1996

Pandora's (E-Mail) Box: E-Mail Monitoring in the Workplace

John Araneo

Follow this and additional works at: http://scholarlycommons.law.hofstra.edu/hlelj

Recommended Citation
Available at: http://scholarlycommons.law.hofstra.edu/hlelj/vol14/iss1/8

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Labor and Employment Law Journal by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.
PANDORA'S (E-MAIL) BOX: E-MAIL MONITORING IN THE WORKPLACE

I. INTRODUCTION

In the battle between employer monitoring and the employee's privacy rights, the most recent, although inadvertent weapon in the employer's arsenal is the use of e-mail. The rapid proliferation\(^1\) of e-mail in the workplace facilitates the employer's ability to monitor their employees\(^2\) and has brought about unanticipated dilemmas.\(^3\) These problems have yet to be addressed with any consistency by the courts to form a foundational body of cogent precedent.\(^4\) The federal wiretap statute,\(^5\) which apparently addresses this problem, was not drafted for the omnipotent and technologically advanced nature of e-mail. The statute's continued application has revealed both its inability to address e-mail issues squarely and the resulting loopholes.\(^6\)

Today, the issues of e-mail privacy and e-mail monitoring linger in a legal vacuum.\(^7\) Many employers are taking advantage of this situation and are using e-mail monitoring as a technological bullystick over their employees.\(^8\) Unfortunately, as the law stands, there is nothing to prevent them from doing so. However, employers who choose to monitor their employees e-mail do so at their own risk,\(^9\) at least until the law can catch up with technology. This Note addresses the new problems in the

4. See id. at 7; see also Robert Barker, E-Mail Issues, INTERNAL AUDITOR, Aug. 1995, at 60, 62.
workplace brought about by e-mail communication, and analyzes the
deficient state of the law with regard to e-mail privacy for employees.
Then a new analytical approach is suggested for devising a remedial
strategy to create harmony between the employer who chooses to monitor
its employees’ e-mail and his employees. Finally, a solution is posed to
the more immediate problem of employer e-mail monitoring as the law
stands today.

A. E-Mail in Today’s Society

As our society further constructs the new information super-
highway, we are coming closer to a digital and paperless society.10 The
Federal Communications Commission Chairman, Reed Hunt, has
appropriately labeled this social metamorphosis as a “communications
revolution.”11 The next generation, eager to surf cyberspace and share
information via the world-wide web will be intimately familiar, if not
dependent, on the most effective way to engage in this sharing; electronic
mail. Today is merely a transitional stage, as the use of e-mail still
connotes a perception of being on the cutting edge of technology.12
However, this perception will not linger in the masses for much longer.
Soon the excitement in “pointing and clicking” your e-mail box will
evolve into a commonplace act such as that of opening letters and
dredging through junk mail.

The increasing popularity of e-mail is most pronounced in the
workplace. It’s efficient, quick, and the perfect tool to both eliminate
phone-tag13 and receive and disseminate information throughout a large
workforce. For larger companies there are savings to be reaped in paper
and postage costs.14 E-mail facilitates the “free exchange of messages
in a manner similar to talking on the telephone and writing a letter, but
with advantages over both, combining the telephone’s immediacy with

10. See Seifman & Trepanier, supra note 7, at 5.
11. Ilene Knable Gotts & Alan D. Rutenberg, Navigating the Global Information Superhigh-
(praising e-mail as a seductive, high tech and magical means of communication); see also Anie M.
Soden, Protect Your Corporation From E-Mail Litigation; Privacy, Copyright Issues Should be
Addressed in Policy, CORP. LEGAL TIMES, May 1995, at 19 (labeling e-mail as part of a
technological explosion in communication).
14. See id.
a letter’s thoroughness.” Computer law specialist Charles R. Merrill points out that e-mail is so useful because it is independent of geography and time. The bottom line is that e-mail is the preferred choice of communication mediums in corporate America.

The penetration rate of e-mail in Fortune 500 companies of 67 percent in 1990 jumped at hyper-speed to 98 percent in only one year. A survey taken by the Electronic Mail Association’s Research and Statistics Committee projected that the number of e-mail users in Fortune 2000 companies would increase from the 1992 number of 8.9 million to an astounding 15.6 million in just the following year. Recent figures also indicate that 90 percent of all companies with 100 employees or more use e-mail. Overall, nearly 60 million Americans use some form of e-mail to conduct business on a daily basis sending approximately two billion messages every month. The Electronic Association’s 1995 Market Research Study Preliminary Report projects the monetary value of the “e-mail market” to reach 61.3 billion dollars by the year 2000.

B. E-Mail Anatomy 101

This Note uses two different models in discussing an “e-mail system.” It should be noted that systems in the real world may not fit directly into just one of the two categories. Many systems are in fact hybrids or mutations of these two general systems.

The first category, and probably the broadest, is where the employee uses e-mail through a public service, such as America Online, Prodigy or CompuServe. In this environment, the user will transmit a message via

17. See Cappel, supra note 13, at 6.
22. See Donald H. Seifman & Craig W. Trepanier, Evolution of the Paperless Office: Legal Issues Arising Out of Technology in the Workplace, 21 EMPLOYEE REL. L.J. 3 at 10 (discussing both the public and the fully private internal models of an e-mail system); see also Randolph S. Sergent, A Forth Amendment Model For Computer Networks and Data Privacy, 81 VA. L. REV. 1181, 1183-84 (1995).
phone lines that are owned by the public provider. Most often in this situation, the employer acts as a liaison between the employee and the commercial service by paying for the service. This role of "provider," becomes significant under the controlling federal statute. The second category is where the employer owns and maintains an internal system of e-mail communication. It is this situation where the law is most convoluted. It is also important to note that it is common practice in both scenarios to automatically create back up files of all data. This is a normal procedure, usually conducted by a system administrator done for convenience, security and overall maintenance of the system.

