2 Va. J.L. & Tech. 4 (Fall 1997) <http://vjolt.student.virginia.edu>
1522-1687 / © 1997 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL of LAW and TECHNOLOGY

UNIVERSITY OF VIRGINIA	FALL 1997	2 VA. J.L. & TECH. 4

Windows Nine-to-Five: *Smyth v. Pillsbury* and the Scope of an Employee's Right of Privacy in Employer Communications

by Rod Dixon[*]

Summary

1. By any measure, the impact of computer communications technology on the workplace is difficult to exaggerate. Recent and rapid proliferation of desktop computers has led to an enormous increase in both the amount and importance of electronic communication.[1] Estimates are that employees will send over 60 billion electronic messages per year by the year 2000 through electronic-mail systems.[2] Notwithstanding the impressive advancements in computer communications, rather than solving all of our communication problems, this technology has created many new problems and, in some instances, increased the severity of old ones. Due to the pervasiveness of computer technology in the workplace, serious questions have arisen concerning whether this technology presumptively may limit an employee's right of privacy.[3]
2. Nearly twenty-five percent of the messages sent by American workers are subject to some type of electronic monitoring[4] by an employer.[5] Although most employers who monitor electronic communications[6] never warn employees about monitoring, many of these employers have come to rely upon electronic monitoring as their 9-to-5 window into an employee's workspace.[7]
3. The most recent federal court to address squarely whether an employer's monitoring of an employee's e-mail communications improperly intrudes upon an employee's right of privacy was the United States District Court for the Eastern District of Pennsylvania in *Smyth v. Pillsbury Co*.[8] *Smyth* is significant because it is the first federal decision to hold that a private sector at-will employee has no right of privacy in the contents of his or her e-mail when the it is sent over an employer's e-mail system.[9] What follows is an examination of the novel question considered in *Smyth:* the extent to which an employee may rely upon common law protection to safeguard his or

her privacy in workplace electronic communications.

4. Whether the discharge or discipline of an employee on the basis of an intercepted e-mail message interferes with an employee's right of privacy, like other issues concerning the right of privacy, essentially depends on societal notions about the degree of personal autonomy an individual should have when he or she is in the workplace or is using an employer's equipment. Even where an employee's conduct may fall outside our current understanding of an employee's right of privacy, the law pertaining to privacy should inform and remind us that the invasive nature of high technology supports the notion that vigilant protection of an employee's right of privacy would be more illusory than real if the scope of the right of privacy does not encompass basic notions that personal autonomy does not become less important simply because the individual enters a workspace.
5. The determination in *Smyth* that employees should have *no* expectation of privacy in the contents of their e-mail communications in an employer's network, is clearly erroneous. Although the holding of *Smyth* is sweeping, it is doubtful that its application should be. The *Smyth* holding is based on several fundamentally flawed interpretations of privacy law and mistaken findings about computer communications technology. *Smyth's* determinations stripped all e-mail communication, *a fortiori*, of privacy protection without regard to the technology used to transmit e-mail or the employee's subjective expectations of privacy.[10]
6. First, the court erred by confusing notions of solitude with those of privacy and singularly focusing on whether a company e-mail system could be thought of as objectively secure or private, rather than also considering whether the employee subjectively believed that his e-mail communications would not be intercepted. Further, the court relied upon a conceptual distinction in privacy law that is on a collision course with technology.[11] Computer communications technology has led to a convergence of telephonic or common-carrier communications and data-driven digital communications.[12] The result is that current privacy law distinctions between common-carrier communications and e-mail communications do not reflect the fact that these communications media essentially have converged. The law is unworkable in its present form because it lags far behind the technological advances already made. While this may not be a novel occurrence, since legal jurisprudence – perhaps for good reason – often trails far behind innovations in modern technology and its impact upon the law, this fact alone should render doubtful the application of *Smyth* to future e-mail privacy cases.
7. Although some courts' ill-defined and vague references to the right of privacy have exacerbated the inconsistent level of protections that the right actually provides, there is no practical or logical reason supporting the current bifurcation of worker privacy rights regarding telephone or common-carrier communications and e-mail or computer communications. This is most evident in the failure of the *Smyth* decision to consider the relevant application of privacy law doctrine in workplace common-carrier communications. In this respect, the court should have recognized that an employee's right of privacy in computer communications should be at least co-extensive with his privacy rights in common carrier communications. Although the *Smyth* court implicitly could have rejected drawing an analogy from common carrier communications and, instead, maintained the law's distinction between e-mail and telephone communications, an understanding of computer technology demonstrates that the distinction is a useless remnant when analyzing contemporary workplace privacy issues. In this regard, an employer's ability to monitor computer

communications should be limited, at the very least, by the restrictions already sanctioned by the law of privacy regarding workplace common-carrier communications.[13]

I. Introduction

8. On January 18, 1996, the United States District Court for the Eastern District of Pennsylvania issued the *Smyth* memorandum opinion concluding that an at-will employee does not have a reasonable expectation of privacy in the contents of his e-mail communications sent through his employer's e-mail system under Pennsylvania's common-law cause of action for wrongful discharge.[14] In addition, the court held that an employer's interest in preventing inappropriate comments or illegal activity from being transmitted over its e-mail system far outweighs any privacy interest an employee may have in his e-mail comments.[15] The court reached its conclusions as a result of a wrongful discharge action filed by Michael Smyth against his employer, the Pillsbury Company (Pillsbury), a food product manufacturer. The court agreed with Pillsbury that Smyth's claim of wrongful discharge should be dismissed for failure to state a claim upon which relief can be granted, pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure.[16]
9. Smyth claimed that he was wrongfully discharged from his position as regional operations manager when Pillsbury discharged him for sending inappropriate e-mail communications to his supervisor. In October 1994, Smyth received e-mail communications sent from his supervisor's computer at Pillsbury to Smyth's home computer. The two employees exchanged e-mail communications concerning recent developments involving Pillsbury's sales management staff. Smyth's e-mail communications contained sarcastic and critical comments.[17]
10. One of Smyth's messages contained what Pillsbury termed threatening language. In it, Smyth stated that he would "kill the backstabbing bastards."[18] Another message referred to a planned company holiday party as the "Jim Jones Koolaid affair."[19] Unknown to Smyth, Pillsbury intercepted his e-mail communications.[20] On January 17, 1995, Pillsbury notified Smyth that it was terminating his employment effective February 1, 1995, for transmitting what it deemed to be inappropriate and unprofessional comments sent over its e-mail communications system in October 1994.[21] In support of its action, Pillsbury claimed that each time an employee logged onto its system, the employee received a message stating that employee e-mail communications were *not* secure, and that management reserved the right to view any e-mail communication at any time.[22] Smyth did not directly dispute Pillsbury's contention; he asserted that Pillsbury repeatedly had informed its employees that their e-mail communications would remain confidential and would not be used as a basis for reprimand or dismissal.[23]
11. The court rejected Smyth's arguments. In granting Pillsbury's Rule 12(b)(6) motion, the court stated that the right of privacy did not extend to the contents of e-mail communications, despite the fact that employees were entitled to a right of privacy on the basis of the public policy favoring privacy rights emanating from tort law under Pennsylvania state law.[24] According to the court, company e-mail does not have privacy protection because e-mail necessarily is public in the manner in which messages travel over an employer's network.[25] In addition, the court

determined that employers have a legitimate need to monitor e-mail communications to safeguard the company-owned computer network and manage worker productivity.[26] This interest, according to the court, may override an employee's interest in privacy, even if an employer makes assurances that e-mail communications are confidential.[27]

