must invoke when performing statutory construction and interpretation, e.g., legislative intent, the statute's actual language, precedent interpreting the statute and other relevant information brought before the court by the parties.