C. Emergence of an Unanticipated Problem

Today's new and exciting technology however, spawns new and exciting problems. E-mail privacy is evolving as one of the most frustrating and perplexing legal issues of the electronic-information era, "representing a burgeoning and unsettled area of the law." In the corporate legal community, it has been labeled as a "potential hothouse" for employment related litigation issues. As a result, the legal community is encountering more and more client questions about e-mail privacy. The prudent attorney needs to become familiar with these issues, and shed the common perception that these are strictly intellectual property issues. Both the employer and the employee have legitimate concerns and formidable arguments.

23. See S. REP. No. 99-541 at 5, 8 (1986) (urging the amendment of the current federal wiretap law as to amend so as to include e-mail as a form of protected communication; see also discussion infra Part I.D.


28. See id.


Employers naturally want to know to what extent they can legally monitor their employee’s e-mail messages. As a cost of doing business, the employer needs to be able to identify and remedy any unauthorized or excessive use. Although the cost-per-message is minuscule, it becomes substantial in the context of a company like E.I. du Pont, with its 90,000 employees. Furthermore, the employer needs to protect confidential and privileged information, such as trade secrets. For example, it has been speculated that if trademarked information is inadvertently passed through an e-mail system, it may lose its protection.

Similarly, information that is protected by the attorney-client relationship may lose its shield if it cannot survive judicial scrutiny in determining exactly who had access to the information on the e-mail system. Unfortunately, there is always the risk of losing sensitive information to “hackers” or other unauthorized users on the Internet. Copyright infringement, which is all too common on the Internet, is usually tolerated by subscribers and “surfers” alike, but when the employee of a company with deep pockets is involved, the viability of a lawsuit becomes more attractive to potential plaintiffs. Employer liability for their workers who slander or defame others is also a concern. Finally, an e-mail system can facilitate many forms of employee theft.

Employer’s also face a magnified exposure to liability in the form of sexual harassment when an e-mail system is incorporated into the mix. The employer, who can be liable even without actual knowledge of the

35. See id. at 22 (supporting the premise that since an individual will lose trademark protection if she does not take reasonable efforts to maintain confidentiality, the information being on the system is indicative of the failure to take these reasonable efforts).
40. See id.
41. See id. at 17-18.
42. See id. at 21-22 (noting the risk employers face with regards to it’s employees misappropriating confidential and proprietary information).
harassment, is further imperiled by e-mail because sexual harassment may be occurring between employees, and even the most cautious manager or supervisor will be ignorant thereof. In the absence of e-mail, the manager or other workers may notice the offending behavior, or at the very least, be aware that the two employees are interacting. However, with e-mail at their disposal, harassers may be sending sexually offensive or “flaming” messages in stealth. The second problem is that when the harassment does eventually come out, the victim may in fact be equipped with a virtual transcript of the conduct, because unlike personal communications, there will almost always be a record of e-mail messages. Thus, the potential for damaging evidence is amplified.

Furthermore, use of a bulletin board on a public or private network can be used to impregnate the workplace with a form of sexual harassment known as a “hostile work environment.” E-mail communications are conducive to the creation of a sexually hostile work environment because unlike human interaction, with e-mail communication, colloquial messages are often sent back and forth without the ability to adjust it’s impact. For example, a message may be put on the system and any intended or unintended reader may be offended by it. This same message that is permanently inscribed for the reader, might well have been cut off in conversation due to the speaker’s perception of the listener’s reaction. In short, e-mail allows no impact adjustment, and thereby only increases the chances for the development of a sexually hostile work environment.

These potential problems have already begun to play out in the courtroom. For example, in a 1993 case of sexual discrimination involving Microsoft, the court allowed sexually suggestive e-mail messages that revealed sex-based discrimination to be admitted as evidence at trial. Although still pending in the courts, Microsoft’s

43. See generally Meritor Savings Bank, FSB v. Vinson, 477 U.S. 57 (1986) (holding that an employer need not have actual knowledge of the harassment to be held liable).
45. See Seifman & Trapanier, supra note 39, at 20.
46. Meritor, 477 U.S. at 66.
47. See Seifman & Trapanier, supra note 39, at 19-20 (discussing the anonymous nature of e-mail).
49. See id. at 1194.
recent motion in limine to exclude admission of the e-mail messages into evidence was denied.\textsuperscript{50}

Other forms of general liability are also a concern, because e-mail is a virtual goldmine of information for discovery purposes in litigation.\textsuperscript{51} Since 1970, Rule 34 of the Federal Rules of Civil Procedure has been amended to accommodate the discovery of electronic communications.\textsuperscript{52} Because of the perception that e-mail, which magically disappears at the touch of a button, has a less corporeal quality than written memorandums, often employees will transmit extremely sensitive, if not potentially incriminating information. This “out of sight, out of mind” perception of many employees can be extremely damaging to companies being sued and incredibly valuable to those bringing suit. Today there are actually new companies who specialize in the service of seeking computer evidence for use in litigation.\textsuperscript{53}

The discoverability of e-mail can also be extremely expensive for an employer who is ordered to produce it for litigation. The courts may push the employer to provide extensive amounts of e-mail for evidence purposes, even at costs exceeding thousands of dollars.\textsuperscript{54} In any event, since the probability of having to disclose e-mail communications in litigation is very likely, and considering the potential degree of harm it can cause, plus the significant monetary costs, this is a legitimate concern for any employer.