II. The Source of an Employee's Right of Privacy in the Workplace

12. Defining what constitutes an employee's right of privacy has proven to be no easy task for courts or legislatures.[28] Furthermore, the assurance of a right of privacy in the workplace largely appears to depend upon the extent to which an employer may exercise its legitimate interest in maintaining control over the workplace without running afoul of an increasing bundle of employee rights. In part, this has been difficult to determine because federal constitutional right of privacy jurisprudence has influenced heavily state and federal court interpretations of privacy rights in the workplace, regardless of whether the employee worked in the public or private sector or whether the source of the employee's right of privacy emanated from sources other than the Federal Constitution.[29]
13. Today, the notion that the scope of an employee's right of privacy, regardless of the source of the right, is limited by the employee's reasonable expectation of privacy is accepted as a threshold principle in evaluating workplace privacy issues, notwithstanding the fact that this principle derives from constitutional law.[30] Evaluating whether an employee's expectation of privacy is reasonable in order to determine whether the privacy right exists has its genesis in the Fourth Amendment of the United States Constitution.[31] Fourth Amendment search and seizure doctrine generally protects an expectation of privacy that society is prepared to consider reasonable.[32] In analyzing the reasonableness of the search, courts often balance the need to search or intrude against the invasion of privacy resulting from the intrusion.[33] In the context of the workplace, courts have been halting and languid in finding invalid intrusions of an employee's privacy.[34] Courts often determine that 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, fraud, or other illegal activity.[35] Although limitations on the government's ability to intrude on the constitutional right of privacy for individuals have been recognized concerning family matters, setting limitations on an employer's invasion of an individual's right of privacy in the workplace has proven to be particularly troublesome for the courts.[36] Even where such delineation has been accomplished, courts often have made widely divergent interpretations of when an employee's right of privacy may be circumscribed by his or her consent to workplace monitoring.[37]
14. Notwithstanding the fact that federal constitutional case law has had a major impact in shaping workplace privacy, surprisingly there is no federal statute squarely on point which protects an employee's privacy interests in his computer or electronic communications transmitted within a computer network owned or operated by his employer.[38] To the extent that courts have attempted to invoke the protections of a federal statute, courts have relied almost exclusively upon the Electronic Communications Privacy Act of 1986 (ECPA).[39] Under the ECPA, private individuals and organizations may be prosecuted for unauthorized interception of electronic

communications.[40] The ECPA, however, does not directly address privacy protections of employees, in relation to their employers, who communicate by e-mail.[41]

15. Perhaps this is so because Congress passed the ECPA, not specifically to address privacy concerns, but, instead, to close loopholes in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[42] The ECPA appears to focus on third party interception. This focus may provide 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.
16. In stark contrast to the lack of federal statutory employee e-mail privacy protection, the bulwark for employee privacy protection has become state common law.[43] Virtually all states have adopted some form of a common law tort of invasion of privacy.[44] The form most relevant to e-mail interception is the "unreasonable intrusion upon the seclusion of another" tort. This tort holds that "one who intentionally intrudes, physically or otherwise, upon the seclusion of another…is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[45]
17. As suggested *supra,* the elements of the tort are similar to the standards used in determining a Fourth Amendment search and seizure or constitutional privacy claim. For behavior to be actionable, the employee must prove that his employer committed a highly offensive intentional intrusion into a private matter.[46] Finally, in determining the offensiveness of an intrusion, courts examine the degree of intrusion, the context, and circumstances surrounding the intrusion, as well as the intruder's motives and objectives and the expectations of those whose privacy is invaded.[47]
18. Recently, some state courts have also interpreted their respective state constitutions and statutes to provide employees with privacy protection and in some instances have found broader privacy protections in state constitutions than the Federal Constitution.[48]

III. Evaluating the *Smyth* Right of Privacy

19. The *Smyth* court concluded that the plaintiff could prove no set of facts in support of his wrongful discharge claims that would entitle him to relief.[49] After acknowledging that Pennsylvania employment law is governed by the at-will employment law doctrine, the court noted that where the discharge of an at-will employee threatens or violates a clear mandate of public policy, the employer may be subject to a cause of action for wrongful discharge.[50] In *Smyth*, the employee claimed, *inter alia*, that his discharge violated Pennsylvania public policy because, in that state, employers were precluded from dismissing employees when the dismissal was based on actions by the employer which violated an employee's right of privacy.[51] In Pennsylvania, the public policy exception to the at-will employment law doctrine must be based on a clear mandate of public policy.[52] In this context, the Pennsylvania Court of Appeals has found such a mandate embodied in the state's common law cause of action for tortious invasion of privacy; namely, the tort of intrusion upon seclusion.[53]

20. Applying the Restatement (Second) of Torts definition of the tort of intrusion upon seclusion to the circumstances surrounding Smyth, the court determined that Smyth could not have had a reasonable expectation of privacy in his e-mail communications. According to the court:

    [U]nlike urinalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.[54]

21. Perhaps anticipating that its holding relied upon a rather elusive and tenuous determination concerning when an employee may loose his reasonable expectation of privacy when using an employer's e-mail system, the court went a step further and held that an employer's interception of an employee's e-mail was not a highly offensive or substantially intrusive invasion of the employee's right of privacy.[55] More importantly, the court swept away any need to undertake an actual balancing of an employee's interest against his or her employer's since the court summarily held that an employer's interest in "preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[56]
22. The court's determinations in *Smyth* are flawed for several reasons. First, the court improperly focused its analysis of whether Smyth maintained any expectation of privacy in his e-mail communications on the fact that Pillsbury's e-mail system was "utilized by the entire company."[57] According to the court, at the very moment Smyth sent his e-mail communication through the wires of the company e-mail system, any expectation of privacy was lost by the mere nature of the system.[58] In this respect, the court seemed to have confused the concept of privacy with that of solitude. The long standing distinction between "privacy" and "solitude" has been accorded significance in privacy law, even in the context of tort actions, to ensure that the right of privacy does not become a right reduced to a measurement of the physical surroundings of the alleged privacy invasion.[59] Courts have wisely eschewed the adoption of a bright line test to measure the contours of a right which protects personal autonomy and is held so fundamental to individuals.[60] Contrary to *Smyth,* the fact that a company's communication system is used widely by multiple users should not thereby transform the contents of any message sent through that system as statements devoid of any expectation of privacy. Indeed, the fact that others have access to the location[61] or physical entity for which privacy protection is being sought has never, in itself, justified a determination that a privacy interest does not exist.[62] There is no reason to believe that Smyth's expectation of privacy should fade away or otherwise be affected by the simple fact that the e-mail system is used by all company employees or by the fact that Pillsbury has the right to make lawful interceptions of an employee's e-mail communication.
23. An employee enjoys an expectation of privacy in the drawers or files within his or her office, notwithstanding the fact that his supervisor or coworkers may enter the workspace.[63] Similarly, Smyth's use of his employer's e-mail system could not remove his subjective expectation of

privacy in the contents of his e-mail messages simply because other employees have access to the computer network. In this regard, the court did note that Pillsbury informed its employees that e-mail messages were confidential, but did not find the employer's statements indicia of Smyth's expectation of privacy.[64]

24. Undoubtedly, had the court properly distinguished between privacy and solitude, it would not have found that Pillsbury's e-mail system, itself, stripped Smyth's e-mail messages of any privacy protection. In this respect, the court's analysis would have advanced forward to determine whether Smyth's expectation of privacy in the contents of his e-mail messages was reasonable.
25. As it stands, *Smyth's* determinations stripped all e-mail communication, *a fortiori*, of privacy protection without regard to the technology used or the employee's subjective expectations of privacy. In this context, *Smyth* so egregiously departed from current doctrine on the law of privacy that the decision may be validly distinguished and limited to its peculiar findings. Although not directly on point, *O'Connor v. Ortega* supports the proposition that the contours of employee privacy are not precisely shaped by the degree of solitude the employee finds himself working in.[65]
26. In *Ortega*, Dr. Ortega was employed as a psychiatrist at a state hospital.[66] He became subject to an investigation regarding various improprieties including his alleged mismanagement of the hospital's residency program.[67] During the investigation, hospital employees entered and searched Ortega's locked office, where numerous items were seized from his desk and files.[68] Subsequently, Ortega was fired and he sued the hospital, complaining that the search violated his Fourth Amendment rights.[69] The district court granted summary judgment for the hospital, and 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.[70] On appeal, the Court found that Ortega had a reasonable expectation of privacy in his desk and file cabinets located inside his office.[71] Justice Scalia's dissent noted that the concepts of privacy and solitude, while similar, are analytically distinct.[72] Justice Scalia acknowledged that there is a distinction between a determination concerning whether an employee maintained a subjective expectation of privacy and whether the physical location of an employee's desk or other so-called private matter warrants an expectation of solitude. The latter goes to the employee's understandings about his employer's practical capability to intrude upon his privacy while the former goes to an employee's expectations concerning his employer's lawful ability to intrude upon his privacy.[73]
27. *Smyth* is also flawed because the decision is not in step with the decisions of other courts regarding the proper focus of inquiry in determining an employee's subjective expectation of privacy in the workplace. For example, in *Walker v. Darby*,[74] the Eleventh Circuit recognized that an employee's expectation of privacy is not solely dependent upon whether the work-space was objectively secure from communication interception, but also depends upon whether the employee subjectively believed that interception would not occur.[75] Regarding e-mail communications, this could be demonstrated by the employee's use of encryption technology or the employer's statements concerning confidentiality. In *Smyth*, the court recognized that Pillsbury had sent notices to employees informing them that their use of company e-mail was considered confidential, but inexplicably gave no weight to this fact in its determination that Smyth had no

subjective expectation of privacy.[76] In *Walker*, the plaintiff who was a letter carrier for the United States Post Office in Florence, Alabama believed that his Caucasian supervisors were trying to terminate him for race-motivated reasons.[77] Someone warned Walker that his supervisors were monitoring his conversations at his workstation. Walker then noticed two objects that looked like intercoms affixed to his workstation.[78] Walker sued his supervisors for illegal interception of his conversations and invasion of privacy.[79]

28. The Eleventh Circuit held in favor of 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.[80] 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.[81] 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; which is distinguished from determining whether Walker had a reasonable expectation of privacy in his workplace area.[82] This distinction was critical to Walker's case.[83]
29. More troubling, the *Smyth* court also misunderstood the fundamental nature of the communications technology involved. Today, the nature and prevalence of computer communications requires courts to consider analogous communications media when determining the contours of an employee's right to privacy. In this respect, courts must recognize that employer limitations on the electronic monitoring of telephone or common-carrier communications in the workplace should also guide an analyses of the permissibility of similar electronic monitoring regarding computer communications.
30. Computer communications incorporate several communications media into one desktop box, which permits computer users to access a range of choices on how to communicate with others.[84] E-mail communication is only one, albeit important method of computer communication. Already, desktop computers have replaced answering machines, facsimile machines, and broadcast devices such as television sets and radios. An employee may use his employer's computer network connection to access the Internet;[85] to fax documents, receive voice mail, record voice mail messages, make phone calls; and to participate in video-conferencing.[86]
31. Paradoxically, the privacy protection afforded postal mail and voice-mail far outstrips that currently afforded e-mail.[87] Moreover, unlike postal mail, e-mail reaches its intended recipient almost instantaneously and may be more secure than postal mail by adopting encryption technology, which could effectively lock-out the eyes of anyone gaining access to the e-mail message except the intended recipient. Further, the anachronistic distinction between the protections afforded employees in their telephone communications versus those afforded employees in their computer communications is no longer legitimate.[88] Advances in communications technology has fueled the convergence of traditional telephonic communication with computer communications.[89]
32. Recent advancements in computer technology has led to the development and use of Universal Messaging Systems, which allow individuals to send e-mail communications or voice mail communications over the company's computer network depending on the employee's

preference.[90] Messages sent as e-mail communications also can be transformed by the receiver into a voice mail message or vice-versa.[91] But, what happens when an e-mail message is retrieved as a voice mail message, and the employer intercepts the voice mail message?[92] Which level of privacy protection should the message be afforded, that common carrier or e-mail? Consider the reverse situation. An employee sends a voice message via telephone, which is retrieved as a computer communication or email message. Should his her expectation of privacy be diminished when that message is intercepted by his or her employer? To these questions, there are no easy answers. Indeed, courts should not have to answer these questions, but yet the current state of privacy law would make such inquiries more than just relevant.

33. Without debate, the widespread use of computer communications technology makes it nearly impossible to determine whether a communication should be categorized as a telephone message and, therefore given heightened privacy protection, or as an e-mail message, which under *Smyth*, would be entitled to no privacy protection at all.[93] This conundrum illustrates why workplace privacy jurisprudence must abandon the archaic distinction between computer communications and traditional telephonic communications. To fail to do so, not only would appear to be obnoxious to the protection of a fundamental right, but inevitably would be unworkable as communications media continue to converge and other technological advances, such as secure or encrypted e-mail transmissions, become commonplace. Although the *Smyth* court cannot be faulted for being ill-equipped to assess the present state of computer communications, or for that matter, for not considering issues that the parties may have failed to make known to it, the court's sweeping holding was clearly inappropriate in light of the rapidly developing communications technology.
34. In addition, the significant transformation of electronic communications that the Internet is bringing about will further alter the subjective expectation of privacy employees will have concerning their e-mail communications. The Internet is an open system. Employers provide their employees with access to the Internet by connecting the company's local area network (or LAN) directly to the Internet. This enables employees to send e-mail communications originating on their personal computer (desktop PC), onto a system of networks not owned or controlled by the employer. With access to the Internet, an employee may send computer communications to a co-worker, client or anyone in the world. This form of computer communications may, if done through use of a computer modem, for example, bypass an employer's e-mail and LAN system entirely. More importantly, once an employer connects his LAN system to the Internet, the bright line distinctions between what occurs on a corporate network from what occurs on the Internet become very faint.[94]
35. Most, if not all, employers connect their local networks to the Internet through a TCP/IP network. TCP/IP network protocols ultimately put an employer's private communications network on an on-ramp onto the very public Internet. When employers grant employees access to the Internet, they permit their employees to participate in a vast and very public communications forum. This form of communications access opens doors to the Internet that cannot be shut or monitored once the TCP/IP connection is made. Every node of a TCP/IP network becomes a door into or out of the employer's computer system.[95] In this respect, the lines blur between what computer communication actually occurs on the employer's private network or on the public Internet. As noted *infra*, this fact provides a significant impediment to an employer's argument that e-mail

interception is necessary to monitor activity occurring on the employer's private communications network, since a great deal of communications activity may be occurring on the public Internet. Most importantly, computer communications that travel across the Internet may heighten an employee's subjective expectation of e-mail privacy and may form the basis for why an employee's expectation of privacy is objectively reasonable. Unquestionably, employers have significantly less control over communications that travel from a desktop PC to the Internet than over the company's computer network.