Another area of concern for the employer is the threat of unionization via e-mail systems. Frank C. Morris, a partner at Epstein, Becker & Green, in Washington D.C. uses the metaphor of “a real sleeping giant”\textsuperscript{55} to indicate how the problem of union solicitation via e-mail may soon be the topic of some interesting legal debate. The evolving


\textsuperscript{54} See, \textit{e.g.}, \textit{In re Brand Name Prescription Drugs Antitrust Litigation}, No. 94 C 897, MDL 997, 1995 WL 360526, at *1 (N.D. Ill. June 15, 1995) (holding that the employer must pay the approximately sixty thousand dollar cost of producing the e-mail evidence requested by the class-plaintiffs). \textit{But see} Bass Public Limited Co. v. Promus Companies, No. 92 Civ. 0969 (SWK), 1994 WL 702052, at *1 (S.D.N.Y. Dec. 15, 1991) (declining to order the employer to produce e-mail communications for a staff of 100 employees in favor of requiring the same for a smaller set of ten employees).

status of "no solicitation rules" in the workplace has been less than consistent, and arguably, the rules developed under the National Labor Relations Act ("NLRA") by the National Labor Relations Board ("NLRB") could not have been articulated with the forethought of such a potent communication medium as e-mail. Employers now must deal with the threat of union infiltration or solicitation through their own e-mail systems.

The limited precedent involving e-mail and union solicitation indicates that traditional rules of discriminatory union treatment to work regulations will apply. Suffice it to say here that companies with valid no solicitation rules will indeed be subject to electronic communications in contravention to these rules. Unfortunately, they may be forced to test the legalities of this issue for the rest of the world.

Employee's concerns are quantifiably minimal in comparison, but qualitatively, they arouse some visceral fundamental rights. Employees that use e-mail are becoming more and more dependent on it as a means of communication. In turn, there is an inherent desire and need for privacy over one's e-mail messages, as there is with personal phone calls or an employee's desk. Employer monitoring presents a vast array of issues with respect to the rights, needs and desires of employees, but what is most pertinent here is the issue of the employee's reasonable expectations of privacy.

58. See E.I. duPont de Nemours & Co., 311 NLRB 893 (1993) (holding that the employer violated § 8(a)(1) of the NLRA by prohibiting the union to use the e-mail system which had been used in the past for non-work purposes).
59. See generally Randolph S. Sergent, A Forth Amendment Model For Computer Networks and Data Privacy, 81 VA. L. REV. 1181 (giving a detailed analysis on the privacy rights that are most often challenged by computer networks).
60. See discussion supra Part I.B.
D. Current Legislation

1. The Electronic Communications Privacy Act of 1986

"There's no law that says your boss can’t read your e-mail or tap your phone."\(^{62}\)

The federal statute that addresses the legality of intercepting and monitoring e-mail communications is the Electronic Communications Privacy Act of 1986 ("ECPA").\(^{63}\) This statute amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968,\(^{64}\) also known more casually as the "Federal Wiretapping Statute,"\(^{65}\) to include electronic communications.\(^{66}\) The ECPA's purpose was to update the current federal statute to account for new technology and electronic mediums.\(^{67}\) As one commentator put it:

In 1986 the United States Congress extensively amended the federal wiretap law in order to bring most electronic communications within it's protective cloak. The new legislation expressly targeted electronic mail (e-mail), as well as other common forms of non-aural electronic data communications. The law, as amended protects e-mail messages from interception by and disclosure to third parties . . . . The law contains several major exemptions, however, some of which should prove important . . . . Employers who choose to take advantage of the exceptions to prohibition should take precautions to ensure that the law protects their conduct.\(^{68}\)

The ECPA has many detailed sections and has received mixed reviews from commentators. The Federal Court of Appeals for the Fifth Circuit has commented that "understanding the Act requires understand-

\(^{62}\) Lauren Coleman-Lochner, *Candid Camera: Many Companies Spy on Their Workers*, BERGEN REC., Jan. 9, 1995, at C4 (quoting Lewis Maltby, Director of Workplace Division, American Civil Liberties Union).


\(^{65}\) Steve Jackson Games, Inc., v. United States Secret Service, 36 F.3d 457, 460 (5th Cir. 1994).


\(^{68}\) Id.
ing and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analysis."\(^6\)\(^9\) Additionally, the Court stated that the act was "famous (if not infamous) for its lack of clarity.\(^7\)\(^0\) Nonetheless, the ECPA has been noted for its ability to prohibit computer eavesdropping,\(^7\)\(^1\) and as legislation that affirmatively intended to close loopholes in the statute which were created by advancing technology.\(^7\)\(^2\) Yet there has been some criticism on how well the act adapts itself to new technology.\(^7\)\(^3\) The concern is that merely rewording a statute originally drafted for telephone eavesdropping cannot be adapted to confront the new and unique quandaries created by technology.\(^7\)\(^4\)

The ECPA prohibits interception, use and disclosure of electronic communications.\(^7\)\(^5\) The statute expressly allows victims of interceptions to bring a civil action.\(^7\)\(^6\) The statute will grant actual damages as well as punitive damages of any profits made by the violator as a result of the violation, and statutory damages of whichever is greater of 100 dollars a day for each day of the violation, or a sum of 10,000 dollars.\(^7\)\(^7\) The ECPA also allows for equitable relief,\(^7\)\(^8\) including declaratory judgments\(^7\)\(^9\) and the granting of attorney and legal fees.\(^8\)\(^0\) Finally, the ECPA may also impose criminal penalties.\(^8\)\(^1\)

The wiretapping statute, prior to the ECPA amendment, only protected interceptions of "wire and aural communications."\(^8\)\(^2\) Not all electronic communications are aural (heard by the human ear). Those that are not aural, by definition, were not protected. The ECPA merely added