36. Notwithstanding the fact that Pillsbury used an e-mail system that functioned on the company's own network, many employers use e-mail systems that function on both a proprietary LAN system and the Internet. Employees are free to send e-mail using an in-house e-mail system or directly through the Internet. While the choice of how an e-mail is sent does not directly affect how the receiver reads the e-mail, it may have the anomalous effect of influencing the degree of privacy an employee is entitled to under the court's analysis. E-mail communications that travel across the Internet through gateway protocols either bypass the employer's network entirely or use the employer's Internet connection to avoid the company's e-mail system. It is in this sense also that the e-mail communication is more like a message transported over a common carrier, which would, of course, under present workplace privacy law, afford an employee greater privacy protection in the content of those e-mail transmissions.
37. Internet e-mail, like most computer transmissions over the Internet, rely on a transmission protocol called "packet switching." Packet switching simply means that each e-mail message is transmitted to the receiver through small packets or discrete digital units. In essence, each e-mail message is shredded by the Internet while the message is traveling. Once the message reaches its destination, a computer server for example, the digital packets are reassembled into the original e-mail message.[96] Not surprisingly, interception of Internet e-mail while the message is in transmission is possible, but not easy. Furthermore, the use of encryption devices could be an employee's clearest indication that there is a subjective expectation of privacy in the contents of his or her e-mail.[97]
38. E-mail can also be accessed using an Internet protocol called "Telnet." Telnet is a communications protocol that enables computer users to connect directly with other networks that may or may not be part of the Internet.[98] When accessing e-mail in this manner, the employee may actually be connecting to a network not owned or operated by the employer. For example, an employee may be a member of a commercial online computer service such as America Online or Compuserve. If he accesses his e-mail on one of these services using Telnet, the employer's obvious justification for snooping or monitoring this e-mail is that the employee used the employer's equipment to connect to the other network, but this justification may not be sufficient to overcome an employee's expectation of privacy. More importantly, if an employer intercepts the e-mail message in the manner claimed by the defendant in Pillsbury, the employer may not be able to determine, without the employee's cooperation, whether the e-mail message was accessed using the company's network or using Telnet – a determination that essentially must be made immediately to accord the appropriate degree of privacy protection to the message contents under current privacy law jurisprudence.[99]
39. Normally, an employee creates an individual password to access the employee's own messages. Such a password undoubtedly encourages a subjective belief among employees that their e-mail

messages are private, given that employees are often unaware that their employer retains the ability to override the password and access their e-mail. It is thus understandable that most of the litigation concerning privacy expectations has concerned whether the expectation is objectively reasonable, since employees have easily demonstrated subjective privacy expectations. This emphasis, however, will become less significant in the future because employers who seek to alter the objective reasonableness of subjective expectations by modifying the extrinsic factors of the work environment will soon recognize that technology has obviated the fact that e-mail users will routinely lock-out individuals from deciphering, decoding, decrypting, or otherwise reading an e-mail that is not intended to be read by anyone other than the sender and receiver.[100]

40. At bottom, an employer would have to justify its interest in e-mail interception as resulting from the fact that the employee used the employer's equipment to send or receive the e-mail communication.[101] That is, the employer's justification would be based on the fact that it owns the desktop computer that was used to access the e-mail message even though the e-mail message could have been protected by a password unknown to the employer, encrypted in a manner that the employer could not defeat the encryption, or that the e-mail message, itself, resided on a computer server, not owned by the employer.

IV. Conclusion

41. The preeminent case evaluating the interest of an employee versus those of his employer when the employer monitors an employee's electronic communication is *Watkins v. L.M. Berry & Co.*, which balanced those interests by examining the degree to which an employee may have consented to the monitoring when the employer has a carefully defined monitoring policy.[102] In *Watkins*, the employer informed its employees that it would monitor their business telephone calls but would monitor their personal calls only to the extent necessary to determine whether a particular call was business or personal.[103]
42. The Eleventh Circuit held that this disclosure constituted employee consent only to the monitoring of business calls and not to the monitoring of the full content of personal calls. The court was clearly concerned that any notion that the employee maintained a right of privacy, in this instance, on the basis of statutory protection, would be thwarted if "consent could routinely be implied from the circumstances."[104] In this respect, the court concluded that an employee's knowledge of his employer's capability of monitoring electronic communications, without more, cannot be considered an implied consent by the employee to permit employer monitoring of all telephone calls regardless of whether the telephone call was personal or business related.[105]
43. Although *Watkins* represents strong support for placing limits on an employer's ability to lawfully monitor telephone calls, the case also demonstrates that employers are not without significant freedom to determine in what cases an employee's computer communications can be intercepted.[106] Even under a regime of privacy protection more significant than what was countenanced by *Smyth*, an employer can safeguard its computer network or e-mail system from improper conduct by employees. Employers may escape wrongful discharge liability for intruding upon a worker's privacy if the employer establishes a comprehensive monitoring policy and abides by the policy's limits. Under a *Watkins*-like scenario, an employee's use of his employer's e-mail

network could constitute consent to employer interception of work-related messages and even personal messages to the extent the interception of personal e-mail messages is needed to determine whether the messages are personal or business in character. In this regard, an employer who publishes such a *Watkins*-like e-mail policy must ensure that the scope of e-mail monitoring match the legitimate business interest justifying the invasion of the employee's right of privacy.

44. Although courts have often failed to balance the distinct interests of employees and employers in terms of workplace efficiency or productivity, a proper balancing of interests may, in fact, weigh more favorably in upholding or safeguarding the employee's privacy interests. It may be highly likely that increased employee privacy could result in a more efficient workplace. 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, an employer who monitors the workplace from nine-to-five and who is privy to all intra-company communications may create a workplace filled with distrust. Undeniably, an employee who does not trust his employer has much less of an incentive to be efficient, resourceful, and productive.
45. Ultimately, the court's view in *Smyth* of workplace efficiency unfortunately may cast the employee as the employer's adversary. This view of the workplace is improper because it portrays the employee as almost incapable of managing his or her given responsibilities. Without debate, companies that find the need to monitor an employee's every move also view the workplace as a battleground of competing interests, but it is quite possible that successful companies do not treat employees as enemies. Instead, these companies provide their employees with both personal and professional incentives to perform productively. Courts should attempt to balance the interests of employees and employers in light of the principles underlying the fundamental right at issue; namely, principles of personal autonomy, individual respect, and mutual trust.[107] In this regard, the scope of an employee's right of privacy would encompass some level of protection concerning the content of his e-mail messages.
46. The determination in *Smyth*, that under Pennsylvania common law employees have no expectation of privacy in the contents of their e-mail communications when such travels along an employer's network, clearly was erroneous. *Smyth's* determinations stripped all e-mail communication *a fortiori* of privacy protection without regard to the technology used or the employee's subjective expectations of privacy. This holding was based on several fundamentally flawed interpretations of privacy law and mistaken findings about computer communications technology. The court erred by confusing notions of solitude with those of privacy and singularly focusing on whether a company e-mail system could be thought of as objectively secure or private, rather than also considering whether the employee subjectively believed that his e-mail communications would not be intercepted. In this regard, the court significantly departed from prevailing workplace privacy jurisprudence when it determined that the Pillsbury company was without limitations in its ability to intercept employee e-mail.
47. In addition, the court relied upon a conceptual distinction in privacy law that is on a collision course with technology. Computer communications technology has led to a convergence of telephonic or common-carrier communications and data-driven digital communications. The result is that current privacy law distinctions between common-carrier communications and e-mail

communications do not reflect the fact that these communications media have converged. The law is unworkable in its present form because it lags far behind the technological advances already made. This fact, alone, should render doubtful the application of *Smyth* to future e-mail privacy cases. The *Smyth* court also misapplied its privacy analysis by focusing upon the issue of solitude in communications, rather than following the presently evolving privacy doctrine, which primarily emphasizes an analysis of whether an employee expects his communication to be intercepted.