---

69. See Jackson Games, 36 F.3d at 461.
70. Id. at 462.
74. See id.
76. See id. § 2520(a).
77. See id. § 2520(2)(A)(B).
78. See id. § 2707(b).
79. See id. § 2707(b)(1).
80. See id. § 2707(b)(3).
81. See id. § 2701(b).
82. 18 U.S.C. § 2510(4) (1968). The statutory definition of "intercept," at that time included only the aural acquisition of the contents of wire or oral communications through the use of a device. Id.
the words "or other," to the definition of intercept.\textsuperscript{83} In addition, assuming this semantic augmentation was not enough, the ECPA also interjected within the statute the term "electronic communication,"\textsuperscript{84} complete with its own definition.\textsuperscript{85}

In short, the most significant changes in the statute boil down to the interpolation of a few words which render the relevant statutory language to read "the aural or other acquisition of the contents of any wire, electronic or oral communication."\textsuperscript{86} Obviously, these words have proved to be less than the ideal solution to the problems brought by new technological communication mediums.\textsuperscript{87}

2. Exceptions and Exemptions

i. Provider/Business Use Exception

In protecting against "interception," the ECPA includes an express provision that results in a latent exception. Pursuant to the statutory language, interception requires the use of any "electronic . . . device."\textsuperscript{88} However, in defining "device,"\textsuperscript{89} the statute exempts any device that is furnished to the user by the "provider of the wire or electronic communication service, in the ordinary course of its business . . . ."\textsuperscript{90} As a result, if the courts will construe an employer as a "provider," then it seems that the employer may indeed have a blanket license to intercept any communication that is related to business use.

The exception is reiterated later in the statute by providing that it shall not be unlawful for an "operator of a switchboard, or an officer, employee or agent of a provider . . . to intercept . . . that communication in the normal course of his employment while engaged in any activity

\textsuperscript{84} Id. § 2510(12).
\textsuperscript{85} Id. "Electronic Communication" is defined 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 photooptical system that affects interstate or foreign commerce, but does not include-(A) any wire or oral communication (B) any communication made through a tone-only paging device; or (C) any communication from a tracking device. Id.
\textsuperscript{86} Id. § 2510(4).
\textsuperscript{87} See Paul Frisman, E-Mail: Dial ‘E’ for ‘Evidence,’ CONN. L. TRIB., Dec. 18, 1995, at 5 (commenting that ECPA provides more protection for phone calls then for e-mail).
\textsuperscript{89} Id. § 2510(5).
\textsuperscript{90} Id. § 2510(5)(a)(i).
which is a necessary incident to the rendition of his service . . . .”

Labeled as the “provider” or the “business use exception,” these two exceptions may indeed be the statutory loopholes for those employers who choose to monitor their employee’s e-mail.

The business use exception has been subject to judicial interpretation, but predominately in the context of intercepting phone calls, not e-mail transmissions. However, because of the similarities between the two mediums, the courts’ interpretations and applications are a good indicator of how it would be applied to e-mail. Briefly, for this exception to apply, it seems that the business purpose must be one that is credible, and the monitoring or intercepting cannot be excessive.

The exception will also extend to situations where the employer can prove he is preventing the corrosion of the work environment by misconduct or that he has a justified suspicion regarding an employee’s disclosure of confidential information.

With the current state of the law and the way the statutory language is drafted, it seems there is a loophole well within the employer’s grasp. If the employer requires that all e-mail is to be used for business purposes only, this will preserve the protection of the business use exception, because all transmissions on the system will either be business related or in violation of the e-mail policy, which in either case gives the employer the right to read them.

ii. Consent

Another caveat lies in the area of consent. The ECPA allows interception of communications where there is some form of consent. Specifically, the statute allows interception where “such person is a party to the communication or one of the parties to the communication has

91. Id. § 2511(2)(a)(i).
92. Pedrow & Kohn, supra note 72, at 37.
95. See Pedrow & Kohn, supra note 72, at 37.
96. See Sanders, 38 F.3d at 741.
97. See id. But see Epps v. St. Mary’s Hosp. of Athen’s Inc., 802 F.2d 412 (11th Cir. 1986) (applying the business use exception to a situation where the employer overheard and recorded a phone conversation containing disparaging remarks between two co-workers).
98. See Epps, 802 F.2d at 417.
given prior consent to such interception." The consent can be express or implied and it has been held that "consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights." Furthermore, there may in fact be implied consent by the employees under many circumstances. For example, employees who use the e-mail system after the employer has announced a clear policy of monitoring the system may have in fact given "implied consent" to the monitoring. However, recent case law indicates that mere knowledge of an employer's capability to monitor does not alone equal implied consent, and an employer's warning alone, without actual proof of notice to the employee that she is in fact being monitored, may not be enough to establish implied consent.

In short, the resulting loophole is actualized merely by implementing creative ways to establish implied consent as per the court precedent. The guileful employer could simply program a pre-logon screen to the system, notifying the users that the company retains the right to monitor all communications for business purposes. Here, the act of the employee logging-on would most likely manifest implied consent. However, because of the capricious nature of the limited case law, the legality of this policy would hinge largely on the clarity and significance of the notice given.

3. Unequal Treatment

In today's workplace, companies with different needs will employ different e-mail systems. Some employers will subscribe to commercial services, others may provide their own gateway onto the Internet and still larger companies may have their own internal, company-owned systems. Unfortunately, in each situation, the ECPA's spotty protection becomes even more convoluted. It seems that where the
employer subscribes to a public service, the law is in its most lucid form.  

In the environment of a company-owned, internal e-mail system, the ECPA’s protection is at its weakest. There are proprietary rights of the employer, derived from the fact that they own the system. Another potential argument is that with internal e-mail systems, the communications do not pass throughout a system that affects interstate or foreign commerce, thereby making the federal statute inapplicable. Despite evidence that Congress did intend for the ECPA to apply to private corporate systems, the prevalent view among lawyers is that with internal systems, employees do not have privacy rights in their e-mail communications. Finally, it is unclear whether the “business use exception” will apply to a private system.