48. Given the impact that communications technology has had upon the workplace, a significant evolution in the law of employee privacy is required. An employee's right of privacy in computer communications should be at least co-extensive with his privacy rights in common carrier communications. There is no practical or logical reason supporting the courts current bifurcation of worker privacy rights regarding phone communications and e-mail or computer communications. Indeed, the trend in communications technology is leading to the convergence of these two communications media. In this regard, an employer's ability to monitor computer communications, as is already true of common carrier communications, should be limited by an employee's reasonable expectation of privacy in the contents of his computer communications.
49. More importantly, privacy rights hinge on important notions of human dignity.[108] The law must advance and evolve with technology to ensure the continued vitality of an employee's right of privacy. Indeed, the *Smyth* decision serves to remind us that the scales need to be re-calibrated to better protect employee privacy. Privacy law requires courts to balance the interests of employees against those of the employer. To this end, effective judicial balancing ferrets out the legitimate interests of the parties when the balance is done to reflect the appropriate backdrop of the interests of the parties.
50. When a court decides that an employer's interest legitimately supports burdening an employee's right of privacy, then the court should carefully circumscribe the permissible instances where electronic monitoring could occur in order to safeguard employees from possible abuses of surveillance technology. While courts need not be experts in computer technology, judicial opinion must reflect a fundamental understanding of the technology involved, if employees are to be left with more than the remnants of the right of privacy in their computer communications.[109]

Footnotes

[*] Rod Dixon, B.A., M.A. (University of Pittsburgh 1984 & 1986), J.D., (George Washington University Law School 1992) is an attorney with the U.S. Department of Education and a graduate law student at Georgetown University Law Center pursuing an LL.M. in Labor Law.

[1] Thomas E. Weber, *Line Between E-mail and Voice Mail Fades*, Wall St. J., Feb. 13, 1997, at B6. Electronic mail, often referred to as "e-mail," is a form of digital communication where text or graphical messages are sent from one computer to another, somewhat like postal mail is sent from one location to another. A computer user sends a message to another person's computer or terminal, which is usually in a different location. The messages are sent instantly and usually travel over communication networks – sometimes called local or wide area networks (LAN or WAN

systems) – or in many instances the messages may travel across phone lines essentially as digital communications. Most company e-mail systems require that the computer user access the system using some type of user name and identification code. This procedure authorizes the user to access the system, and provides some level of security ensuring that the e-mail messages read by the computer user are addressed to the identified user. *See* R.J. Ignelzi, *Privacy In the Workplace Part Two: Under Scrutiny E-mail, phone calls, voice mail legally can be monitored by boss,* San Diego Union-Trib., July 3, 1995 at D1.

[2] Scott Dean, *E-mail Forces Companies to Grapple With Privacy Issues*, Corp. Legal Times, Sept. 1993, at 11.

[3] *See* R.J. Ignelzi, *Privacy In the Workplace Part Two: Under Scrutiny E-mail, phone calls, voice mail legally can be monitored by boss,* San Diego Union-Trib., July 3, 1995 at D1.

[4] Jerry Mahoney, *Watchful Workplace; Employee Monitoring Has New Dimensions and Old Concerns,* Austin Am.-Statesman, Sept. 8, 1996. Electronic monitoring generally refers to an employer recording, reading, or listening to telephone or computer communications sent to employees by others. In a few specific contexts, the law governing electronic communications establishes a technical definition of what electronic monitoring may encompass; those definitions are addressed below when appropriate.

[5] Dean, *supra* at 11. Corporate e-mail grew 83 percent among the Fortune 2000 firms between 1991 and 1993, and nine out of ten employers of over 1,000 workers in the United States. now use e-mail. John Thackery, *Electronic-Mail Boxes a Dumping Ground for Meaningless Data*, Ottawa Citizen, May 28, 1994, at B4.

[6] Although throughout this article I use the term "e-mail," the term "electronic or computer communication" should be preferred because computer communications actually include a great deal more than what typically is referred to as e-mail. Indeed, the thesis of this paper is based, in part, on the proposition that some courts and commentators have often mistakenly drawn an artificial and anachronistic distinction between e-mail communications and non-e-mail computer communications. I also will refer explicitly to e-mail communications with the caveat that I see no relevant distinction between e-mail communication and other forms of computer communications when addressing workplace privacy issues.

[7] *But see*, Lory Zottola Dix, *Some Organizations are Defining E-Mail Privacy*, Computerworld, Nov. 23, 1992, at 87 (user group establishes formal e-mail privacy policy); Don J. DeBenedictis, *E-mail Snoops: Reading Others' Computer Messages May Be Against the Law*, A.B.A.J., Sept.1990, at 26-27 (certain laws may ban unauthorized reading of e-mail); Bruce Caldwell, *E-Mail Privacy: A Raw Nerve For Readers,* informationweek, July 30, 1990, at 52 (collecting reader’s views on monitoring email).

[8] 914 F. Supp. 97 (E.D. Pa. 1996). *See also Bohach v. City of Reno*, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (holding no right to privacy with messages sent on police department's computerized paging system because it is in ordinary course of business for police departments to record information, and department members were informed messages are logged onto network).

[9] The court's decision in *Smyth* clearly represented new ground for the district court. Prior to its decision in *Smyth*, the district court had never reviewed a wrongful discharge action concerning computer communications. The court made no explicit references to relevant and analogous case law on the subject, nor did the court rely on interpretations of relevant state or federal statutes to guide its analysis in this complex area. *See generally* 914 F. Supp at 98-101.

[10] 914 F. Supp. at 101.

[11] *See id*.

[12] *Alcatel Introduces Cross Connect Technology Key to the Establishment of the All-Optical Central Office*, Bus. Wire, Sept. 22, 1997. In most modem communications, the modem first converts the digital computer data into analog signals or sounds. Then, the telephone network converts the transmitted analog signal to a digital signal to enable the data to travel along a patchwork of digital and analog phone lines, which ultimately enables computer users to communicate via computer through several forms of communication, including desktop video conferencing, e-mail transmissions, voice or sound transmissions, and even through a connection to the Internet to receive live radio broadcasts. W. John Blyth & Mary M. Blyth, Telecommunications: Concepts, Developments, and Management 80-81 (2d ed. 1990).

[13] A communications common carrier provides transmission service facilities to the general public, like a telephone service company. *Id.* at 329.

[14] 914 F. Supp.at 100. Since at least 1891, Pennsylvania has recognized the common-law rule, often referred to as at-will employment, that employees may be discharged at any time, for any reason or for no reason at all. *Henry v. Pittsburgh & Lake Erie R.R.*, 21 A. 157 (Pa. 1891); *Forman v. BRI Corp.*, 532 F. Supp. 49, 50 (E.D. Pa. 1982). The employment relationship exists at the will of both parties, and either is free to terminate the relationship at any time. More recently, however, courts consistently have brought *employers* out of the at-will relationship by granting employees a right of action against the employer for wrongful discharge when the employer is found to have terminated the employee in violation a clear mandate of public policy. *See Geary v. United States Steel Corp.*, 319 A.2d 174, 180 (Pa. 1974); *Perks v. Firestone Tire & Rubber Co.*, 611 F.2d 1363, 1365-66 (3d Cir. 1979).

[15] 914 F. Supp. at 101.

[16] *Id*.

[17] *Id*. at 98, n.1.

[18] *Id*.

[19] *Id*. This statement appears to be a reference to the 911 followers of religious cult leader Jim Jones who committed mass suicide by drinking a poison-laced beverage in Jonestown, Guyana, in 1978. Jonathan Friedland and Raphael Pura, *Log Heaven: Troubled at Home, Asian Timber Firms Set Sights on the Amazon*, Wall St. J., Nov. 11, 1996 at A1.