As stated earlier, many systems will automatically create back-up files of all computer data. It is common knowledge that there are legitimate reasons for doing so; computer viruses, lost files, and overall maintenance of the system. However, with an internal system, the back-up files now become the property of the company. Since the information is “stored,” access to it is not considered an interception, because the acquisition is not “contemporaneous with its transmission.”

However, Title II of the ECPA was drafted to account for this situation. Chapter 121 of the ECPA is entitled “Store Wire and Electronic

111. See generally Steve Jackson Games, 36 F.3d 457 (holding that stored e-mail, the fruits of an internal system, were given less protection then contemporaneously sent messages).
113. The ECPA only regulates communications that effect interstate or foreign commerce. 18 U.S.C. § 2510(12) (1994).
114. See Laurie T. Lee, Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop,' 28 J. MARSHALL L. Rv. 139, 152 (1994) (noting that Congress did intend for ECPA to include intra-company networks, but only expressly to wire communications).
118. See Bourke v. Nissan Motor Corp., 2 Civil B068705 (Cal. Ct. App. 1993) (holding that the company had a right to anything on the e-mail system because it was owned by the employer).
119. Steve Jackson Games, 36 F.3d at 460.
120. Id.
Communications and Transactional Records Access." Here, "access without authorization" to the stored information is prohibited. The ECPA distinguishes the two scenarios by providing separate definitions for "electronic communications," and e-mail messages that are kept in "electronic storage." The term "electronic storage" refers to any temporary, or intermediate storage of a wire or electronic communication including all back-up files.

A thorough analysis of the statutory provisions reveals that "stored" electronic communications are not protected as vigilantly as contemporaneous electronic communications. First, when comparing stored "wire" communications from stored "electronic" communications, the former requires a court order, while the latter is only conditioned upon a search warrant. Second, with contemporaneous electronic communications, a court order allowing authorization of interception is confined to certain limitations on how the interception is to be conducted. The interception must be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception," and "must terminate upon attainment of the authorized objective." There are no such requirements for acquiring stored electronic communications through a search warrant. Finally, intercepting electronic communications are acutely restricted in duration by providing that an interception may not be conducted "for any period longer than necessary . . . nor in any event, longer than thirty days." Again, there are no such restrictions for accessing stored communications.

This distinction between electronic communications and those that are stored is significant in the environment of a company-owned internal system. This is because the employer is endowed with the ability to

122. Id. § 2701(a)(1).
123. See supra note 85.
125. Id. § 2510(17)(a).
126. Id. § 2510(17)(b). The statutory definition for "electronic storage" reads: (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. Id. § 2510(17).
127. See Steve Jackson Games, 36 F.3d at 462.
129. Id. § 2703.
130. See id. § 2518(5).
131. Id.
132. Id.
133. Id.
create backup files of all data transcribed on the system, and use it as they wish.\textsuperscript{134} The need to "intercept" as per the ECPA's definition is therefore extinguished. Moreover, the tangible nature of these backup files is more conducive to the assertion of property rights than are the transmissions themselves. This grants the company with the right to view the files on the hard drive and every message passing through the system that is put on backup.\textsuperscript{135} The end result is that an employer who has no right to intercept a given communication may avoid liability by waiting for the system to store it in backup.\textsuperscript{136}

Thus, the ECPA is to be commended for its spirit in attempting to confront the problems created by new technology. However, it fails in practical applicability.\textsuperscript{137} Since its enactment in 1986, the evolution of the ECPA has exposed both its unanticipated flaws and the resulting statutory loopholes. Perhaps the problems lie not in the statute itself, but in the drafter's ignorance of the need for new legislation. The poignant words of Thomas Jefferson are illustrative of the problem:

\begin{quote}
Laws and Institutions must go hand and hand with the progress of the human mind. As that becomes more enlightened, as new discoveries are made, new truths discovered and manner and opinions . . . advance also to keep pace with the times. We might as well require a man to wear still the coat which fitted him when a boy.\textsuperscript{138}
\end{quote}

Unfortunately, the essence of the ECPA's remedial efforts is comprised of cosmetic alterations of a statute originally drafted for phone lines, not the sophisticated, technological mediums of the future. Rather than trying to adapt or reclothe the weathered original, it is imperative that new legislation be drafted from scratch to adequately and squarely confront the unique dilemmas of the modern era.

Furthermore, the sporadic composition of case law tackles only a few of the problems presented, and serves only as the beginning of

\begin{flushleft}

\textsuperscript{135} See Cahoon, \textit{supra} note 117, at 56.


\end{flushleft}
foundational precedent that the courts will ultimately build upon. Until there is a more complete body of cogent precedent, the case law remains convoluted and insufficient. Thus, the current state of the law is in a state of flux. As it stands, employers will continue to have the right to monitor and read their employees’ e-mail in most situations.

In order to reach the gravamen of the problem, it is imperative to step back from the legal sphere of existing laws, new amendments and court interpretations, and look to where the problems lie; the workplace. It is only in this context that the real problems will emerge, and a legitimate remedial strategy can be created.

The first step is to realize that there is a conceptual dichotomy between the expectations of the employer and that of the employee. One author describes the two opposing spheres of thought as the “casualness of speech” versus the “permanence of writing.” An employer who either pays for access to a public service or pays for the entire system has a justified perception of the system's utility; that being a business tool used for business purposes. Moreover, today's employer is fully cognizant of the virtual window e-mail can create to the inner workings of her company. Many ephemeral comments usually made within the halls, bathrooms or even in discrete private meetings may be sent through the system by an employee. Since these comments can mature into hard copy documents, there is the risk of them being used against the company, or losing them to discovery in litigation.

However, from the employee’s perspective, the e-mail system is a convenient way to communicate from one computer to another, or to many others. Common in e-mail transmissions are the spelling errors and typos which are so universally forbidden on the more perennial written memo. Also a typical occurrence is the latest O.J. Simpson joke sent through the e-mail system. These are just two indicators of what the average employee perceives the system to be; a casual, convenient and transient way to communicate with other employees.

Also extremely inviting, but equally inaccurate, are the begging analogies to the telephone and the United States Postal Mail. The use of

139. See James J. Cappel, Closing the E-Mail Privacy Gap, 44 J. SYS. MGMT. 6, 11 (1993) (discussing the lack of precedent that states whether e-mail monitoring is legal).
140. See id.
141. See, e.g., Cappel, supra note 139; see also Eric S. Freidburn, Get the Message? Workers Don’t Own Their E-Mail, CRANs SMALL BUS. CHI., Sept. 5, 1994, at 33.
142. See Paul Frisman, E-Mail: Dial 'E' for 'Evidence,' CONN. L. TRIB., Dec. 18, 1995, at 1 (praising e-mail as a seductive, high tech and magical means of communication).
143. See id.
the work phone for personal matters is a necessity for anyone working a full-time job, and thus, accepted by the employers. It is reasonable to expect privacy for these matters over the phone, so why should this theory change just because the e-mail system is used instead of the phone system? Furthermore, since e-mail is a form of "mail," there is an inherent connotation of the strict privacy safeguards in the postal mail.\textsuperscript{144} The fact that there are user passwords on the typical system\textsuperscript{145} only reinforces this presumption. Finally, when the employee deletes the message, he or she has every right to believe it is in fact deleted.\textsuperscript{146} But as discussed earlier, there is always some type of backup being stored, and it seems that this backup is almost impossible to hide from expert computer hackers.\textsuperscript{147}

It is important to note that neither perception is unfeasible. Both the employer and the employee have tenable arguments and legitimate concerns. After the recognition of this "conceptual dichotomy," it becomes clear that both parties are in the dark as to the natural perceptions of their counterpart. Moreover, the natural tendency to parallel e-mail to either the postal mail or to telephone communications only exacerbates the distance between the two opposing perceptions. E-mail has its own identity and character, and ultimately it brings to the table new problems of employee privacy and employer monitoring. Once this concept is fully digested, only then can appropriate legislation be drafted.

II. PROPOSAL

A. Require Employers to Develop and Publish an E-Mail Policy

In amending the federal wiretap statute, the ECPA merely rephrased and altered the statutory language. Unfortunately, this was not the ideal means to the desired end of finding the appropriate balance between employee privacy rights to their e-mail\textsuperscript{148} and the employer's reciprocal

\begin{footnotes}
\item[145] See Cappel, supra note 139, at 12.
\item[146] See Pedrow & Kohn, supra note 144, at 36-37.
\item[147] See supra note 27 and accompanying text.
\item[148] See generally Witt, supra note 137.
\end{footnotes}
rights to monitor the e-mail system.\textsuperscript{149} The purpose of this writing however, is not to achieve this equilibrium nor even to suggest its existence, but rather to urge a simple solution to the problem at hand. Until the law can catch up with technology, the employer should be required to provide clear and detailed policies for how the e-mail system is to be regulated in the workplace. The employer who embraces this philosophy clearly retains control over how their system is governed, yet is practicing defensive management against the unreliable state of the law. The incorporation of such a policy would clearly delineate the rights retained by the employer and those granted to the employees. The effect then, would penetrate the core of the “conceptual dichotomy,” because it pins down all the wandering perceptions of both parties and converts them into rights and wrongs.

Enacting an e-mail policy detailing how the system will be maintained and regulated will be beneficial to the employer and at the same time allow them to remain autonomous in choosing how to run their own environment. For example, many companies today such as Federal Express, Du Pont and United Parcel Service outwardly proclaim their rights over their employees’ e-mail.\textsuperscript{150} Other companies like General Motors, McDonnell Douglas and Citibank have adopted a “hands off” philosophy\textsuperscript{151} that is based on “mutual trust and respect.”\textsuperscript{152} Therefore, a requirement to enact an e-mail policy preserves the employer’s independence to choose the philosophy that is most suitable to its corporate culture. What a policy will do is provide notice to the employees of exactly what rights are granted to them and those that remain vested in the employer. This in turn, clearly informs the employees as to what type of environment they are in, and how to act accordingly. In fact, studies show that employees will be more amenable to an announced monitoring policy than to being kept in the dark, even if the announced policy reserves the highest degree of employer monitoring.\textsuperscript{153}

\textsuperscript{149} See Robert Barker, \textit{E-Mail Issues}, \textit{INTERNAL AUDITOR}, Aug. 1995, at 62 (suggesting there is little in the way of statutory or case law that would allow the employer to determine what is allowed or what can be done to protect the company from exposure to liability if it decides to monitor it’s employees e-mail).

\textsuperscript{150} See Cappel, supra note 139, at 6-7.

\textsuperscript{151} John K. Keitt, Jr., & Cynthia L. Kahn, \textit{Special Report; The Law of Intellectual Properties; Changes and Complexities}, \textit{LEGAL TIMES}, May 2, 1994, at 24, 28.

\textsuperscript{152} Id.