[20] 914 F. Supp. at 98. The parties disputed whether Pillsbury actually intercepted Smyth's e-mail communications electronically. Despite Smyth's claims, Pillsbury reported that it obtained the e-mail communications in print form when another worker saw a printed copy of the messages in a pile of papers to be recycled and brought the messages to the management's attention. *Id*.

[21] *Id.* at 98-99.

[22] See also Jonathan Wallace, High Technology and the Law, A Legal Perspective on the Open Systems Industry, E-Mail Privacy: What are your Rights?, http://www.uniform.org/news/html/publications/ufm/aug96/legal.html; 22 Computer Law & Tax Report 12 Firing based on E-mail not Wrongful Discharge (June 1996).

[23] See also Jonathan Wallace, High Technology and the Law, A Legal Perspective on the Open Systems Industry, E-Mail Privacy: What are your Rights?, http://www.uniform.org/news/html/publications/ufm/aug96/legal.html; 22 Computer Law & Tax Report 12 Firing based on E-mail not Wrongful Discharge (June 1996).

[24] 914 F. Supp. at 101. Notably, the Smyth court declined to follow the line of case law that would have permitted Smyth's wrongful discharge action to be based on the public policy emanating from the federal constitution's privacy right. Courts have acknowledged that private sector employees should be protected from the threat of discharge where such action may be opposed to constitutionally protected interests. See, e.g., Novosel v. Nationwide Ins. Co., 721 F.2d 894, 900 (3d Cir. 1983) (employee's constitutional right to express himself politically is sufficient to state a public policy under Pennsylvania law).

[25] *Id.*

[26] *Id.*

[27] *Id.* Pennsylvania has an anti-wiretapping statute, although the Smyth court made no note of it.

See 18 Pa. Const. Stat. Ann. § 5721 (West 1983 & Supp. 1997). As noted, infra, similar state statutes often form the basis of employee privacy actions. It is unclear whether reliance on the statute, rather than common law, would have resulted in a different result for the Smyth court since, as discussed below, privacy issues often are evaluated using the same analysis regardless of the source of law.

[28] In 1965, the Supreme Court held in *Griswold v. Connecticut*, 381 U.S. 479, 484-86 (1965), that there was a right of privacy protected by the Federal Constitution. The court held that a Connecticut contraceptive statute was unconstitutional as applied to a married couple.

[29] Indeed, the "right of privacy" may be more appropriately described as a bundle of rights, which derive from at least four distinct sources: the Federal Constitution, various state constitutions, statutory and regulatory sources, and the common law of most states. The Supreme Court laid the framework for the constitutional right of privacy in the early 1920s, in *Meyer v. Nebraska*, 262 U.S. 390, 399-403 (1923), and *Pierce v. Society of Sisters*, 268 U.S. 510, 534-36 (1925). These cases recognized that parents had the right to make decisions concerning the educational welfare of their children. As a result, parents ostensibly were afforded a privacy right of protection from state intrusion into the family unit. The Court moved closer to granting an express right of privacy in *Prince v. Massachusetts*, 321 U.S. 158, 164-71 (1944), by holding that the family unit, in the confines of the home, cannot be subject to state intrusion.

[30] The Search and Seizure clause of the Federal Constitution does not protect citizens from unreasonable searches by private parties. *See, e.g., United States v. Jacobsen*, 466 U.S. 109, 113-14 (1984); *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345, 349 (1974).

[31] 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.

[32] In a reasonable search, the searcher typically has obtained a warrant based on probable cause. Searches conducted without a warrant are adjudged *per se* unreasonable. *Katz v. United States*, 389 U.S. 347, 357 (1967).

[33] *Terry v. Ohio*, 392 U.S. 1, 21 (1968).

[34] *See e.g. National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 672 (1989)

(employees involved with drug interdiction to who are required to carry firearms can expect diminished level of privacy); *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (some employees' expectations of privacy are unreasonable when search is by supervisor).

[35] *See e.g. United States v. McLaren*, 957 F. Supp. 215, 219 (M.D. Fla. 1997) (employer can monitor telephone when substantial nexus exists between use of telephone instrument and specific fraudulent activity being investigated); *T.B. Proprietary Corp. v. Sposato Builders, Inc.*, No. CIV. A. 94-6475, 1996 WL 290036, at *2 (E.D. Pa. May 31, 1996) (monitoring extension telephone or other telephone equipment in Pennsylvania in ordinary course of business is not prohibited); *Ali v. Douglas Cable Communications*, 929 F. Supp. 1362, 1390-91 (D. Kan. 1996) (monitoring telephone calls of employee accused of theft is acceptable ordinary business decision).

[36] This is true with regard to public employees as well as private sector workers. Many commentators have concluded that the Supreme Court has fashioned search and seizure law poorly for the public workplace because it continues to rely on a radically outdated view of how the workplace functions. The Supreme Court has all but eliminated constitutional protection for public employees with respect to work-related searches and seizures. *See O'Connor v. Ortega*, 480 U.S. 709, 730-31 (1987) (Scalia, J. concurring).

[37] C. Leigh Haynes, Note, *The Envelope, Please: Problems and Proposals for Electronic Mail Surveillance*, 14 Hastings Const. L.Q. 421, 431-37 (1987). *See also* Barbara Garson, The Electronic Sweatshop 205-24 (1988) (collecting personal anecdotes regarding surveillance).

[38] *See, e.g.*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) [hereinafter 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. 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. S. Rep. No. 541, 99th Cong., 2d Sess. pt. 1 at 8 (1986) (report discusses areas that Congress did not intend the ECPA to reach).

[39] 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, and other forms of electronic communications not carried over public networks. 18 U.S.C. §§ 2511-2711 (1988).

[40] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.)

[41] *See, e.g.*, H.R. Rep. No. 1218, pts. 2-7 (1991). First, the ECPA amended the definitions of "wire" and "oral" in Title III to include the term "electronic." An "electronic communication"

specifically includes e-mail. 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. Second, Title III was amended to include the words "aural or other acquisition." Amending this section allowed Congress to include non-aural, electronic communications within the purview of Title III's protection. 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. 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.

[42] 18 U.S.C. §§ 2510-2521 (1988). The Act is generally referred to as Title III, and the scope of communications covered the title include wire, oral and electronic communications. Title III defines "electronic communications" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photoptical system that affects interstate or foreign commerce," but excludes cordless telephones, tone-only paging devices and tracking devices. 18 U.S.C. § 2510(12) (A), (B) and (C) (1988).

[43] Courts have developed a cause of action for injury based on a tortious invasion of privacy. *See K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632, 635-36 (Tex. Ct. App. 1984) (citing *Billings v. Atkinson*, 489 S.W. 2d 858, 859 (Tex. 1973)) (court stated that the essence of our right of privacy is our right of be left alone, to live a life free from intrusion and unwanted publicity), *writ refused*, 686 S.W.2d 593 (Tex. 1985). Similarly, this is the basis of Smyth's lawsuit.

[44] The tort normally includes a scheme of four distinct torts protects the right of privacy: (1) unreasonable intrusion upon the seclusion of another; (2) misappropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; and (4) publicity that unreasonably places another in a false light before the public. William L. Prosser, *Privacy*, 48 Cal L. Rev. 383, 389. Each tort recognizes a "substantial zone of freedom," where an individual has the right "to be left alone." *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632, 635-36 (Tex.Ct.App.1984).

[45] Restatement (Second) of Torts § 652 B (1977).

[46] Such an intrusion may occur by a defendant's use of mechanical aids. Restatement of Torts (Second) § 652 B, comment B (1977). In deciding whether the intrusion is into a private matter, courts require not only that the employee have a subjective expectation of privacy but also that the expectation be objectively reasonable. *K-Mart Stores Corp.*, 677 S.W.2d at 636.

[47] Restatement of Torts (Second) § 652B (1977).

[48] *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. (stating "all people are by nature free…") 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 (Cal. 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).

[49] 914 F. Supp. at 100-101.

[50] 914 F. Supp. at 99. In "at-will" employment jurisdictions, like Pennsylvania, an employer may discharge an employee with or without cause, at pleasure, unless restrained by contract. Reciprocal rights exists for employees, who may end an employment relationship with an employer for good cause, bad cause, or no cause at all in the absence of an employment contract. *See Henry v. Pittsburgh & Lake Erie Railroad Co.*, 21 A. 157 (Pa. 1891); *Johnson v. Resources for Human Development, Inc.,* 843 F. Supp. 974, 979 (E.D. Pa. 1994).

[51] 914 F. Supp. at 100. The court rejected Smyth's promissory estoppel claim. According to the court, despite Pillsbury's assurances that it would not reprimand or dismiss employees based on the content of an e-mail communication, the common law of Pennsylvania precludes an employer from being estopped from dismissing an employee based upon a promise, even when reliance is demonstrated. 914 F. Supp. at 100 n. 2.

[52] *Id*. at 99.

[53] *Id*. at 100 (citing *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611, 620 (3d Cir. 1992).

[54] *Id*. at 101.

[55] *Id.*

[56] *Id.* The court's statement appears to constitute dictum since the resolution of the motion to dismiss did not require it to reach the issue of what interest Pillsbury had in intercepting Smyth's e-mail communications. Indeed, under a Rule 12(b)(6) motion, the court had to assume that Pillsbury intercepted the e-mail communications in contravention of company policy. In this regard, Pillsbury's legitimate interests undoubtedly would be substantially diminished when balanced against an employee's interests in his workplace privacy.

[57] *Id.*

[58] *Id.*

[59] *See O'Connor v. Ortega*, 480 U.S. 709, 730 (1987) (Scalia, J., concurring noting that "it is privacy that is protected by the Fourth Amendment, not solitude."); *Mancusi v. DeForte*, 392 U.S. 364, 369 (1968) (stating that privacy expectation did not change simply because a person shared an office with others).

[60] *See Ohio v. Robinette*, 519 U.S. ___., 117 S. Ct. 417, 421, 136 L.Ed. 2d 347 (1996) (court addressed issue of reasonableness in the context of the 4th Amendment).

[61] Of course, computer communications actually occur without palpable physical dimensions. Although some computer users can actually see and talk to each other through video-conferencing or some other such device, most users send computer communications through an electronic system for which they have no idea where the actual computer server is physically located or where the digitized data travels once it is transmitted.

[62] *See, e.g., Mancusi v. DeForte*, 392 U.S. 364, 369 (1968) (holding that an employee may have a privacy interest in an office even if the office is shared by two other employees); *Katz v. United States*, 389 U.S. 347, 353 (1967) (holding that electronic surveillance of a public telephone without a warrant violates the Fourth Amendment).

[63] *See, e.g., Ortega at 718, infra; Mancusi*, 392 U.S. at 369.

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

[65] *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. Similarly, an individual's expectation of privacy is not eliminated merely because of the fact that each time a person makes a telephone call, subscribes to a magazine or purchases goods or services using a credit card information concerning the contents of the transaction is recorded in database somewhere.

[66] Ortega, 380 U.S. 709, 712.

[67] *Id*.

[68] *Id*. at 713.

[69] *Id*. at 713-714.

[70] *Id*. at 714.

[71] *Id.* at 718.

[72] *Id*. at 730.

[73] *Ortega*, 480 U.S. at 730-731. (Scalia, J. dissenting). Stated another way, while an employee may expect conversations uttered in a normal tone of voice to be overheard by others situated near her, she may not expect to have her conversations lawfully intercepted and monitored in an office in another part of the building by her employer.

[74] 911 F.2d 1573 (11th Cir. 1990).

[75] 911 F.2d at 1577. *Walker* could be considered doctrinally different because Walker sued his employer under Title III of the Omnibus Crime Control and Safe Streets Act of 1968. 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. The issues in *Walker* remarkably resemble issues which might arise in the workplace regarding computer technologies such as e-mail.

[76] 914 F. Supp. at 101.

[77] *Walker, 911* F.2d at 1575.

[78] *Id*.

[79] *Id.* The district court granted summary judgment for Darby who was the named defendant for the United States Postal Service. *Id.* at 1577. 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. *Id*. At 1578.

[80] *Walker* 911 F.2d. at 1577.

[81] *Id.* at 1578.

[82] *Id.*

[83] Important to the discussion of e-mail privacy is Title III's distinction between protected oral communications and protected wire and electronic communications, the latter including e-mail. Title III's definition of "oral communication" is drawn from the principle enunciated in *Katz v. United States*, which protects such communications only when the speaker has a reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 389 U.S. 347, 353 (1967). The ECPA, however, protects "wire communications" and "electronic communications" against interception without reference to the privacy expectations of the parties to the communication. The ECPA includes three primary exceptions to its prohibition against the interception or accession of electronic communications: (1) an exception allowing interception if one of the parties consents; (2) an exception allowing providers of wire or electronic communication services to monitor their lines to ensure adequate service; and (3) an exception allowing interception if done by a device provided by the communications provider or subscriber and done in the intercepter's "ordinary course of business." 18 U.S.C.A. § 2510. Currently, several reported cases have applied the ECPA in the case of new cellular technologies and display pagers, but only one federal case has explicitly applied the Act to e-mail interception or accession. *See Wesley College v. Leslie Pitts*, 1997 WL 547324 (D.Del. 1997); *U.S. v. Carazana*, 921 F.2d 1557 (11th Cir. Fla.), Jan. 30, 1991, (No. 88-5557).

[84] Indeed, Congress recognized that computers were causing the convergence of communications media when it enacted the Telecommunications Act of 1996, Pub. L. No. 104-114 (codified as amended at 47 U.S.C. § 151 *et seq.* (1996)). The Act removed the artificial barriers that Congress had set up under the Communications Act of 1934 between telephone and cable services and recognized that advancement in technology no longer made the restrictive regulation of distinct media meaningful.

[85] The Internet is simply 100,000 or so interconnected networks that enable computer users connected to one of those networks to transmit electronic data to computer users connected to any one of the interconnected networks. This network of networks is global and may include as many as 10,000,000 computers. Some of the networks connected to the Internet are vast and are often referred to as the backbone providers of the Internet; such networks would include Sprint, UUnet, and MCI Communications Corp. *See American Civil Liberties Union v. Reno,* 929 F. Supp. 824, 830-835 (E.D. Pa. 1996) (noting the fundamental impact of the Internet on modern-day communications).

[86] *See, e.g., American Civil Liberties Union v. Reno*, 929 F. Supp. 824 (S.D.N.Y. 1996) *supra* note 79.

[87] *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).

[88] See *Sable Communications of California, Inc. v. FCC*, 492 U.S. 115, 127-128 (1989) (recognizing that there are justifications for different levels of scrutiny in regulating varying

communications media). *But cf. American Civil Liberties Union v. Reno,* 929 F. Supp. 824, 972-883 (S.D.N.Y. 1996)(recognizing that the Internet is a global, decentralized communications medium and, as such, is more akin to telephone communications than to other media).

[89] *See, e.g.,* Thomas E. Weber, *Line Between e-mail and Voice Mail Fades,* Wall St. J., Thursday, Feb. 13, 1997, at B6. (discussing the emergence of unified messaging technology which allows the user to integrate e-mail and voice-mail messages).

[90] These advancements are noteworthy because we know that Congress did not amend Title III of the ECPA until technological advances made Title III obsolete.