\textsuperscript{153} See Cappel, supra note 139, at 9.
The realities in today's workplace illustrate further the need to require employers to devise an e-mail policy. One survey indicates that 22 percent of the responding companies reviewed their employees' e-mail,154 and 60 percent of these companies concealed this fact.155 Thus, most companies that admit to e-mail monitoring are keeping their employees in the dark. Other data have indicated that less than 10 percent of United States companies have e-mail policies.156 Finally, another report has indicated that 76 percent of the companies studied were unaware if an e-mail policy existed at all within their environment.157

It follows then, that there is a noticeable amount of ignorance in the workplace as to the need for e-mail guidelines and monitoring policies, and currently employers have yet to take a proactive stance.158 The increasing likelihood that e-mail will be subject to and pursued for discovery purposes159 also extends the need for employers to enact a clear policy, from a defensive point of view. If employers make clear the sensitive and unprotected nature of e-mail to their employees, this may prevent the inadvertent disclosure of vital information, in the event of litigation.160 While a similar notification made to employees during the course of a pending lawsuit or investigation may tend to inculpate the company, implementing this policy ahead of time will be viewed as a prudent preventative management practice.161

Ideally, new legislation is needed to successfully remedy the problems with employer e-mail monitoring. Encouraging employers to develop e-mail policies and publish them to their employees however, is a simple interim solution to the problem of e-mail monitoring. It avoids the more intricate and complicated arguments of to what degree the

155. See Jeffery A. Van Doren, E-mail Policies are a Must, AM. LAW., Dec. 1995, at 14.
158. But cf. Margaret C. Phillips, The Challenge of Defining 'Acceptable Use,' LEGAL TIMES, Jan. 22, 1996, at 838 (suggesting that some employers have enacted policies on their e-mail monitoring practices, although most are already obsolete).
159. See Paul Frisman, E-Mail: Dial 'E' for 'Evidence', CONN. L. TRIB., Dec. 18, 1995, at 1; see also supra notes 53-54 and accompanying text.
161. See id; see also Robert Barker, E-Mail Issues, INTERNAL AUDITOR, Aug. 1995, at 62 (asserting simple e-mail regulations and policies will help limit the potential for legal issues to arise).
employer can, in fact, monitor the e-mail system,162 and the right to employee monitoring in general,163 as they are issues that require new legislative efforts.

It is important to note the implicit concession made by the courts to the employer in holding that they should have the choice to reasonably monitor the system.164 In return for this concession then, the employer should be required to exercise their advantageous role responsibly. The creation, implementation and dissemination of the type of e-mail monitoring practice chosen by the employer is the ideal avenue to reach this goal.165

The premise of enacting an e-mail policy is not necessarily an infant theory. Many articles have discussed their legitimacy,166 and even suggested its adoption.167 In fact, there is even a toolkit available to assist employers in developing e-mail policies.168 One author even asserts that there are already a lineage of e-mail policies in many companies across the country, and that they are already obsolete.169 However, the reality is that most companies have yet to collectively adopt these policies, and empirical data supports the notion that companies are completely ignorant of what an e-mail policy is and what it can do.170

As discussed earlier, the current state of the law puts the employer in such an advantageous position,171 he or she may not see the need to spend the time or the energy to create and implement an e-mail policy. However, this perception will only backfire on the employer because without a policy, she stands on weaker footing in the face of sexual

164. See, e.g., Frisman, supra note 159, at 5 (conceding that employers do have the right to monitor e-mail systems under the current state of the law).
166. See Van Doren, supra note 155 at 14.
169. See Phillips, supra note 158, at S39.
170. See discussion supra Part II.A.
171. See discussion supra notes 135-36 and accompanying text.
harassment claims, discovery requests for litigation and the risk of losing privileged or confidential information.

The best way to initiate a trend or clear a path for the adoption of e-mail policies is to require the employer to enact them by statute. Until a more appropriate body of legislation is enacted, employers who benefit from using e-mail should be required to implement a basic e-mail policy. The essence of the policy will be to provide notice of how the system will be maintained and monitored. The ideal policy, discussed below, should also inform the employees of the sensitive nature of e-mail communications. A statutory, administrative or regulatory requirement will not hinder the employer because it poses no restrictions on them besides that of documentation of the policy. The employer still retains its autonomy to decide how to regulate its system. The instability of the current state of the law and the rapid proliferation of e-mail in the workplace are fusing together to create a certain clash between the opposing perceptions of the employer and the employee. It is predicted that the problems will soon penetrate the courtrooms to develop into the next litigation nightmare. This can be rectified at an early stage if the employer is forced to take a proactive stance in developing an e-mail policy.

B. Pending Legislation

The idea of requiring employers to develop e-mail policies by statute has in fact been previously attempted. The Privacy for Consumers and Workers Act ("PCWA"), was such an attempt. The PCWA has many supporters, its primary sponsor being Senator Paul Simon (D-Ill.). The House sponsor is Pat Williams (D-Mont.), and the American Civil Liberties Union. In addition, members of corporate America have assisted in the bill’s drafting and revisions.

172. See supra notes 43-50 and accompanying text.
173. See supra notes 51-54 and accompanying text.
174. See supra notes 34-38 and accompanying text.
175. See Cappel, supra note 168, at 7 (commenting that e-mail privacy has emerged as one of the stickiest legal issues of our time).
178. Lewis Maltby, Director of the ACLU’s Workplace Division has helped draft and revise the bill. See Coleman-Lochner, supra note 177, at C4.
179. See Coleman-Lochner, supra note 177, at C3. One member of corporate America is Micheal Tamer, the owner of Teknkon, a manufacturer of surveillance equipment. His presence was an effort
The bill was created as a response to the current anomaly of the ECPA's aftermath. For example, under the ECPA, the Federal Bureau of Investigation is required by law to obtain a court order to wiretap a conversation, even in cases of national security, yet private employers are permitted to spy at will on their employees and the public.\textsuperscript{180} Both the House version\textsuperscript{181} and the Senate version\textsuperscript{182} have been introduced to their respective legislative bodies in the 102nd and 103rd congressional sessions.\textsuperscript{183} However, to date, neither version has been passed.\textsuperscript{184}