[91] A further advancement in computer communications technology is the emergence of Internet Telephony. Internet Telephony allows computer users, who have access to the Internet, to make what ostensibly is a low cost long distance telephone call to other computer users using a computer's voice communications capability. Internet Telephony calls add no additional cost to companies already connected to the Internet through the company's LAN system and consumer users can use Internet Telephony to make long distance "phone calls" for the price of a local phone call. Video-conferencing is already used using the Internet Telephony technology by many businesses. The FCC issued a Notice of Proposed Rulemaking for Access Charge Reform, April 1996, in response to complaints filed with the agency from local and long distance phone carriers alleging that Internet Telephony technology impermissibly permitted Internet software companies to offer unregulated phone services over the Internet. The FCC is not expected to act until fall 1997. 62 Fed. Reg. 4670 (1997), 1997 WL 34505.

[92] A few commentators have suggested that the purported ease with which computer communications can be intercepted coupled with the fact that computer communications, especially e-mail communications, can be protected via encrypton so that only the person to whom the message is addressed may read the contents, demonstrates that users who do not protect their e-mail communications have little or no expectation of privacy in those communications. Yet, the jurisprudence of the right of privacy has rarely inquired as to what safeguards an individual adopts to establish whether an expectation of privacy exists. Although telephones, and most notably cellular communications, can be tapped or intercepted, individuals using such devices may still expect that the contents of their communications to remain private. Significantly, whether an individual's expectation of privacy is reasonable may, in fact, depend on whether the individual adopted readily available devices to safeguard against known privacy risks associated with the communications device. Currently, it seems doubtful that a court would deem an employee's failure to use encryption when transmitting e-mail as a factor supporting the employee's subjective lack of an expectation of privacy. Use of encryption technology is far from readily available. For one, most useful encryption devices still require computer acumen far above that of the average e-mail user to implement the safeguards. More important, many useful encryption programs are heavily regulated as firearm devices, which cannot be exported outside the United States.

[93] This morass of privacy protections depending on the communications medium used is no insignificant factor when you consider that in *Smyth*, Pillsbury contended that its retrieval of a discarded printout of the contents of Smyth's e-mail communication was not an interception of an e-mail message. *See* Barbara Woller, *Workers have little if any privacy with e-mail,* the Courier-J., June 10, 1996 at 06B (the author quotes James Boudreau, who is identified as an attorney for Morgan, Lewis, & Bockius in Philadelphia, the firm that represented Pillsbury). Under current jurisprudence, an employee could be faced with the difficult burden of determining whether the print out was the result of a digitized voice mail or e-mail communication.

[94] *See generally, ACLU v. Reno,* 929 F.Supp. 824 (E.D. Pa. 1996)(findings of fact paragraphs 12 & 46).

[95] *The Firewall Dilemma: Too few locks, Too many doors,* Byte, August 1996 at 72.

[96] *See generally, American Library Association v. Pataki, 97 Civ. 0222 [LAP]* (N.Y. Sep. Ct., June 20, 1997)(findings of fact).

[97] Even where an employer does not permit its employees to encrypt their e-mail, the fact that an employee does so despite the employer's policy would still seem to manifest the employee's expectation of privacy. Unauthorized use of encryption by an employee would not, by itself, seem to permit an employer to decrypt the message, although the employee could be subject to discipline or discharge for violating company policy.

[98] An employer could also justify monitoring e-mail to prevent employees from leaking trade secrets or committing acts for which a court could hold the employer vicariously liable. *See* John P. Furfaro & Maury B. Josephson, *Electronic Monitoring in the Workplace*, N.Y.L.J., July 6, 1990, at 3; *but cf.* Kirk W. Munroe, *Commercial Eavesdroppin*g: *A Catch 22*, 63 Fla. B.J. 1, 11 (Mar. 1989) (arguing that a company which monitors to prevent employee misconduct potentially exposes itself to "lawsuits, penalties and damages").

[99] *See e.g.*, David F. Linowes & Ray C. Spencer, *Privacy: The Workplace Issue of the 90's*, 23 J. Marshall L. Rev. 591 (1990) (discussing the history of workplace privacy actions); *Vernars v. Young*, 539 F.2d 966, 969 (3d Cir. 1976) (finding a cause of action for invasion of privacy may be maintained if an unauthorized person opens the mail of another).

[100] *See* James Hannan, A Practical Guide to Data Communications Management, 105-08 (1982) (thorough analysis of the basic e-mail encryption devices); *see* Stan Miastkowski, *Put a Positive Lock on your Data*, Byte, Feb. 1989, at 100 (describing the importance of using an e-mail encryption device).

[101] Regarding the final inquiry in assessing the right of privacy in *Smyth*, it is unclear what the

ultimate outcome would be. Clearly, procedurally, the court should have denied Pillsbury's Rule 12(b)(6) motion. Whether, given the benefit of trial, the court would have balanced the interests more favorably for Smyth is open to considerable doubt if Pillsbury obtained the printed e-mail messages from Smyth's trash dispenser. Nonetheless, this point is vigorously disputed by the parties and, therefore, cannot be answered by anyone without the benefit of fact-finding.

[102] 704 F.2d 577 (11th Cir. 1983).

[103] *Id.* at 579

[104] *Id.* at 581.

[105] *Id.* at 581-582. The *Watkins* court stated that it could not expand "the phrase 'in the ordinary course of business' to mean anything that interests a company" because such a broad interpretation of the exception would "flout the words of the statute." *Id. at* 582. Furthermore, the court acknowledged that if a situation ever existed in which an employer could monitor a personal call, then this constituted such a case because the employee discussed matters of great interest to the employer. *Id*. at 583. However, the court concluded that it is unacceptable to formulate a rule including the interception of personal telephone calls within the ordinary course of business. *Id.*

[106] Employers may, however, run afoul state wire-taping laws which often offer victims the opportunity to obtain statutory damages. These laws are often broad enough to protect workers in some states. *See, e.g.*, *Deal v. Spears*, 780 F. Supp. 618, 624 (W.D. Ark. 1991) (finding the two defendant-employers liable for statutory damages to both parties for the monitored telephone conversations and mandating that each defendant pay each conversant $10,000).

[107] Notably, employers have taken widely divergent positions on this issue. Richard A. Danca, *Privacy Act Would Force Firms to Inform Their Employees About E-Mail Monitoring: Privacy Issue Comes of Age in the Networked World*, PC Wk., June 28, 1993, at 203. The American Civil Liberties Union's Task Force on Civil Liberties in the Workplace takes the position that employers should not read employee e-mail. *Id.* The Computer Professionals for Social Responsibility (CPSR), which in fact lobbied Congress to specifically include e-mail in its proposed legislation, says that companies should give individuals more privacy, but that company policies could spell out monitoring practices. *Id*. The Electronic Frontier Foundation in Washington favors employee privacy. *Id.*

[108] Privacy law, as a common law tort, often refers to "the right to enjoy life--the right to be let alone." *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privac*y, 4 Harv. L. Rev. 193, 193 (1890).

[109] Although the emphasis throughout this paper has been on the courts' responses to the

question whether an employer's monitoring of an employee's e-mail communication improperly intrudes upon an employee's right of privacy, it appears dubious that this issue is the kind where each state's judicial system or legislature should be left to deal with this issue as best as it can. Notwithstanding that a significant body of law protecting American workers has emanated from states and local governments, a federal law would have the advantage of reaching beyond the borders of any given state. Consequently, many of the questions that have arisen since *Smyth* could be answered with federal legislation. Notably, as a matter of historical record, important worker protections, ranging from employment discrimination to occupational health and safety, have been the province of a federal statute.