There has been some political resistance to the PCWA that is preventing it from being passed. One of the drafters has blatantly commented that it's prospects are bleak, presumably because of the Republican sweep in Congress.\textsuperscript{185} Other authors find flaw in the bill due to the fact that the two versions are incompatible and that it provides inconsistent protection to employees based on seniority.\textsuperscript{186}

The bill, in general, relates to electronic monitoring and surveillance, only one method of which is e-mail. Its core provision is that "people have a right to know when they're being watched."\textsuperscript{187} If passed, the PCWA would regulate any individual or business entity employing any number of workers\textsuperscript{188} and require these employers to tell their new employees when and how they would be monitored.\textsuperscript{189} The Senate's version requires that the day and hour of the monitoring be given,\textsuperscript{190} but the latest revision of the House bill does not.\textsuperscript{191} The total time an employee could be monitored would be capped at two hours per week as per the Senate version,\textsuperscript{192} although the House bill does not limit this at all for the first sixty days of employment.\textsuperscript{193} Finally, the random
monitoring of employees who have over five years at the company would be prohibited in the Senate version, but is permitted to continue under the House version. The bill does not, however require notice to the employees of monitoring if the employer suspects the employee is engaged in unlawful activity, or misconduct that would have an adverse effect on the employer.

The PCWA, as discussed, has met with political obstinence for various reasons. One of those reasons was that the bill contained too many vague terms. The implication of this is that perhaps, if the bill were stripped down to a leaner, more focused proposition, it would be more palatable to the legislature. Although this is an ambitious conclusion stemming from only one of several reasons for its rejection, it is not untenable. Furthermore, since the main premise of this note (providing notice to the employees of the employer's monitoring practices via an e-mail policy) was only one of the requirements of the PCWA, it is logical that a more acute bill embodying only this premise may indeed have a better chance of being passed. The PCWA has in effect, carved a path through the legislative channels for a new statutory, administrative or regulatory endeavor to require employers to create and implement e-mail policies.

C. A Model Policy

Creating, implementing and maintaining the ideal e-mail monitoring policy can be done with minimal effort. There are some fundamental considerations, which are listed here. They are however, by no means exhaustive. Undoubtedly, and somewhat ironically, there is a plethora of such suggestions to be found on the Internet. Employers are encouraged to keep the following ideas in mind when devising their own policies.

1. First and foremost, the employer needs to inform the employees of the type of e-mail monitoring it chooses to adopt. This is vital to set the tone of the working environment and set the employees expectations of using the system.

2. Employers should also discuss the sensitive nature of e-mail. The begging analogies to both the postal mail and telephone calls should be

---

194. S. 984, §5(B)(3).
195. H.R. 1900, §5.
196. S. 984, §5(C)(1).
197. See discussion supra note 184 and accompanying text.
clearly discredited, informing them the latter two forms have certain privacy safeguards, while e-mail does not.

(3) Employees should be reminded of the potential use of e-mail in litigation whenever they use the system.

(4) Employers should warn employees that technology is always building a better mousetrap and their messages are never completely safe from third party access.

(5) A document retention time frame should be implemented. This keeps the employee aware of the fact that backup is kept only for a limited amount of time. The benefit to the employer is that with less backup available, there will be less risk of liability. This also encourages the employees to be more efficient in the sense that they need to be aware of what files they actually have, instead of falling into more laxadasical habits of relying on backup.

(6) Employers may also want to provide passwords or encryption facilities to protect individual files, and mandate that no employees can enter the files of another without consent. Note, however, that taking this step may create an implicit expectation of privacy. The employer should disarm this expectation by reminding the employees that although these safeguards are implemented, there is no zone of guaranteed privacy.

(7) E-mail messages of a harassing, intimidating, offensive or discriminating nature should be strictly prohibited, and be designated as grounds for dismissal.

(8) Regardless of whether the employer enacts a restrictive or permissive monitoring practice, she should require that e-mail is to be used for business purposes only. This will activate the "business use exception," and allow the employer to investigate legitimate business concerns.

(9) To implement the policy, employers should have a policy submitted to the entire staff, new hires, and periodically redistribute it. Each copy should have an assigned release form, to be signed by the employee, signifying that they have read and understand the policy. Access to the system should be frozen until the form has been returned.

(10) Finally, an efficient method to ensure notice has been provided is to install a pre-logon screen into the system saying that there is an existing e-mail policy each user should be aware of. If the screen informs

199. See discussion supra Part I.D.2.
the user that the employer reserves the right to monitor the system, the logging on may later be construed as a manifestation of implied consent.

III. CONCLUSION

In closing, the problem of e-mail monitoring in the workplace inevitably brings the needs of the employer into a head-on collision with the privacy rights of their employees. As discussed, both parties have legitimate concerns underlying their respective positions. Unfortunately the law, in its current state, offers no clear cut rules to work with. The controlling federal statute is clearly inadequate in addressing the problems that are occurring in the workplace today. The case law is just beginning to surface and thus is not a strong body of legal precedent.

Therefore the law is in a state of flux with regard to employee e-mail monitoring by employers. Employers have taken advantage of this legal vacuum by monitoring their employee's e-mail and justifying their actions through assertions of the e-mail being employer property or by coercing consent by employee's using the e-mail system. There has been at least one legislative endeavor to address this problem, which remains an unpassed bill, largely for political reasons. Unfortunately, the problem endures, and some action must be taken. This Note urges employers to create, adopt and announce an e-mail monitoring policy. Until the law can catch up with technology and address this problem, such policies will bring a needed balance to the positions of both parties.

John Araneo